LockBit ransomware group assemble strike team to breach banks, law firms and governments.

By Kevin Beaumont

Published: 2023-11-14 · Archived: 2026-04-05 16:29:20 UTC

Recently, I've been tracking LockBit ransomware group as they've been breaching large enterprises:

I thought it would be good to break down what is happening and how they're doing it, since LockBit are breaching some of the world's largest organisations — many of whom have incredibly large security budgets.

Through data allowing the tracking of ransomware operators, it has been possible to track individual targets. Recently, it has become clear they have been targeting a vulnerability in Citrix Netscaler, called CitrixBleed. Prior reading:

This has been done in a co-ordinated fashion amongst multiple LockBit operators — a strike team to break into organisations using CitrixBleed and then hold them to ransom.

The Strike

This vulnerability allows the bypass of all multi-factor authentication controls, and provides a point and click desktop PC within the impacted victim's internal network via "VDI" — think Remote Desktop or RDP.

LOCKBIT STRIKE TEAM

The patch became available on October 10th, however as of writing around five thousand organisations still have not installed the patch.

It is also incredibly easy to exploit, and initial exploitation has no logs *at all* as Citrix Netscaler/Gateway fails to log the exploit request — a product defect that Citrix really need to own and fix.

An initial challenge has been maintaining access, as hijacking a session boots off the legitimate user, and the legitimate user boots off the attacker when they reconnect.

To combat this, LockBit have been deploying remote access tools such as Atera — which does not trigger antivirus or EDR alerts — to allow remote, interactive PowerShell requests without any visible signs to the end user. This access also persists after patching CitrixBleed.

The Team

After access is obtained, the victims are passed to the execution team. This team escalates privileges via a variety of techniques, terminates EDR controls, steals data and ultimate deploys ransomware.

The Victims

I am tracking over 10 victims currently being extorted, and lots more in initial stages. As a sample, these include:

- Allen & Overy, one of the world's biggest law firms — attackers entered via an unpatched for CitrixBleed vulnerability Netscaler instance on https://myao-us.myallenovery.net/ — this has now been patched post incident.

  Press enter or click to view image in full size

12:04

69

Detail

Detail

Catalin Cimpanu

@campuscodi@mastodon.soc...

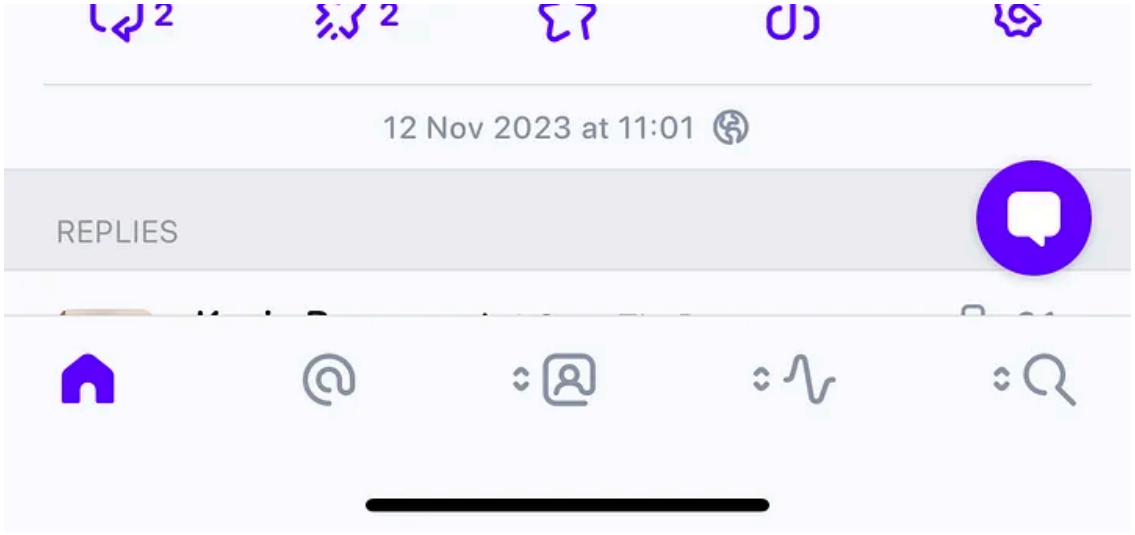
FOLLOWS YOU

A ransomware attack has disrupted the activities of Allen & Overy, one of the largest law firms in the world.

