THE THREAT OF GEOPOLITICAL ISSUES ON NEW ZEALAND CYBERSECURITY

CHILLISOFT

BY ALEX TEH, CHILLISOFT CEO

ALEX TEH

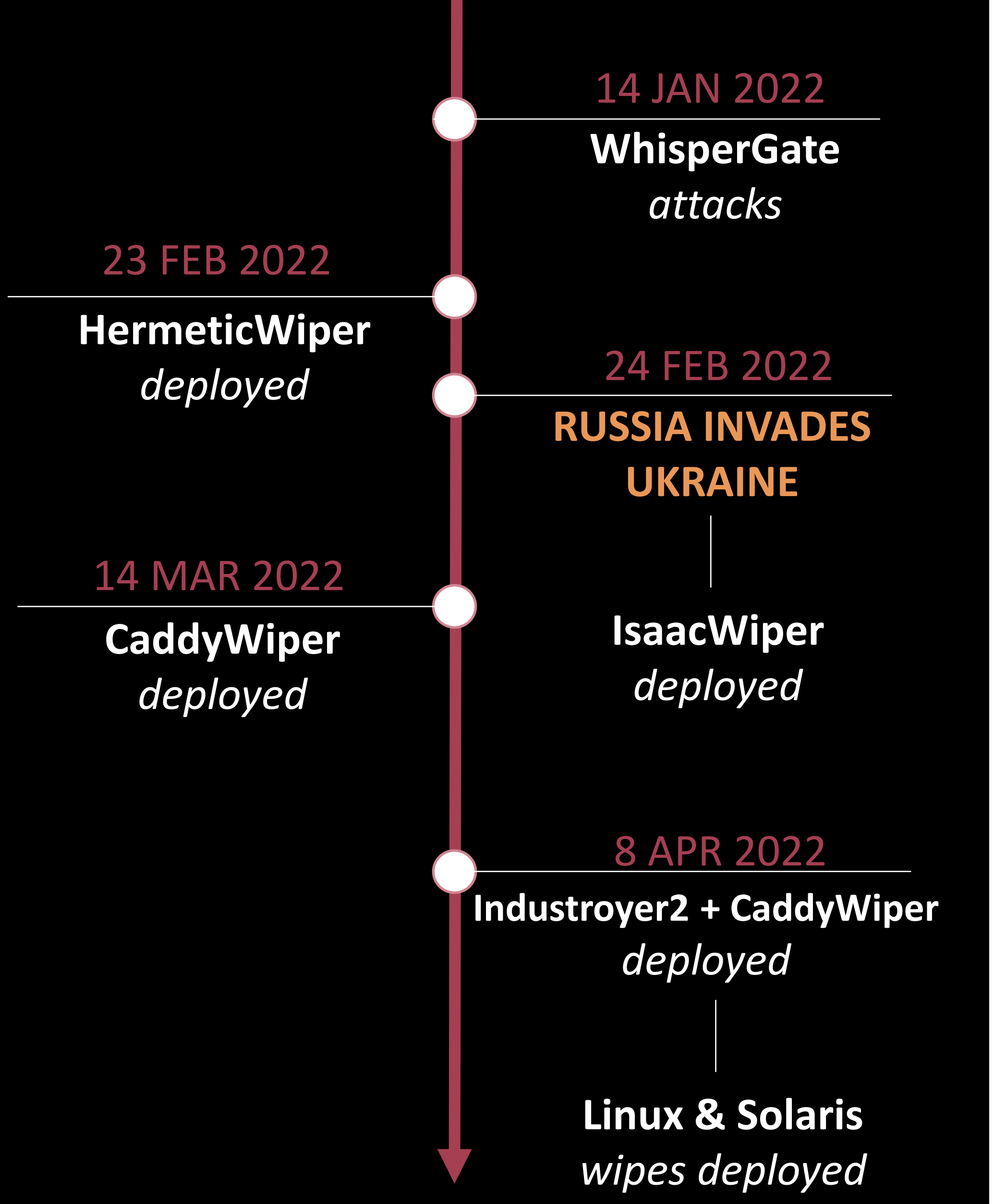
CHILLISOFT CEO

- 25 Years in cybersecurity UK / ANZ
- NZ largest cybersecurity distributor
- Independent 100% kiwi owned
- Represent Gartner leading vendors in every class

A GRIM PICTURE

THE FUTURE IS NOW. CYBER-WARFARE IS PART OF MODERN WARFARE.

ESET Researchers timeline of attacks: Russian invasion of Ukraine



14 JAN 2022

WhisperGate
attacks

23 FEB 2022

HermeticWiper
deployed

24 FEB 2022

RUSSIA INVADES UKRAINE

IsaacWiper
deployed

14 MAR 2022

CaddyWiper
deployed

8 APR 2022

Industroyer2 + CaddyWiper
deployed

Linux & Solaris
wipes deployed

STATE SPONSORED ATTACKS

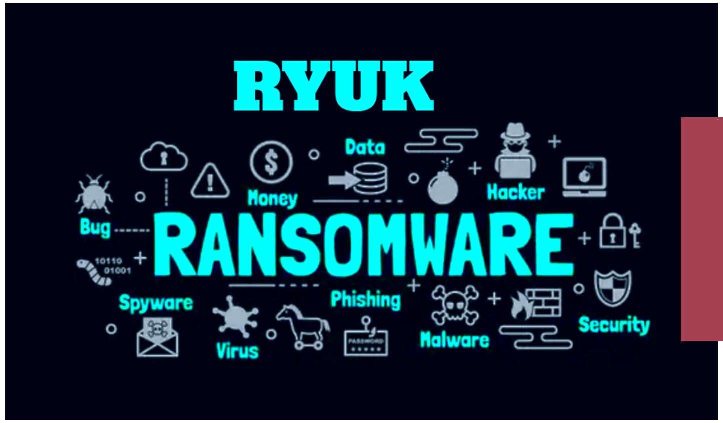
How the Russian attack unfolded

- 1 hour before invasion
  - Viasat US satellite company compromised.
- Ukranian military used Viasat
- “Wiper” malware called Acidrain (modems & router)
- Largest war time hack in history!
- Cross fire also hit 5800 German wind turbines

STATE SPONSORED CYBER WARFARE

CONTI (Russia) VS Anonymous (West)

STATE SPONSORED CYBER WARFARE



CONTI GROUP

Who is Conti Group:

- Inventors of RYUK ransomware
- First successful attack on a Ukranian power station (2015)
- Conti group have an annual payroll of $6mil USD
  *100+ hackers!

