AIRGAP

Top 5 Ransomware Trends in 2021

Ransomware attacks have been on a constant rise for a number of years now. The number of ransomware attacks skyrocketed in 2020 - an increase of about 715% in 2020, according to the Mid-Year Threat Landscape Report 2020. There's no reason to believe that this onslaught is going to stop anytime soon. Cybercriminals are coming up with more sophisticated and creative ways to penetrate corporate and home networks. Here we look at the top 5 ransomware trends in 2021.

Phishing - Human Factor

Around 67% of ransomware attacks involve phishing[1] and getting people to click on links sent via emails, download software, and a hundred other things that caused such attacks in the past as well. Despite money being invested in advanced security techs, the human element is far from extinction and remains to be one of the top trends in ransomware.

Cyber hygiene failures such as silly misconfigurations, lack of due diligence, people leaving things like their 7-digit default passwords exposed with weak user credentials are continuously failing security against ransomware attacks. Lack of cybersecurity training causes around 36% of total ransomware attacks[2].

On the technical front, the use of RDP remote desktop protocol and Powershell are helping hackers to find a way into your network without having to program sophisticated ransomware. Most ransomware that goes out is programmed for such defaults and basic errors.

The question here is,

How to protect against **human errors**?

As stated earlier, cybersecurity education and training are required. However, it only reduces the threat a little bit - Data suggests that around 4-7% of the workforce will still click on a link, come what may!

To ensure foolproof security against the human error trend in ransomware, a **zero-trust defense should be adopted** - move on the assumption that someone is going to click. Then security controls that are adequate enough to fill such human errors should be brought into place.

Data Breach Extortion & Cost of Ransomware Attacks

A large percentage of ransomware attacks move on monetary motives. According to reports, the total global cost of ransomware attacks has gone up from $11.5 billion in 2019 to $20 billion in 2020[3], and 2021 is expected to see more of the same trend. Ransom payments form a major chunk of such costs - about 10% of all ransom demands are over $5,000[4].

Attackers demand ransom for an organization's stolen or encrypted data. They also encrypt your backups should you think about resorting to them. Nowadays, if you face a ransomware attack, there are high chances that you'll be faced with a data breach extortion as well.

Should you **pay the ransom**?

Unfortunately, there is no correct answer to that! One absurd trend is that companies are starting to budget for ransomware!

There's a downside to both - paying the ransom and not paying it. If you say no, you'll be threatened with a public leak of all your sensitive data. You can also declare a data breach but the increased public attention might not be worth it.

On the flip side, if you choose to pay the ransom (and around 40% of ransomware victims do[5]), the attackers now know that you will pay and they'll come back time and again.

Also, the treasury blacklisted a couple of countries and organizations to which the hackers may belong so you'll be violating the treasury restrictions by paying one such organization of one such country.

Here is where cyber insurance comes into place. It is advised to never pay the ransom without a cyber insurance agent that has your back.

Ransomware on the Cloud

Excess reliance on the cloud has led to increased ransomware on it too. Earlier, the cloud was just a part of the infrastructure but today, the infrastructure is the cloud.

This trend is expected to prevail in 2021 as well given that clouds are weak and easy targets because of the same old misconfigurations and cyber hygiene failures as mentioned earlier. Lots of data is stored in clouds and with data comes malware opportunities. Reportedly, the average company has around 1,900 SaaS apps or equivalents.

The work-from-home scenario isn't helping either - with everyone and everything shifting to the cloud that wasn't already on it.

Cloud gives more efficacy but it encircles an entire organization unlike a couple of VLANs that may cover just a part of the entire network. This puts the entire organization at risk in case of a breach.

Stealth Methods for Ransomware Attacks

The world knows what happened with Solarwind. The attackers were able to insert malware into the code through a platform that was not there in the traditional RAL. The malware sat there for numerous days/weeks and was triggered at a later date. However, this seems to be the result of a more creative approach to ransomware instead of a new sophisticated variant

A stealth mode ransomware attack is going to become increasingly prevalent in the coming time.

One of the causes is poor supply chain security. The scary part is that even third parties' signed delivery of software contains malware. The autopatch updates, which were once considered a must, have become risky! This creates a dilemma between denying a patch update and approving it (with the risk of malware).

Such third-party products have become the perfect avenues to get the ransomware in and kickstart the whole process. The depth of connectivity of the targeted company can be another add-on issue. For example, if the organization that is compromised is connected to nuclear resources or other high-risk sectors, it puts more than just that organization in jeopardy.

What's the **solution?**

Supply Chain & Third-Party risk management strategy.

There is no way to test every product or chip by a third-party vendor. Hence, due diligence, awareness, and asking the right questions to your vendor become key to your security.

Look at the stability of the company you're dealing with (not 100% reliable because even companies such as Microsoft faced an issue). It's all about understanding and mitigating the risks by thoroughly gauging the vendor's security controls.

Establishing compensating controls such as monitoring functions to spot a false action due to malware can go a long way in minimizing threats by ransomware.