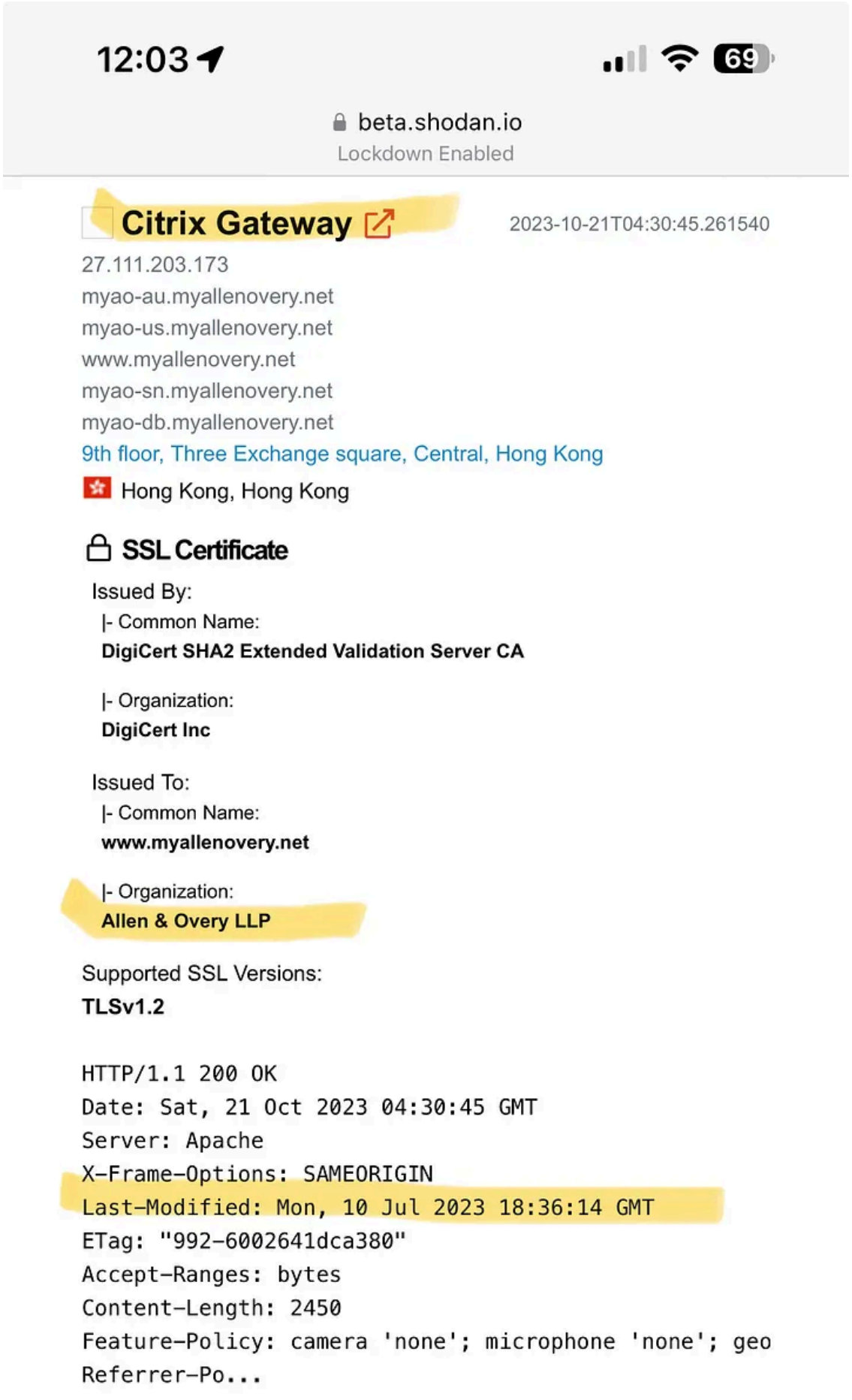
The company confirmed the incident after members of the Lockbit ransomware gang took credit for the attack.