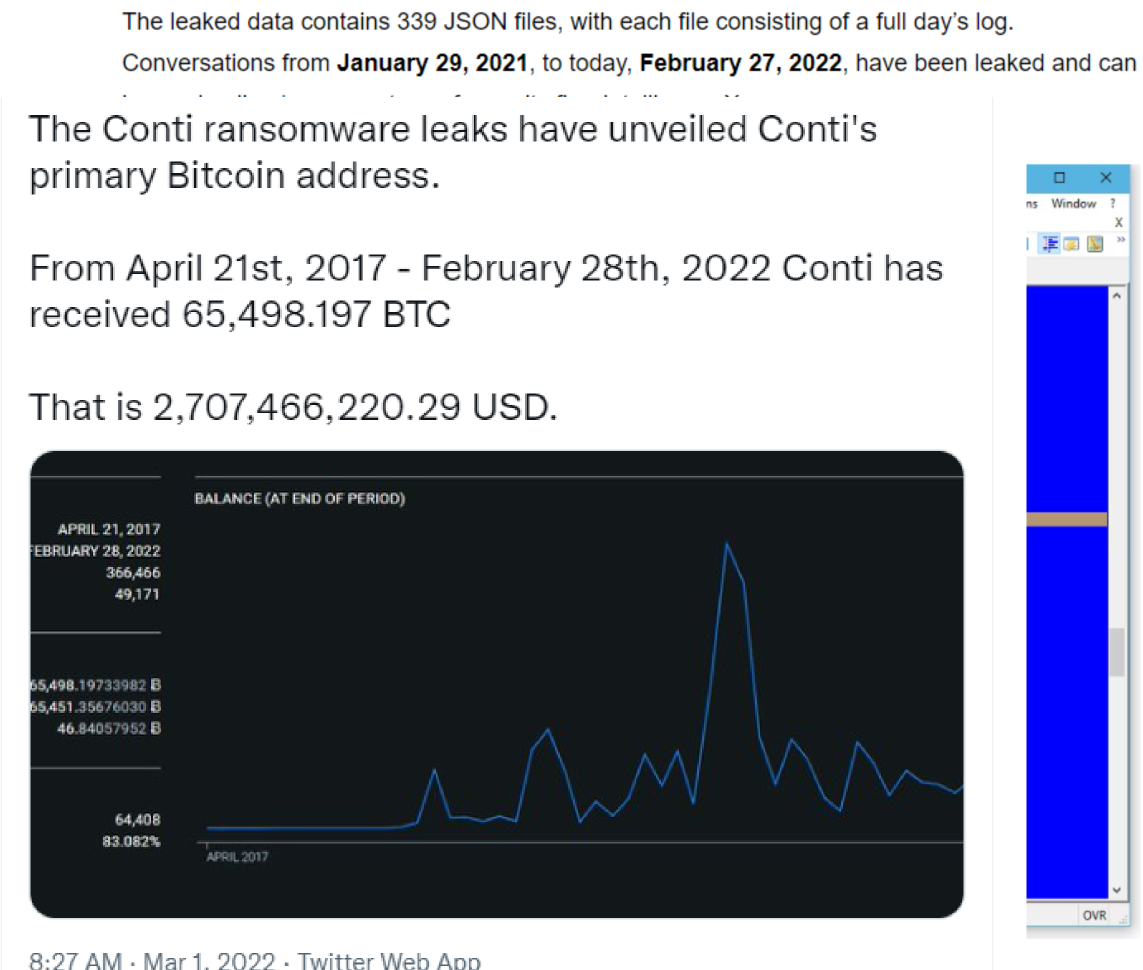
_the situation

- Russian & Ukrainian division splinter
- Internal chat posted on dark web
- Location of a crypto wallet worth $700mil USD of BTC posted
- Total net worth of the “CONTI GROUP” ransomware gang is $2.7BILLION

- UNLIMITED RESOURCES

STATE SPONSORED CYBER WARFARE

RUSSIAN CONTI GROUP



The leaked data contains 339 JSON files, with each file consisting of a full day’s log. Conversations from **January 29, 2021**, to today, **February 27, 2022**, have been leaked and can

The Conti ransomware leaks have unveiled Conti's primary Bitcoin address.

From April 21st, 2017 - February 28th, 2022 Conti has received 65,498.197 BTC

That is 2,707,466,220.29 USD.

8:27 AM · Mar 1, 2022 · Twitter Web App

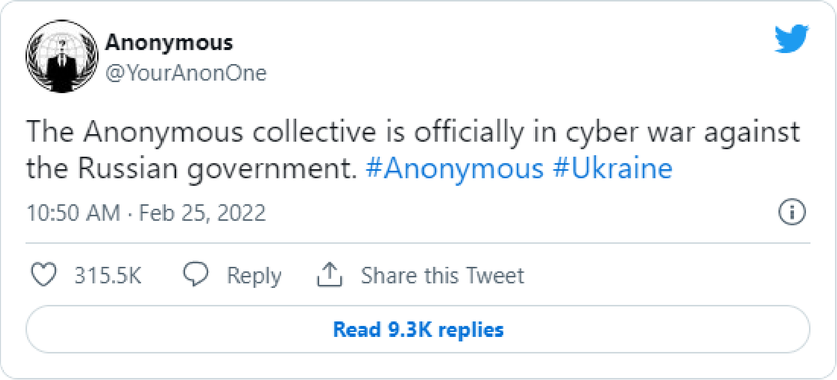
Image: The Record

“We promise it is very interesting,” the leaker wrote in the email sent earlier today.

STATE SPONSORED CYBER WARFARE

HACKIVIST GROUP ANONYMOUS – TOP HACKS:

- **George Floyd Murder**
  – US police force websites take down
- **Arab Spring**
  - GOV of Tunisia, Egypt, Syria all disrupted
- **DDOS attacks on VISA & Mastercard**
  - Payback campaign
- **Free Korea**
  - Demands incl. free speech, democracy + removal of Kim Jong-un



Anonymous
@YourAnonOne

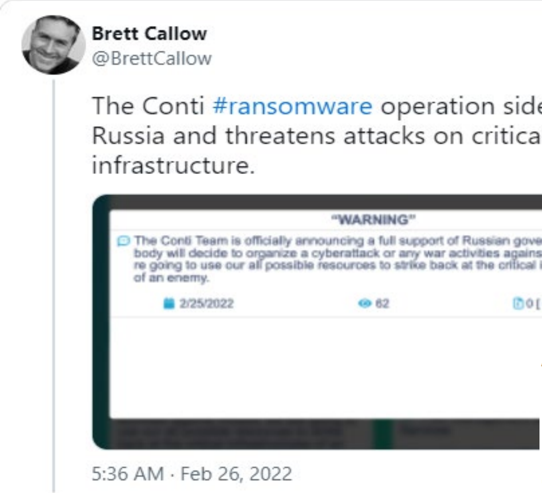
The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine

10:50 AM · Feb 25, 2022

ANONYMOUS

```
<body>
▼<div id="app">
  ▼<todo-application>
    ▼#shadow-root (open)
        <link rel="stylesheet" type="text/css" href="//
        maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta.2/css/
        bootstrap.min.css">
      ▶<style>…</style>
      ▶<nav class="navbar navbar-expand-md navbar-dark bg-
      ▼<main class="container">
        ▼<todo-form>
          ▶<style>…</style>
          ▶<div class="card todo-form">…</div>
         </todo-form>
         <hr>
        ▼<todo-list ref="list">
          ▶<style>…</style>
           <h2>Tasks:</h2>
          ▼<ul ref="todos" class="list-group">
            ▶<todo-task ref="task-1517176192142" id="ta
            …</todo-task> == $0
            ▶<todo-task ref="task-1517176320397" id="t
            …</todo-task>
            ▶<todo-task ref="task-1517176329096" id="t
            …</todo-task>
            ▶<todo-task ref="task-15171763
            …</todo-task>
  </todo-list>
/main>
o-application>
```

STATE SPONSORED CYBER WARFARE



Brett Callow
@BrettCallow

The Conti #ransomware operation sides with Russia and threatens attacks on critical infrastructure.