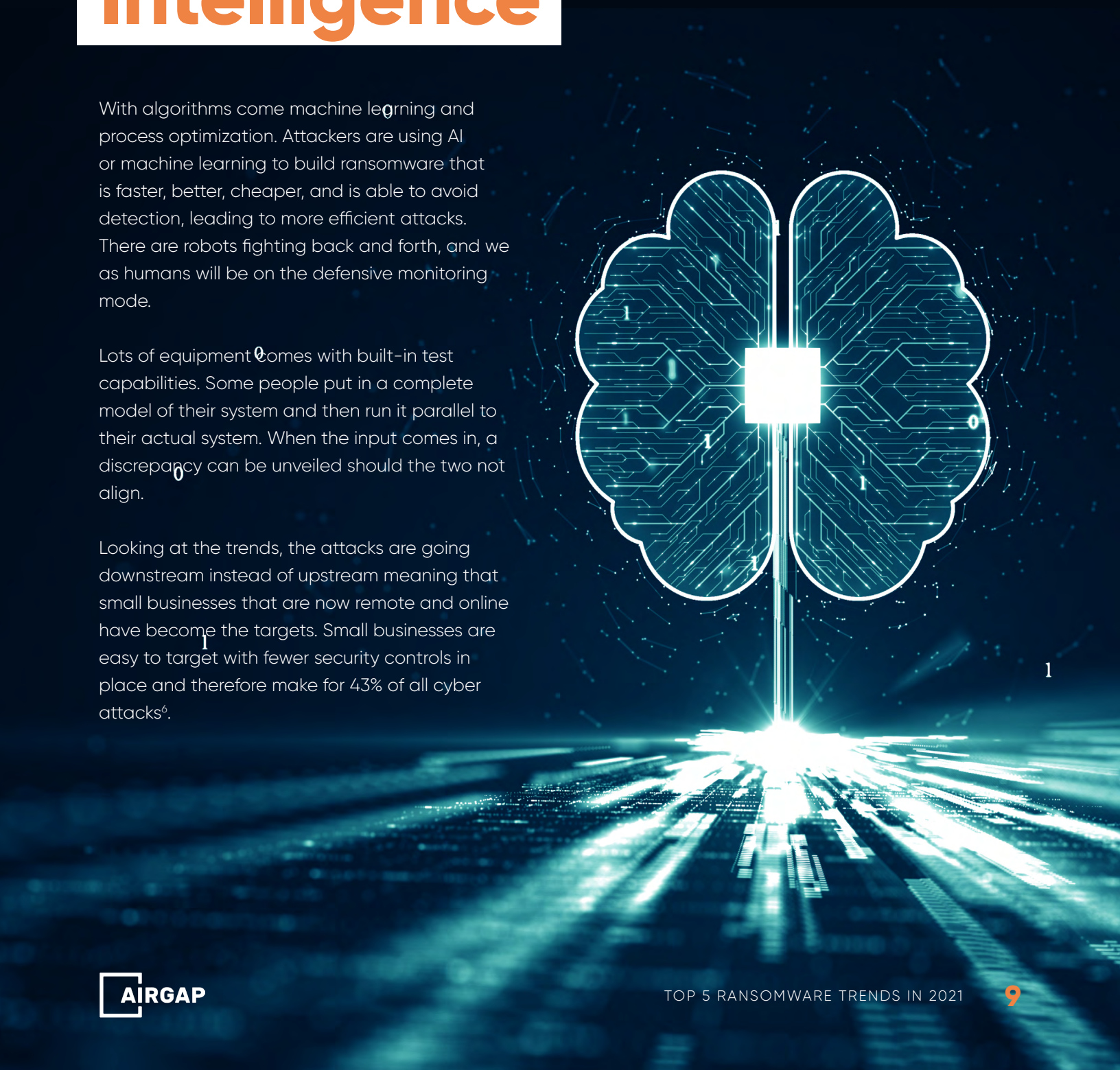
Need a secure and dependent security control for your organization? Let **Airgap** help you! Our **Zero-Trust Defence** and **Ransomware Kill Switch** will instantly put a halt to any unauthorized lateral propagation and ensure safety against a ransomware attack.

Artificial Intelligence

With algorithms come machine learning and process optimization. Attackers are using AI or machine learning to build ransomware that is faster, better, cheaper, and is able to avoid detection, leading to more efficient attacks. There are robots fighting back and forth, and we as humans will be on the defensive monitoring mode.

Lots of equipment comes with built-in test capabilities. Some people put in a complete model of their system and then run it parallel to their actual system. When the input comes in, a discrepancy can be unveiled should the two not align.

Looking at the trends, the attacks are going downstream instead of upstream meaning that small businesses that are now remote and online have become the targets. Small businesses are easy to target with fewer security controls in place and therefore make for 43% of all cyber attacks[6].



Final Thoughts

It can be inferred from the above-mentioned top 5 ransomware trends that the complexity and quantity of ransomware attacks are going to increase in 2021.

Following are the key takeaways:

- Ensure cyber hygiene and do the due diligence part.
- Don't think you're not a target. You are!
- You have the capability to evade an attack - it's more about strategy and tactics than about technology.

References to (1) to (6): https://purplesec.us/resources/cyber-security-statistics/ransomware/#:~:text=30%25%20of%20organizations%20who%20pay,ransomware%20victims%20paid%20the%20ransom.&text=A%20new%20organization%20will%20fall,sites%20are%20created%20every%20month.

Airgap's Zero Trust Isolation Platform protects your organization even if your perimeter is breached and even if you have vulnerable unpatched applications inside your organization. Airgap's patent pending "Ransomware Kill Switch" is industry's only solution that locks down the entire network with a single click. Airgap can be deployed in minutes without any agents, forklift upgrades, or design changes. The company is founded by highly experienced cybersecurity experts and the solution is trusted by large enterprises and service providers. For more details, check out https://airgap.io or contact info@airgap.io