

Understanding Cyber Risks

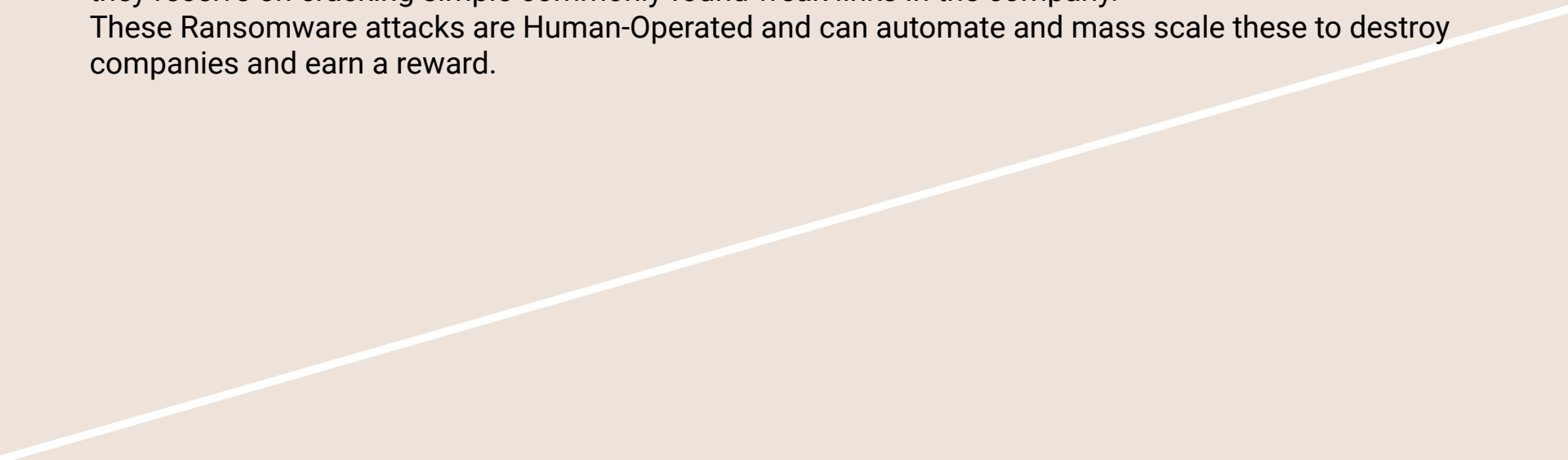
By Devarsh Parmar

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

Understanding the Environment

There is a rapid increase in the number of ransomware hackers. These increase due to the profit that they receive on cracking simple commonly found weak links in the company.

These Ransomware attacks are Human-Operated and can automate and mass scale these to destroy companies and earn a reward.



How do these attacks occur?

In most cases, initial access in human-operated ransomware attacks stems from the compromise of workstations with phishing emails or servers by exploiting unpatched vulnerabilities in internet-facing services.

Poor protection of privileged accounts allows attackers to compromise credentials.

The key issue that we are facing that is the backups stored at a service provider is not being constantly monitored. This gives the attackers ample time to penetrate the network and quickly do privilege-escalation. If we check after the network has been attack, there is no comebacks. So we need to report any issue as soon as it pops up. Thereby to achieve that we will need active monitoring on the backups.

Deter potential attackers with credible defensive capabilities

The ways by which attacks can be started and their solutions are:

1. Phishing Attacks: These attacks are generally sent on mail which contain a phishing link that can do wonders. Therefore, to prevent that we will need to educate our staff on this.
2. Liability on Detection Tools: There are a few detection services like Blood Hound and Cobalt Strike. No doubt they are great but they do can have some loopholes. Being a hacker, they will specifically target those.
3. Active Directory: Many privilege escalation attacks have been caused due to carelessness about the Active Directory. It is seen as an IT Tool and therefore in not configured by keeping security in mind.
4. Remote Logins can themselves have loopholes such as SSH configuration error and causes easy remote login into the network.

How should we
respond to
sustainably reduce
their organisation's
vulnerability to these
attacks:

There are three steps for the same:

1. Understand and report on their organisation's vulnerability to the threat.
2. Deliver targeted improvements to immediately reduce risk, and validate their implementation.
3. Build capabilities to deliver sustainable cyber risk reduction.

Areas of focus to reduce the risk of human-operated ransomware attacks

1. Prevent workstations being compromised by phishing attacks.
2. Remediate internet-facing vulnerabilities and reduce the attack surface.
3. Protect privileged accounts from being compromised.
4. Remediate common hygiene issues used by attackers to escalate privileges.
5. Restrict the ability of an attacker to compromise further systems.
6. Rapidly detect and contain incidents before they escalate.

Defeat the attack by sufficiently degrading, deflecting or destroying the attacking force's capabilities

To achieve this, we can do a few steps such as:

1. Disconnect few crown jewels, or important nodes, thereby reducing the surface of the attack.
2. To prevent an attack in the first place, we can have routinely checks across for any vulnerabilities.
3. Educating the staff from phishing, and enabling 2FA are also small steps to ensure a safe network.
4. Privilege Escalation, Active Directory and Brute Force attacks should also have their own set of measures.