"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 62 0 [0.00 B]

5:36 AM · Feb 26, 2022

Conti Group threatens western critical infrastructure

Anonymous declare 'cyber war' against Russia

RT.com has also been targeted in what appears to be a widespread denial-of-service (DDoS) attack

'V for Vendetta' Guy Fawkes mask commonly used by Anonymous © Getty Images / artpartner-images

Hacker collective 'Anonymous' has declared a *"cyber war"* against Russia, claiming to have disabled several Russian government websites and that of RT.

Social media accounts claiming to represent the group announced on Thursday evening that they were *"officially in cyber war against the Russian government,"* and had taken down dozens of websites in response to the country's military action in Ukraine.

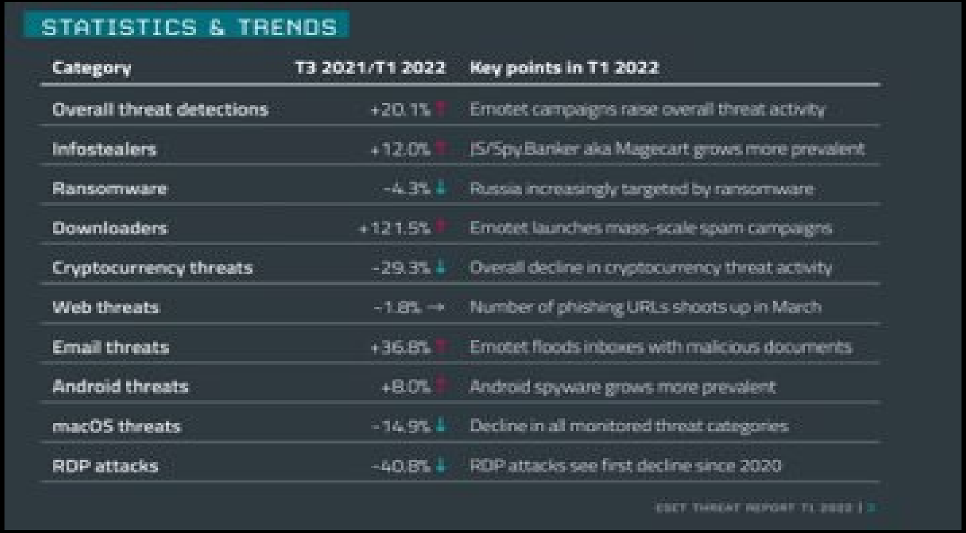
The websites of the Russian government, the Kremlin, the Duma, the Ministry of Defence, and RT were all affected by the apparent cyberattack, with some of the websites slowing down and others being taken offline for extended periods throughout the day.

Anonymous DDOS attacks on Russian Television

20+ DIFFERENT HACKING GROUPS IN THE WAR ON BOTH SIDES!

A lot quieter in the west… For now.

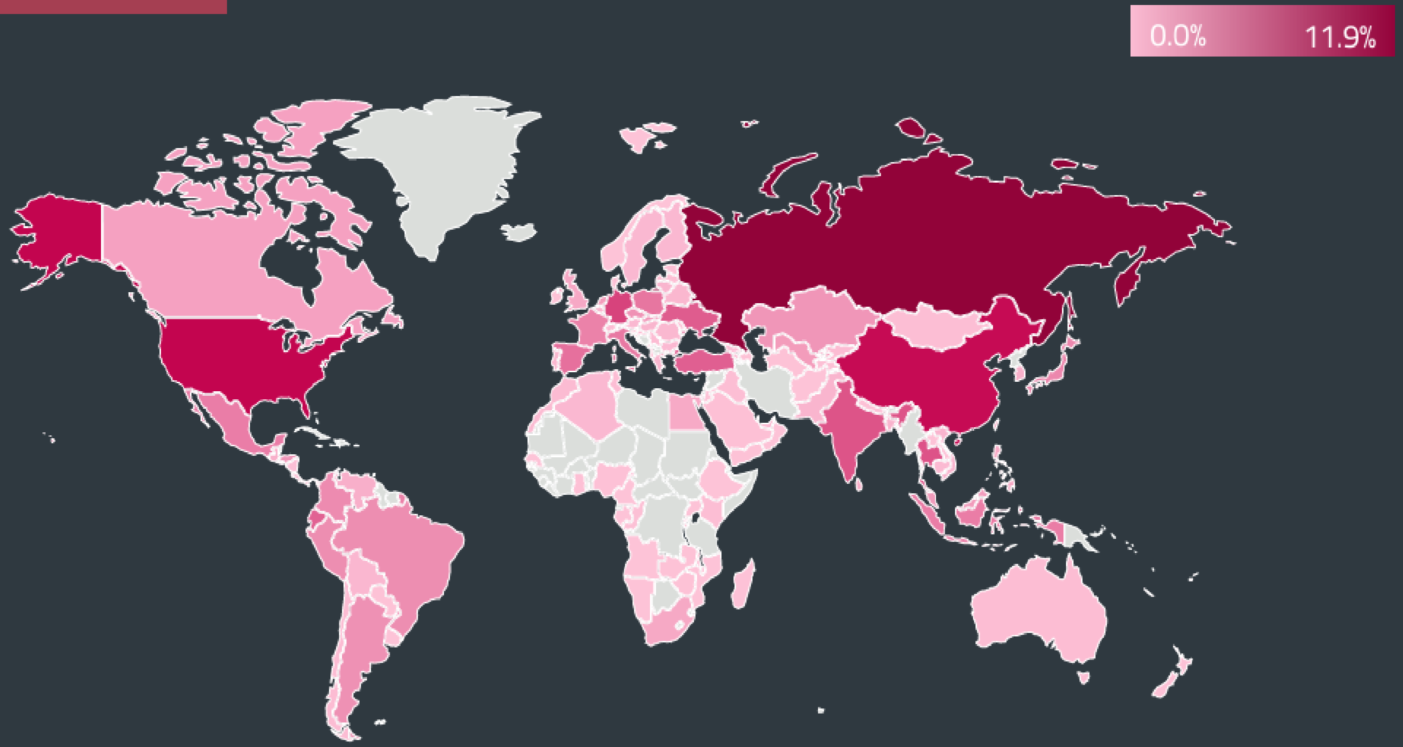
1. Ransomware attacks dropped for the first time in years (-4%)
2. Same time, Russia received 11.9% increase
3. Reduced fear in retribution from Russia



STATISTICS & TRENDS

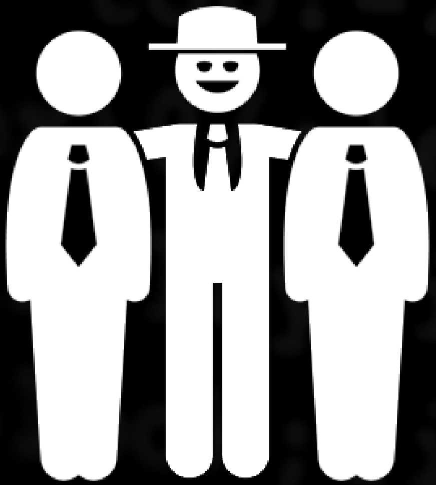
Category	T3 2021/T1 2022	Key points in T1 2022
Overall threat detections	+20.1% ↑	Emotet campaigns raise overall threat activity
Infostealers	+12.0% ↑	JS/Spy.Banker aka Magecart grows more prevalent
Ransomware	-4.3% ↓	Russia increasingly targeted by ransomware
Downloaders	+121.5% ↑	Emotet launches mass-scale spam campaigns
Cryptocurrency threats	-29.3% ↓	Overall decline in cryptocurrency threat activity
Web threats	-1.8% →	Number of phishing URLs shoots up in March
Email threats	+36.8% ↑	Emotet floods inboxes with malicious documents
Android threats	+8.0% ↑	Android spyware grows more prevalent
macOS threats	-14.9% ↓	Decline in all monitored threat categories
RDP attacks	-40.8% ↓	RDP attacks see first decline since 2020

