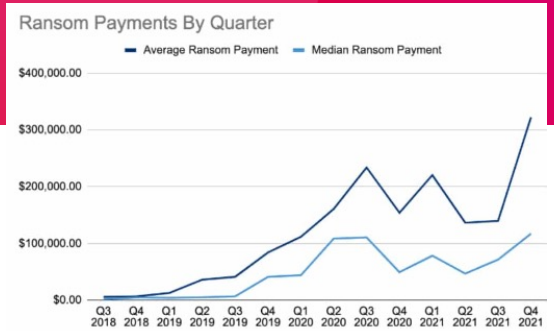
Presentation Headline Slide

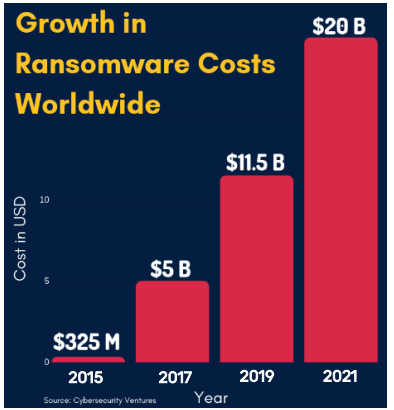
FUJITSU

Ransomware

Developments and remediation

Ransomware





Developments worldwide

- IT technology (dependency) increases
- Successful ransomware attacks increases
- Ransomware attacks become more sophisticated and faster

Ransomware and Financial Malware

(the everyday battle driven 86% by nation states)

Financial services saw a 35% increase in ransomware attacks in Q1 2022

Steve Zurier 9 June 2022

Okta ends Lapsus$ hack investigation, says breach lasted just 25 minutes

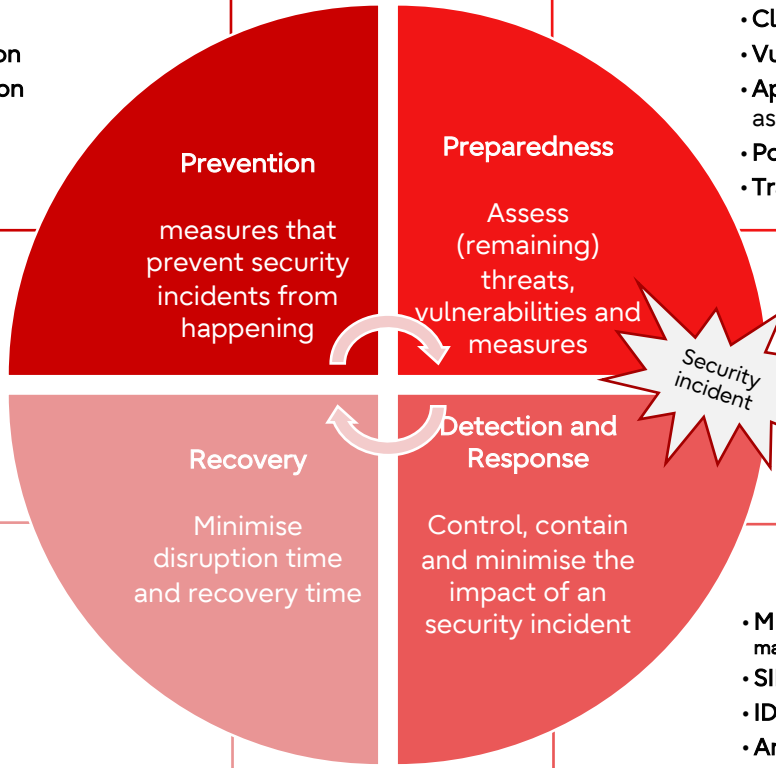
A forensic report concluded that the scope of access was far smaller than first thought, but customer trust may be hard to recover

By Corin Faife | @corintxt | Apr 20, 2022, 4:42pm EDT

THE VERGE

Strategies

- **Firewalls**
- **Network segmentation**
- **Multi Factor Authentication**
- **Laptop harddisk encryption**



- **Determine risk appetite**
- **Classification of data** (assets)
- **Vulnerability analysis**
- **Applying risk strategy** (on assets)
- **Policy, plans and procedures**
- **Training**

Is your strategy quick and effective enough, against modern ransomware threats?

- **Execute**
  -Business Conitinuity Plans
  -Disaster Recovery Plans
- **Restore from**
  -online backups
  -offline backups

- **MDR + EDR products** (anti-malware)
- **SIEM / SOAR**
- **IDS / IPS**
- **Anomaly detection**

Ransomware casus 2022

FUJITSU

Lapsus$, a few 16 year old teens, robbed Millions by bribing companies with ransomware and fast; 25 minutes from infection to encryption of the servers.

The young criminals run predefined automated scripts:

- send an email with attachment (spear phishing)
- The victim opens the document in email
- By using zero day exploits, access rights are obtained (undetected)
- Use “live-of-the-land-techniques” to access other machines
- Install the ransomware on all machines
- Encrypt the files on all machines
- Negotiate about ransom and/or publish sensitive information.

Weapons of choice

Family	Median Duration
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
Average of the median	**00:42:52**

Min. Sec.

Figure 4. Median ransomware speed measured across 10 ransomware families.