Allen & Overy hit by suspected ransomware attack

fnlondon.com



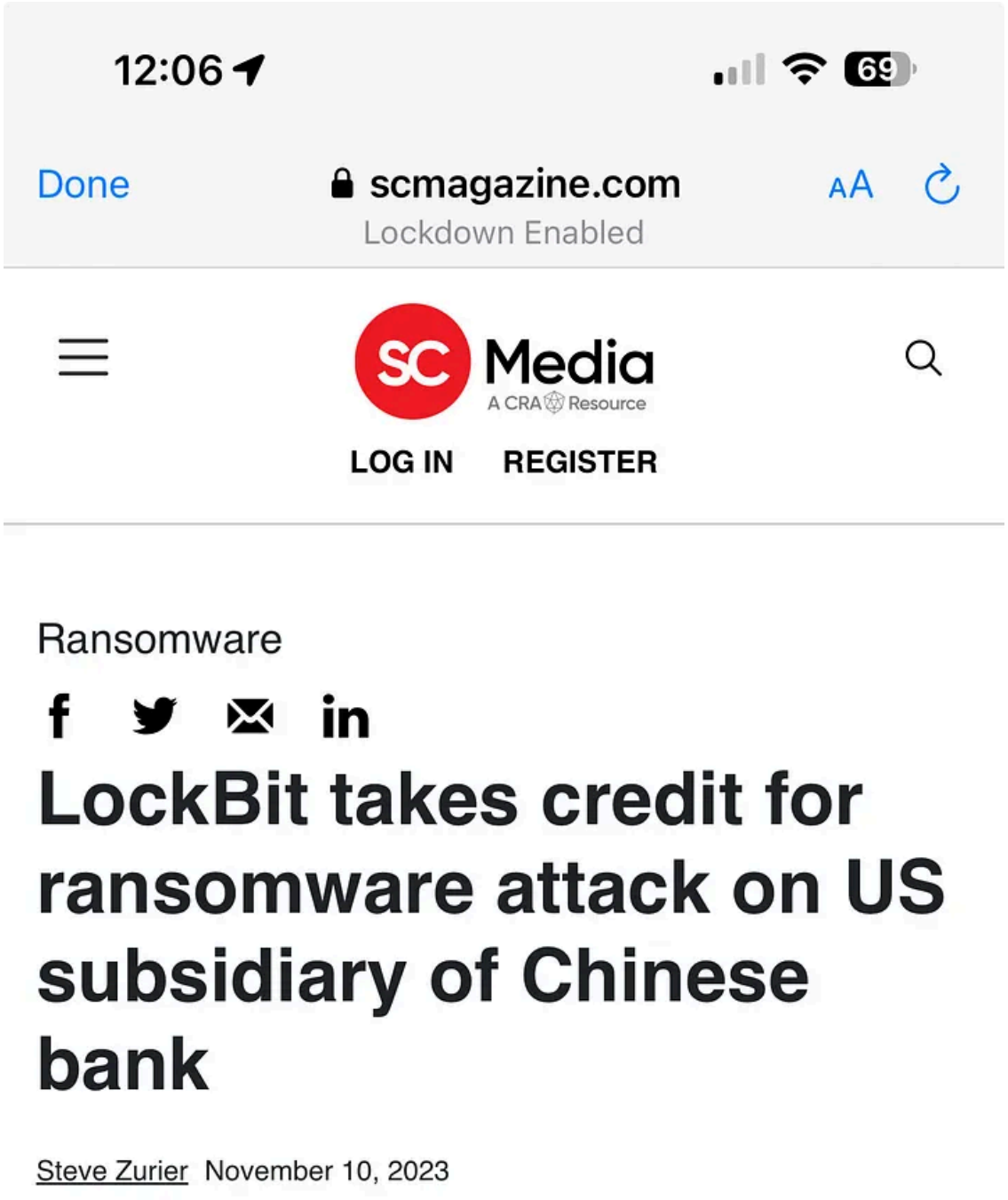
Press enter or click to view image in full size