ESET THREAT REPORT T1 2022 |



Global distribution of Ransomware detections in T1 2022

A THREAT ENGINE TO SMART CITIES – SERIOUS ORGANIZED CRIME (SOC)



Crime as a Service

Cryptoware

Malware & I.D. Theft

DDOS and Network Attack

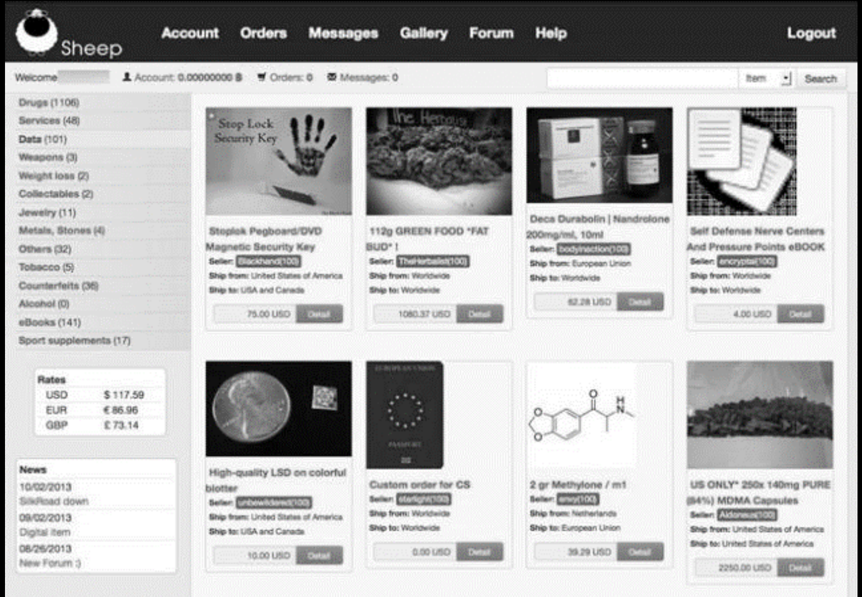
Payment Card / Order Fraud

SERIOUS ORGANIZED CRIME

‘PRODUCTIZATION’ (DARK WEB)

_post war

Highly motivated hacking groups will sell their new tools and bots on the dark web.



Welcome [redacted] Account: 0.00000000 ฿ Orders: 0 Messages: 0

Drugs (1106)
Services (48)
Data (101)
Weapons (3)
Weight loss (2)
Collectables (2)
Jewelry (11)
Metals, Stones (4)
Others (32)
Tobacco (5)
Counterfeits (36)
Alcohol (0)
eBooks (141)
Sport supplements (17)

Rates	
USD	$ 117.59
EUR	€ 86.96
GBP	£ 73.14

News
10/02/2013
SilkRoad down
09/02/2013
Digital item
08/26/2013
New Forum :)

Stoplok Pegboard/DVD Magnetic Security Key
Seller: Blackhand(100)
Ship from: United States of America
Ship to: USA and Canada
75.00 USD

112g GREEN FOOD *FAT BUD* !
Seller: TheHerbalist(100)
Ship from: Worldwide
Ship to: Worldwide
1080.37 USD

Deca Durabolin | Nandrolone 200mg/ml, 10ml
Seller: bodyinaction(100)
Ship from: European Union
Ship to: Worldwide
62.28 USD

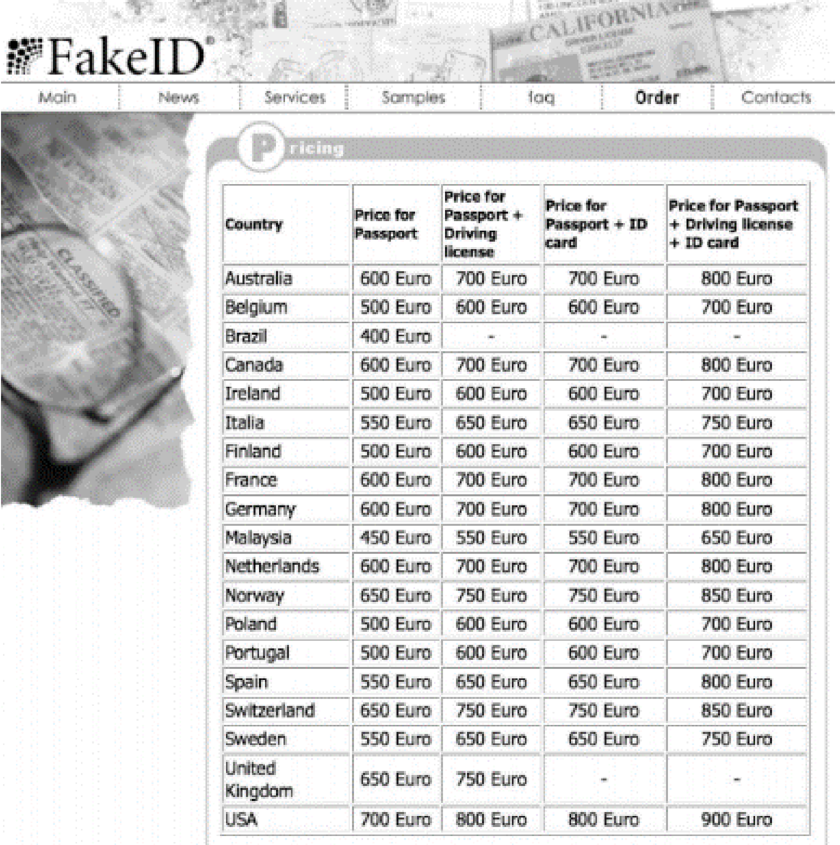
Self Defense Nerve Centers And Pressure Points eBOOK
Seller: encryptal(100)
Ship from: Worldwide
Ship to: Worldwide
4.00 USD

High-quality LSD on colorful blotter
Seller: unbewildered(100)
Ship from: United States of America
Ship to: USA and Canada
10.00 USD

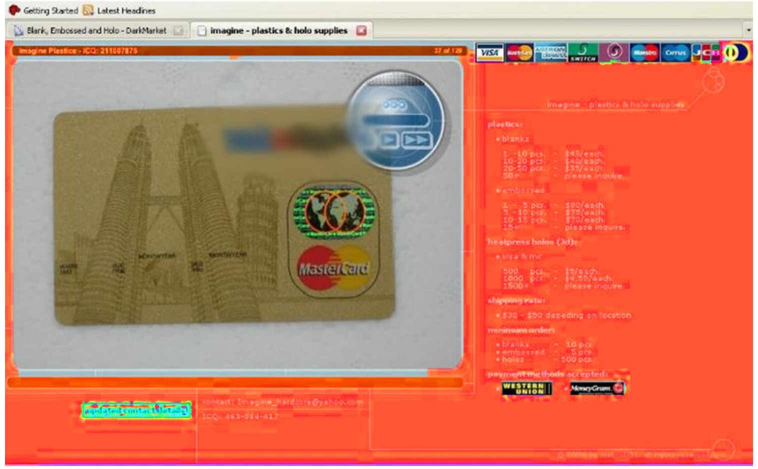
Custom order for CS
Seller: starlight(100)
Ship from: Worldwide
Ship to: Worldwide
0.00 USD

