1. **Read the article carefully.**

Ransomware groups to increase Zero-day-exploit-based access methods in the future.

Ransomware groups are expected to tweak **their** tactics, techniques and procedures (TTPs) and shift their business models as organizations strengthen their cybersecurity measures, law enforcement gets better at tracking down threat actors and governments tighten regulations on cryptocurrencies, according to Trend Micro's latest research paper.

In the report, published on 15 December and titled *The Near and Far Future of Ransomware Business Models*, Trend Micro highlighted 10 potential evolutions of ransomware groups' TTPs.

Those include increased use of zero-day vulnerabilities to get initial access to the targets' networks.

"Current ransomware teams explore options for access such as having separate teams to pen test entry vectors to potential victims' networks, purchase legitimate credentials from sellers in the underground, or use known exploits for vulnerabilities in any of the software being used by the target. One possible track is for these ransomware groups to allocate resources in developing **their** own vulnerability research and exploitation teams," the report reads.

"Moreover, considering the availability of these skills are scarce, another possible income source is when these groups also offer "first to refuse" agreements with known exploit developers: interested parties will pay to have a first look at the exploit and get the right to buy **them** first before the 'product' is offered to the developer's other clients."

Another possible evolution in ransomware attacks involves an increasing focus on targeting cloud infrastructure.

"We see these groups potentially diverting in two phases: first, criminals will adapt their current business models to work in cloud environments, treating instances as standard data to be encrypted. Second, they will gain maturity in understanding their targets and cloud environments and create more cloud-specific ransomware families designed specifically with unique cloud services in mind, creating new forms of ransomware attacks."

Aside from **these** tweaks, which Trend Micro called 'evolutions', the firm also analyzed deeper changes – or 'revolutions' – in how ransomware groups monetize their craft, with more threat actors either working for governments or crossing paths with traditional organized crime groups, sometimes at the same time, or shifting towards other criminal business models that monetize initial access, such as short and distort (stocks fraud), business email compromise (BEC), and cryptocurrency theft.

Abridged and adapted from https://www.infosecurity-magazine.com/news/ransomware-groups-increase-zeroday/

1. **Give definitions to these words (using your own words as far as possible).**

   a) Ransomware
   A type of malware whose purpose is to lock down the victim's files, encrypt them and demand payment (a ransom) to decrypt said files. Usually done with cryptocurrencies and by malicious threat actors looking to do the most damage.

   b) Zero-day
   Zero-day is a type of vulnerability that has not been found and/or researched by the developers of the software in question, hence the "0 Day" moniker.

   c) Vulnerability

   A vulnerability in the cybersecurity world is a weak point, in which an attacker could gain unwanted access, whether it be a system, a server or an application.

2. **To what words or expressions do the words highlighted in the text refer?**

   a) Their Ransomware groups' tactics
   b) Those Ransomware groups' TTPs (Techniques and Procedures)
   c) Their Ransomware groups' own vulnerability research
   d) Them Ransomware groups' "First to refuse" agreements
   e) These Ways in which ransomware groups develop and monetize their attacks

3. **Answer the following questions.**

   a) What are the motives behind the expected change in ransomware groups' tactics?
   Ransomware groups change tactics as "organizations strengthen their cybersecurity measures, law enforcement gets better at tracking down threat actors and governments tighten regulations on cryptocurrencies".

   b) How does the author believe they may start monetizing their attacks?
   Ransomware groups may start monetizing by "developing their own vulnerability research and exploitation
   teams"

c) Considering what you know about the subject, do you agree with the tone of the article? Are there any other changes you believe will happen?
The tone is stern, yet honest and straight to the point. In my personal opinion, that's the best way to go about these sorts of situations, as knowledge around this area of expertise can be scarce and should be concise and easy to read, as to allow maximum reach among experts and "noobies" alike.

d) What is the role of a cybersecurity technician in this constantly evolving atmosphere?

The role of a technician in this area is to gain knowledge and develop the tools and resources to fight againt these sorts of attacks, such as making sure that security measures are in place, systems are updated and backed up on a regular basis and having a good strategy in case these sorts of threats emerge.

4. ***Mirror, Mirror on the Firewall*… You are going to listen to some people talking about the trends for 2023 in Cybersecurity. According to the audio:**

a) What is the percentage of cybersecurity threats that can be avoided?
93%

b) What is the average time a company goes offline after a major data loss?
22 days

c) How much are the estimated revenue losses?
Between $10,000 and $5,000,000 per hour.

d) What will be the number one trend for 2023?
Secure Access Service Edge (SASE)

e) How much of your IT budget should be invested in cybersecurity policies?
10-15%

5. **Look at the following image!**

- **It displays several *hard skills* for a technician in the Cybersecurity field. Do you think all of them are necessary to be a good professional? What technical skills would you add?**
- **How about *soft skills* (character traits and interpersonal skills that characterize a person's relationships with other people)? What do you think are the most important ones?**
- **Write a +150-word comment, based on this image and the questions above, about what you expect your future professional life to be like and the role of this course in achieving it.**

The skills displayed in the image are more than essential to any expert or anyone working in the cybersecurity field. There are a few skills such as Cloud Security and Ethical Hacking that could be "skippable", but they are incredible skills to help think like an attacker, understand how they could perform certain attacks and mitigate the damage they can cause on a company's systems.

But just as hard skills are important, soft skills can be beneficial to these sorts of positions, especially regarding the psychological spectrum. Being able to blend in, talk to anyone and have an understanding of how an attacker's mind works are great skills to dominate in the field, whether it be physical or digital.

Enrolling in this course has allowed me to sharpen up on some older skills, develop new ones and make connections that can lead to good business partnerships in the professional world. Even skills deemed strange such as lock picking or learning how to use and abuse different operating systems, that I found to be uninteresting when I first started, have been a topic of great interest for me and my colleagues over these past couple months.