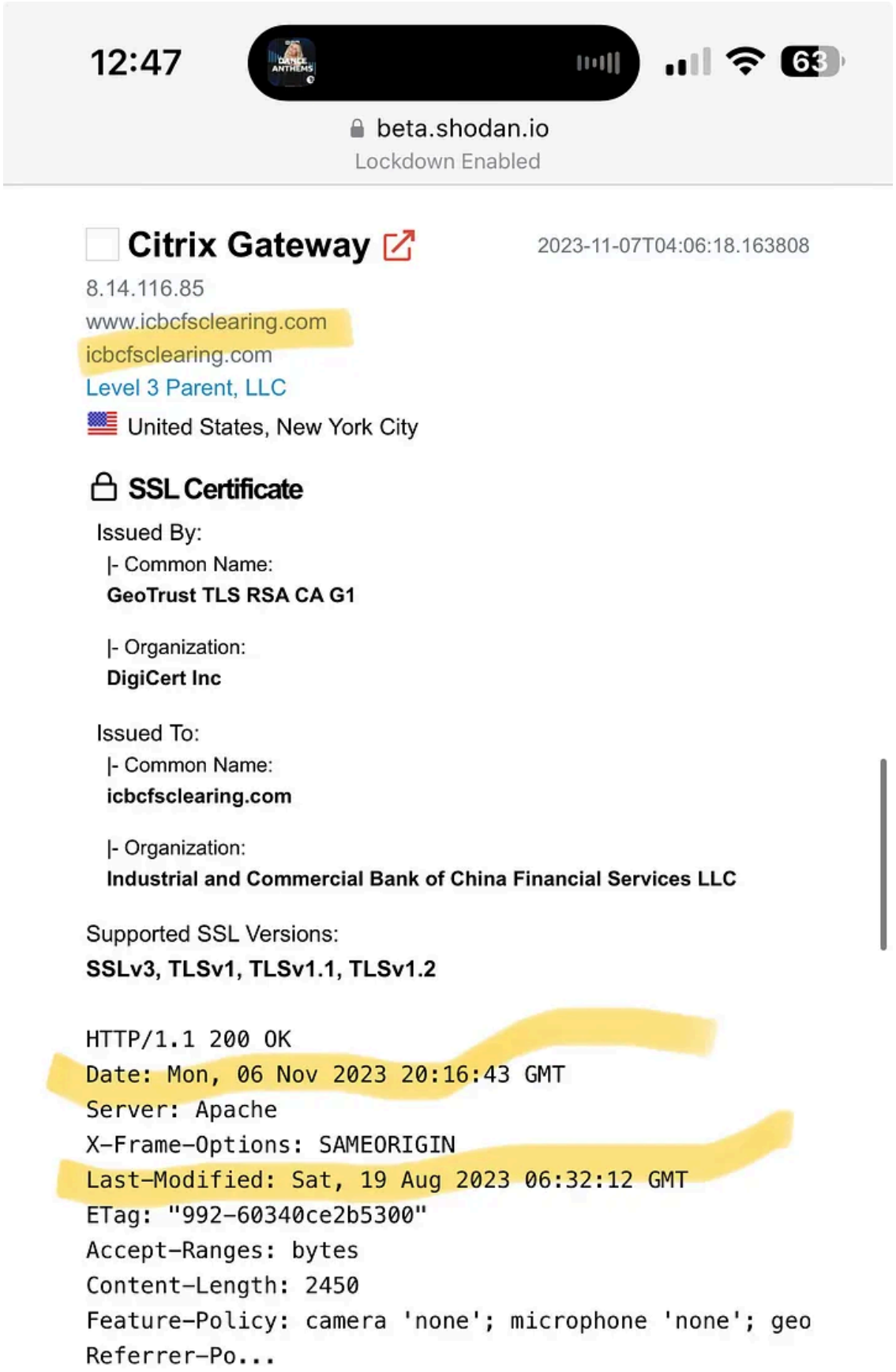
Shodan.io data

- Industrial and Commercial Bank of China (ICBC) Financial Services, the world's biggest bank — attackers entered via an unpatched for CitrixBleed vulnerability Citrix Netscaler on https://icbcfsclearing.com/ — this is still offline.