2 gr Methylone / m1
Seller: envy(100)
Ship from: Netherlands
Ship to: European Union
39.29 USD

US ONLY* 250x 140mg PURE (84%) MDMA Capsules
Seller: Aldoneus(100)
Ship from: United States of America
Ship to: United States of America
2250.00 USD



Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro



Imagine Plastics - ICQ: 211507875

27 of 120

imagine - plastics & holo supplies

plastics:

- blanks

```
1 - 10 pcs.   -  $45/each.
10-20 pcs.    -  $40/each.
20-50 pcs.    -  $35/each.
50+           -  please inquire.
```

- embossed

```
1 - 5 pcs.    -  $80/each.
5 - 10 pcs.   -  $75/each.
10-15 pcs.    -  $70/each.
15+           -  please inquire.
```

heatpress holos (3d):

- visa & mc

```
500  pcs.     -  $5/each.
1000 pcs.     -  $4.50/each.
1500+         -  please inquire.
```

shipping rate:

- $30 - $50 depending on location

minimum order:

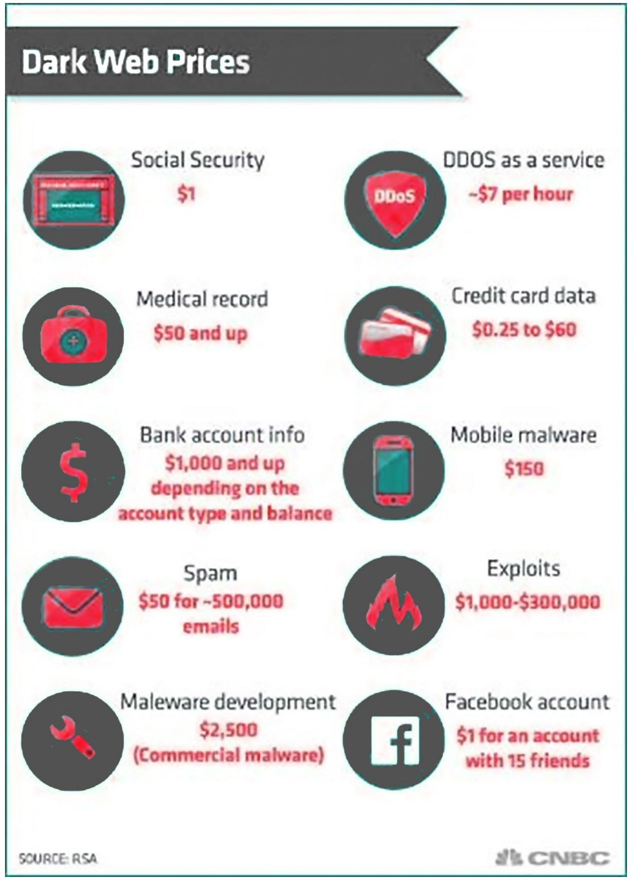
- blanks - 10 pcs.
- embossed - 5 pcs.
- holos - 500 pcs.

payment methods accepted:

updated contact details

contact: imagine_hardcore@yahoo.com

ICQ: 443-014-417



Dark Web Prices

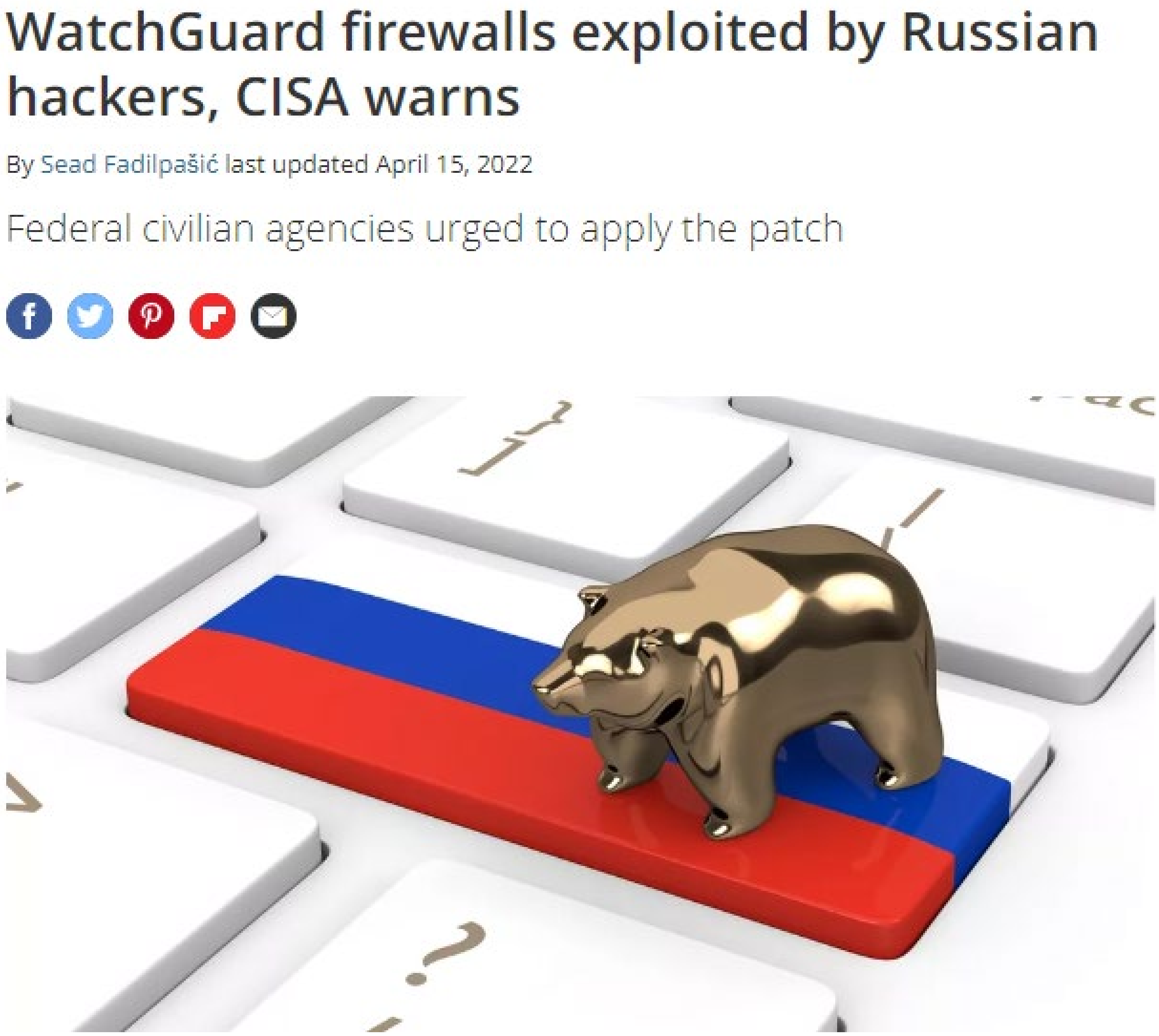
Social Security	$1
DDOS as a service	~$7 per hour
Medical record	$50 and up
Credit card data	$0.25 to $60
Bank account info	$1,000 and up depending on the account type and balance
Mobile malware	$150
Spam	$50 for ~500,000 emails
Exploits	$1,000-$300,000
Maleware development	$2,500 (Commercial malware)
Facebook account	$1 for an account with 15 friends

SOURCE: RSA

CNBC

MORE DDOS BOT NETWORKS CREATED

1. US agency CISA discovered and worked with Watchguard to remediate the problem.
2. Russian group Sandworm developed Cyclops Blink to conduct cyber espionage
3. FBI took down large scale Sandworm botnet network
4. Remember… 2.7 Billion of Bitcoin in one wallet! Unlimited resources.