Victims with anti-malware in place: Nvidia, Microsoft Azure, Samsung, Okta, Brazil Gov, T-Mobile, Vodafone, UK Gov (among others)

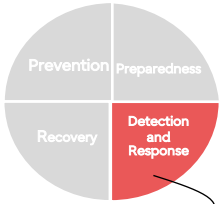
Endpoint protection effectiveness

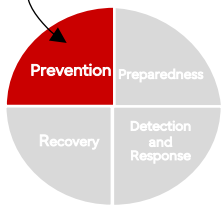
FUJITSU

Detection can take up hours to days

- Bad protection
- Limited protection
- Full protection
- Malicious office doc.
- Malicious executable
- Phishing email
- Infected USB (drive)

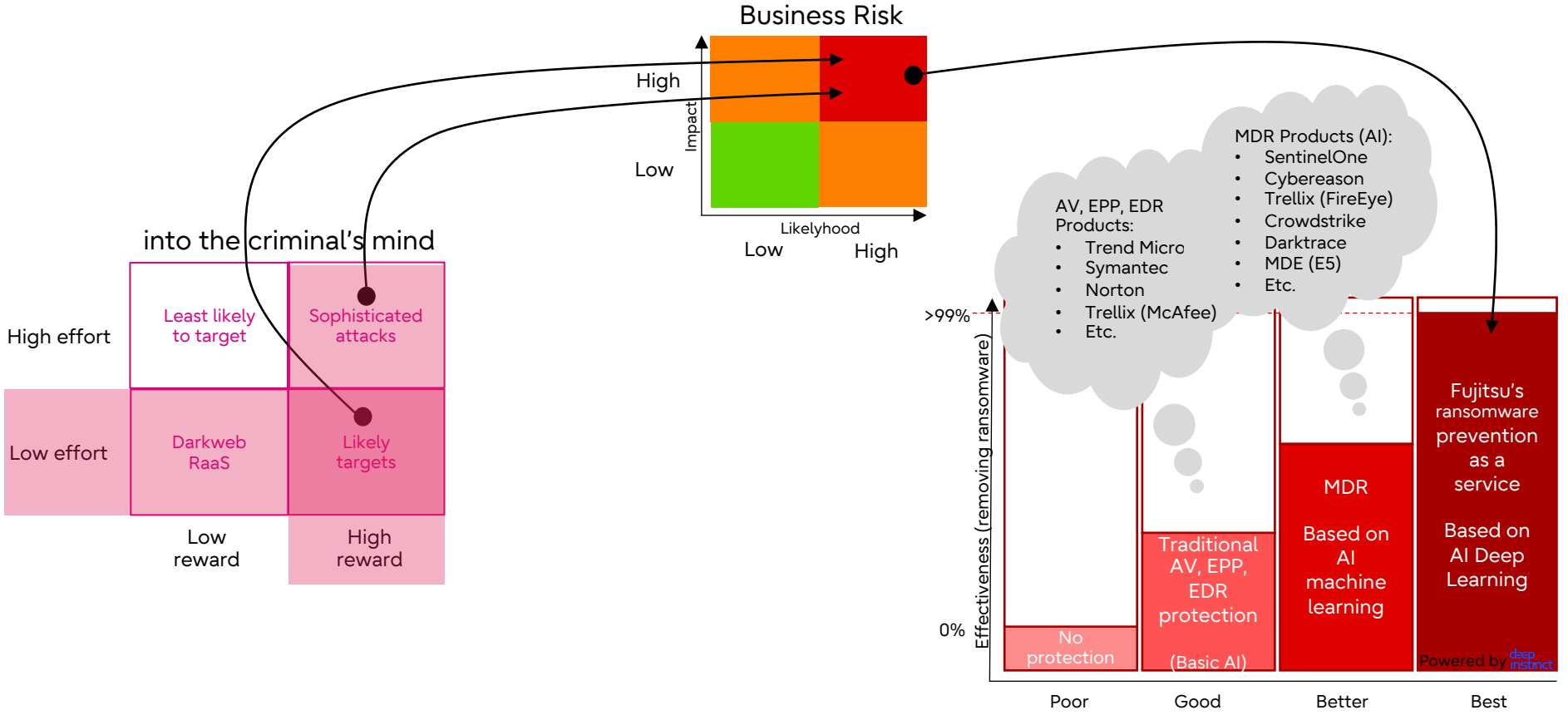
	Known Malware >30 days	Recent Malware 1<30 days	Unknown Malware 0-day	
Online connected to internet				Current MDR + EDR products
Offline				
Online connected to internet				Ransomware prevention as a Service
Offline				





Prevention in miliseconds

Ransomware risks



Take aways

Consider to uplift your ransomware protection:

- If you feel that you can become the next victim, due to:
  - vulnerable legacy systems
  - lots of vulnerabilities on the network
  - uncontrolled and unmanaged systems/ engineers on your network
  - criminals that are likely to target your company (because of your attractive assets)
- If you do not have sufficient protection place

Ask for a POC of "Ransomware Prevention as a Service" powered by deep instinct

- to compare with your existing protection and see for yourself
- to learn how this service integrates with your existing security
- when you are convinced that 'prevention' is always better than 'detection and response'

Thanks