  Press enter or click to view image in full size



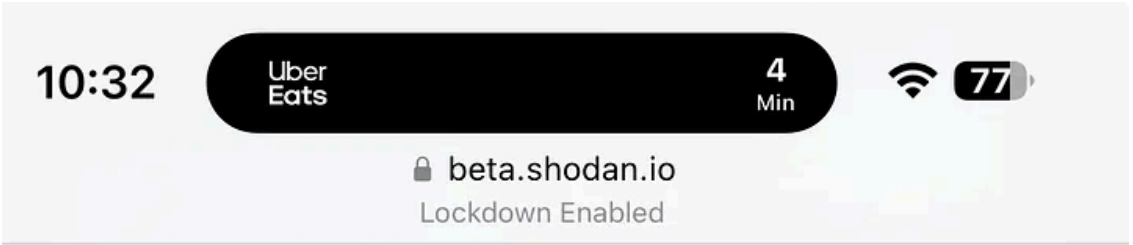
  Press enter or click to view image in full size



Shodan.io data

Other victims with unpatched Citrix Netscaler devices for CitrixBleed on Shodan include Boeing — one of the world's largest defence companies, and DP World — a large freight shipping company that Australia relies upon:

Press enter or click to view image in full size



Citrix Gateway

2023-11-06T12:20:23.114477

202.8.92.29
guestsdc.dpworld.com.au
DP World Australia Limited
Australia, Sydney

SSL Certificate

Issued By:
|- Common Name:
DigiCert TLS RSA SHA256 2020 CA1

|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
***.dpworld.com.au**

|- Organization:
DP World Australia Limited

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Age:          1
Date: Mon, 06 Nov 2023 12:20:22 GMT
Cache-Control: no-store,must-revalidate
Connection: Keep-Alive
Via: NS-CACHE-10.0:  58
ETag: "861-601474eb42ac0"
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 25 Jul 2023 03:27:15 GMT
Accept-Ranges: byt...
```

Most of the victims are not listed on LockBit's portal, which suggests they are negotiating payment or have already paid.

So what?

Ransomware groups are often staffed by almost all teenagers, and haven't been taken seriously for far too long as a threat. They are a threat to civil society as long as organisations keep paying.

Focusing on cybersecurity fundamentals for enterprise scale organisations is a challenge, as often people are chasing after the perceived next big thing — metaverse (remember that?), NFTs, generative AI — without being able to do the fundamentals well. Large scale enterprises need to be able to patch vulnerabilities like CitrixBleed quickly.

Press enter or click to view image in full size

LockBit operators hacking into your local government between CoD matches

The cybersecurity reality we live in now is teenagers are running around in organised crime gangs with digital bazooka's. They probably have a better asset inventory of your network than you, and they don't have to wait 4

weeks for 38 people to approve a change request for patching 1 thing.

Know your network boundary and risky products as well as LockBit do. You need to be able to identify and patch something like CitrixBleed within 24 hours — if you cannot, there is a very real possibility it isn't the ideal product fit for your organisation due to the level of risk it poses, and you need to rethink if the architecture of your house is fit for purpose.

Vendors like Citrix need to have clear statements of intent for securing *their* products, as piling on patch after patch after patch is not sustainable for many organisations — or customers should opt with their wallets for more proven solutions. The reality is many vendors are shipping appliance products with cybersecurity standards worse than when I started my career in the late 90s — while also advertising themselves as the experts. Marketing is a hell of a drug.

In the case of ICBC — the world's biggest bank — Reuters report the bank has paid the ransom:

This feeds into my earlier blog about ransomware:

By LockBit earning hundreds of millions of dollars, they are able to purchase new exploits, tools, resources and people to carry out attacks.

How are schools, libraries and small business — the life blood of the global economy — with usually small IT budgets and nobody responsible for cybersecurity — supposed to compete with teenagers who have bigger attack budgets than their entire IT budget for a year (or in many cases, a decade)?

Governments need to aggressively pursue ransomware, and stop payments. It is not a solved problem. Vendors need to make better secured products, or be forced into action by governments. We need to break this cycle, where civil society is suffering. Let's get to work.