WatchGuard firewalls exploited by Russian hackers, CISA warns

By Sead Fadilpašić last updated April 15, 2022

Federal civilian agencies urged to apply the patch

NZX Attacks in 2020

1. DDOS attacks came from Ukraine
2. Hacking group – Fancy Bear
   - Started with Web app attacks
   - Moved to Network DDOS attacks
   - NZ Stock exchange down for weeks

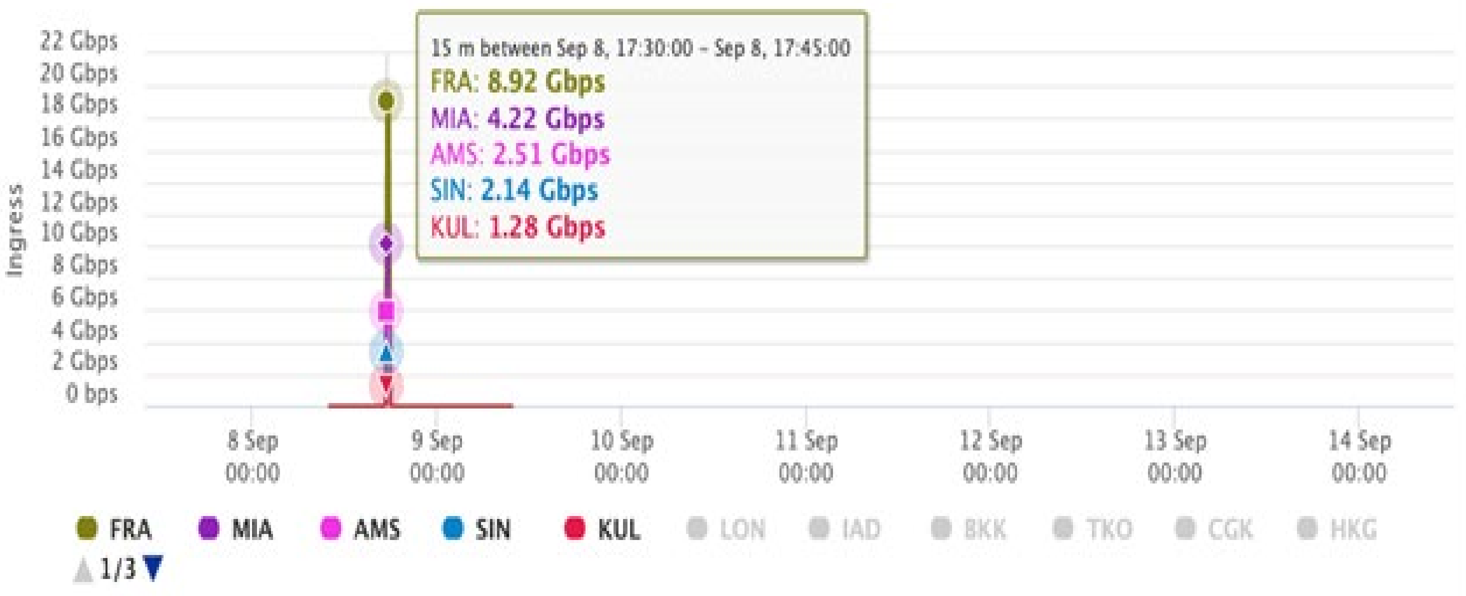
Our website is currently temporarily unavailable.

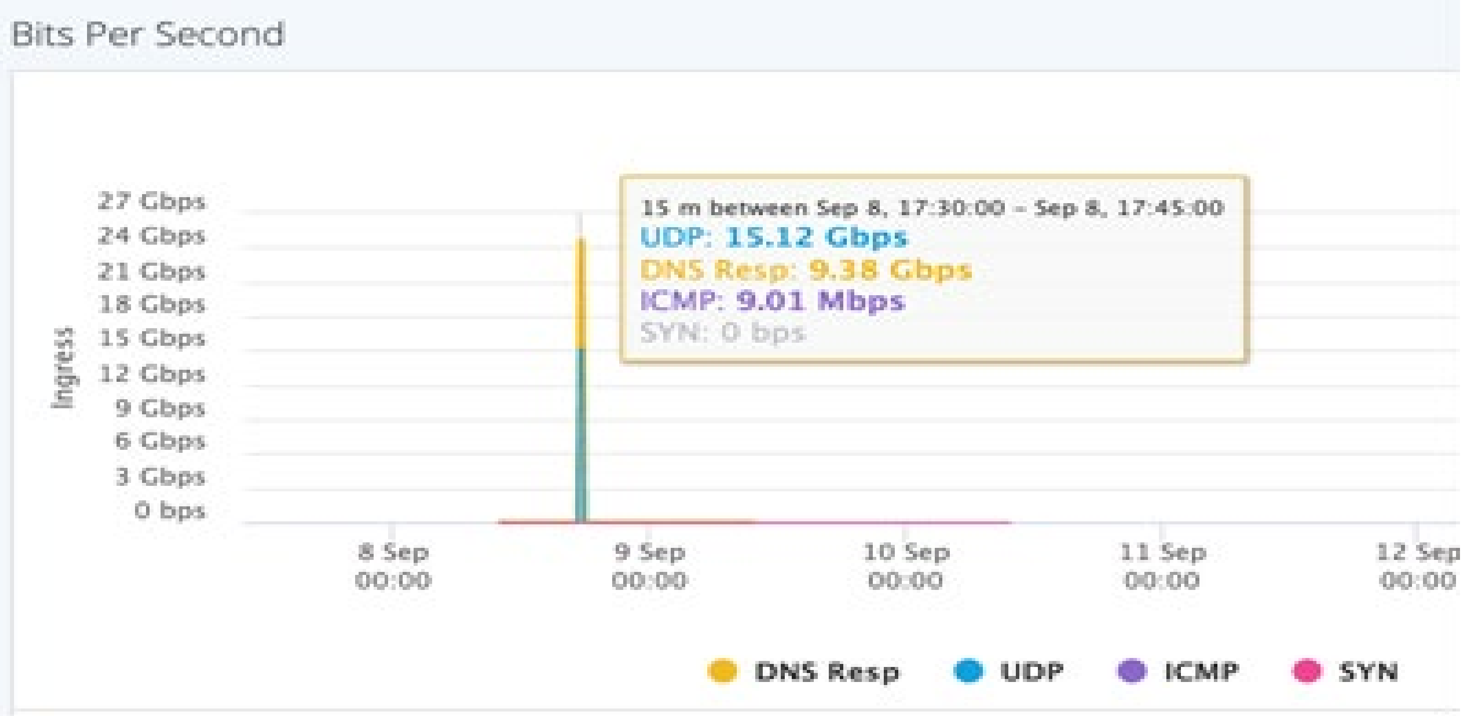
Apologies for any inconvenience that this has caused.

We'll be back soon.

DDOS Attacks in 2021

1. DDOS attacks focused on DNS servers creating issues with customer portals
2. Attacks from Europe and Asia
3. Varied attack protocol vectors
    - DDOS can’t ‘just’ be blocked in NZ
    - Blocking must be done using global DDOS scrubbing centers
    - Attacks on our banks were 6x greater than the attack on NZX
    - Imperva and Radware identified and successfully blocked similar style attacks on their customers.





DDOS Attacks in 2021

1. Volumetric DDOS attacks are more frequent.

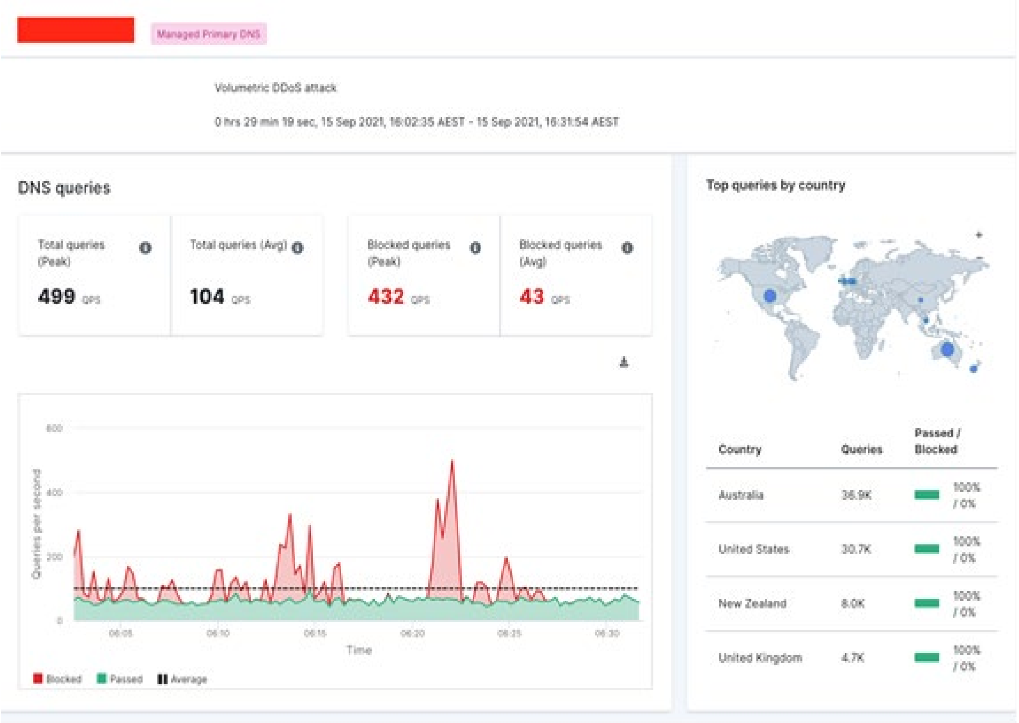
- 42 on one customer which is why you see internal issues!

2. Peaking close to 500 incidents within the hour!

3. DNS attacks show more than 500 queries per minute

4. Many DNS serves have inadequate protection, are outsourced to cloud solutions that do not have appropriate DDOS protection.

5. BOTS are coming from traditional Alliance countries (US, AU, UK)



[redacted] Managed Primary DNS

Volumetric DDoS attack

0 hrs 29 min 19 sec, 15 Sep 2021, 16:02:35 AEST - 15 Sep 2021, 16:31:54 AEST

DNS queries

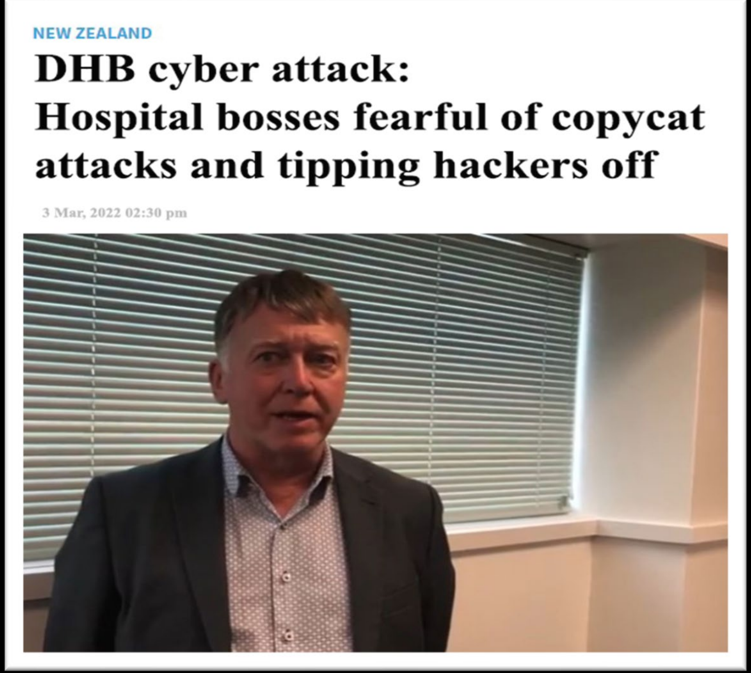
Total queries (Peak)	Total queries (Avg)	Blocked queries (Peak)	Blocked queries (Avg)
499 QPS	104 QPS	432 QPS	43 QPS

Top queries by country

Country	Queries	Passed / Blocked
Australia	36.9K	100% / 0%
United States	30.7K	100% / 0%
New Zealand	8.0K	100% / 0%
United Kingdom	4.7K	100% / 0%

Ransomware on the rise!

1. An NZ DHB became the highest profile attack
2. Five hospitals effected for months
3. 4000+ patient data leaked onto dark web
4. Ministry of Health spending $75mil+ on cyber defenses



NEW ZEALAND

DHB cyber attack: Hospital bosses fearful of copycat attacks and tipping hackers off

3 Mar, 2022 02:30 pm

NZ Threat Landscape – Lets not forget!

10% work from home to 100% in lockdown.

New norm with higher percentage continuing working from home post lockdown.

Multi layer attacks including:

- Covid19 phishing attacks (38% increase)
- Compromised remote users
- Compromised VPN & RDP via brute force attacks
- Compromised network & domain admin
- Disabled, encrypted and data loss of backups

Double ransomware ($1.25mil for decryption and additional $1.25mil for not selling stolen data)

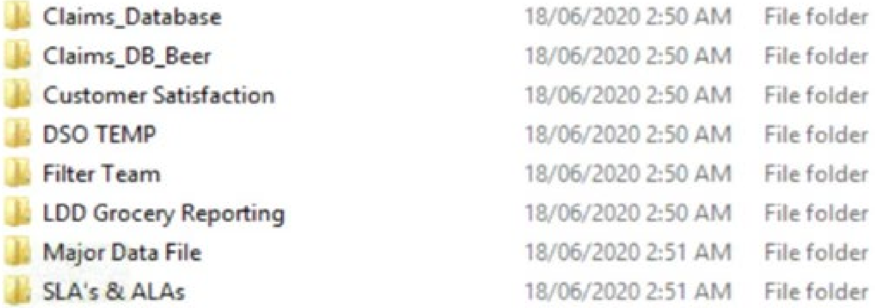
Ransomware attack causing significant problems for large brewery.
12 June 2020

NZ Appliance manufacturer falls victim to ransomware Scourge.
11 June 2020

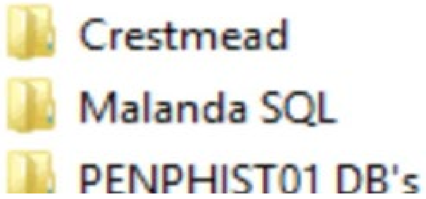
NZ THREAT LANDSCAPE – IT’S COSTLY.

BREWERY THREAT FROM RANSOMWARE

Hello, you have 5 days to contact us and pay, otherwise all your financial, personal information your clients and other important confidentinal documents will be published or put up for auction.



Claims_Database	18/06/2020 2:50 AM	File folder
Claims_DB_Beer	18/06/2020 2:50 AM	File folder
Customer Satisfaction	18/06/2020 2:50 AM	File folder
DSO TEMP	18/06/2020 2:50 AM	File folder
Filter Team	18/06/2020 2:50 AM	File folder
LDD Grocery Reporting	18/06/2020 2:50 AM	File folder
Major Data File	18/06/2020 2:51 AM	File folder
SLA's & ALAs	18/06/2020 2:51 AM	File folder



Crestmead
Malanda SQL
PENPHIST01 DB's

SecurityBrief

Too quick to click: New Zealanders falling for phishing emails

Cyber incidents in NZ surged last year

Comes as CERT NZ warns of coronavirus-themed scams doing the roun

Leon Spencer (New Zealand Reseller News)
19 March, 2020 14:49

Credit: Dreamstime

The number of cyber security incidents reported to the Computer Emergency Response Team (CERT) NZ by businesses and individuals in 2019 surged by 38 per cent compared to the previous year's total, to 4,740.

FOLL

W
us
• Sec
• Dat
• Cas

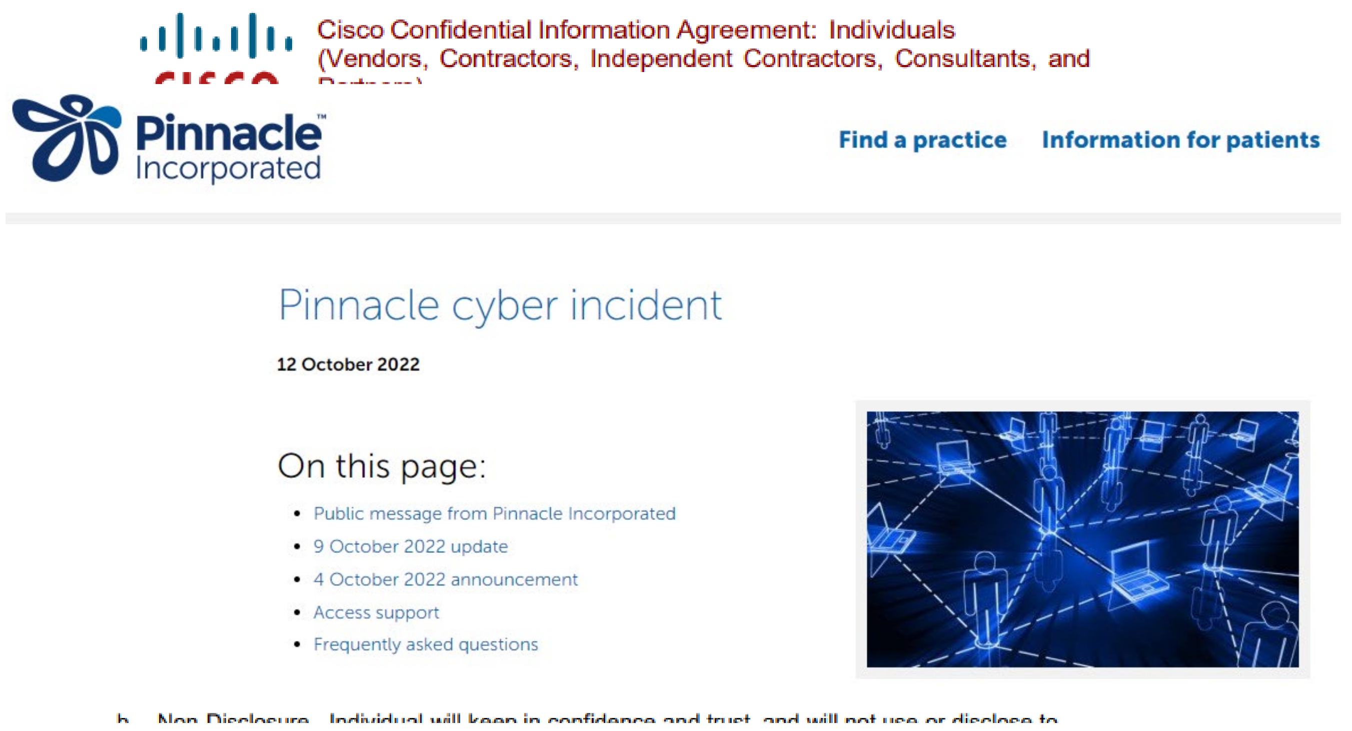
EVEN

Supply chain attacks

- Social engineering caused MFA users to be hacked.
- CITRIX servers & domain controllers compromised through lateral movement.
- 2.75GB of data and 3100 files
- Leaked files uploaded publicly on the web.
- Pinnacle Midlands Health - 3rd party server

- Up to 500,000 patient records exposed

HACKED!



Cisco Confidential Information Agreement: Individuals (Vendors, Contractors, Independent Contractors, Consultants, and Partners)

Pinnacle cyber incident

12 October 2022

On this page:

- Public message from Pinnacle Incorporated
- 9 October 2022 update
- 4 October 2022 announcement
- Access support
- Frequently asked questions

b. Non Disclosure. Individual will keep in confidence and trust, and will not use or disclose to

WHAT CAN WE DO?

ENCOURAGE NEXT GENERATION
TRAINING & INTERN PROGRAMS

SUPPORT LOCAL MSSP'S
WITH LOCAL TEAMS

WORK WITH GCSB+ NCSC
USE MALWARE FREE NETWORK

ADOPT MODERN CYBER PRODUCTS
WITH BUILT IN A.I DRIVEN AUTOMATION

SUPPORT LOCAL MSSP’S

Chillisoft helped build six Security Operation Centers in New Zealand

Cyber CX

Advantage

Inde

JAMES MONTGOMERY FLAGG
I WANT YOU
FOR Cyber Security
NEAREST RECRUITING STATION
CHILLISOFT
COPYRIGHT, 1917, LESLIE-JUDGE CO, N.Y.

Chillisoft Cybersecurity training Centre

- Certified and accredited courses
- Regional and on prem training
- Hands on technical and sales training
- Enables partners to install, consult, and support all our products
- 1000 SOC analyst trained in last 2 years
- We train EDR and SIEM SOC analysts!

“We are Kiwis's, we always punch above our weight, we will fight them on the dark web, we will fight them at our gateways, we shall defend our island, whatever the cost may be and we shall never surrender! We will find our way....

Cyber Tsunami