MINERVA

Never Pay Ransome.

WHAT MAKES RANSOMWARE SO DIFFERENT FROM OTHER MALWARE AND CYBER THREATS?

Cyber threats are nothing new. In the late 80s viruses like the ping pong virus would simply place an annoying ping pong ball on the screen which would tenaciously bounce around the screen with the relatively innocent intent of annoying whoever is trying to work on the computer.

Fast forward ~25 years, and cyber threats have not only advanced technologically and become more complex, but they have also become much more sinister in nature, trying not only to merely annoy and upset the victim, but to actually perform malicious actions, which have slowly turned into financially incentivized coordinated attacks with devastating results.

Threat actors are no longer just amateur pranksters trying to create little islands of mayhem, but have evolved into complex criminal organizations that behave like regular tech organizations with almost start-up like structures and behavior.

These are today's ransomware groups. Most of the larger and well-known groups today have clear business models and strategies which entail extorting millions of dollars from organizations which they manage to penetrate.

How does all this make ransomware behavior different from other malware?

Unlike other attack types, the commercial aspect of ransomware dictates different behavior. When a ransomware threat actor performs an attack on an organization, they don't just go in, encrypt one single computer and ask for ransom. They need to go through a few stages (a variation of the cyber kill chain). The short version of this is that after they manage to gain initial access to the network, they'll want to spread out and infect as much of the network as possible through something known as lateral movement.

For example:

- A threat actor manages to penetrate a single computer in an organization with a thousand computers and then proceeds to immediately encrypt it and then ask for a ransom.

  While this might mean one employee will most likely be having a bad day, the organization is not very likely to shell out a large sum of money to get that data back (or even to prevent the attacker from exposing that data to the world). They'll most likely accept the loss and just format the computer or just replace it.

- Now, what if that same ransomware actor were to gain initial access, and then slowly trickle through to additional computers in the network, penetrating, say 800 of the 1000 computers, and then one day detonate and encrypt all 800 computers at once. This would now be a very different story, and pretty much everyone in the company would be having a bad day. In this case, shelling out a few million dollars to get your files back doesn't look like such a far fetched outcome anymore does it?

This is what makes ransomware different and so much more dangerous than other malware.

Ransomware is a business

In order for to be able to get the best "revenue" from a victim, ransomware threat actors need to gain as much of a foothold as possible in their victim's network.

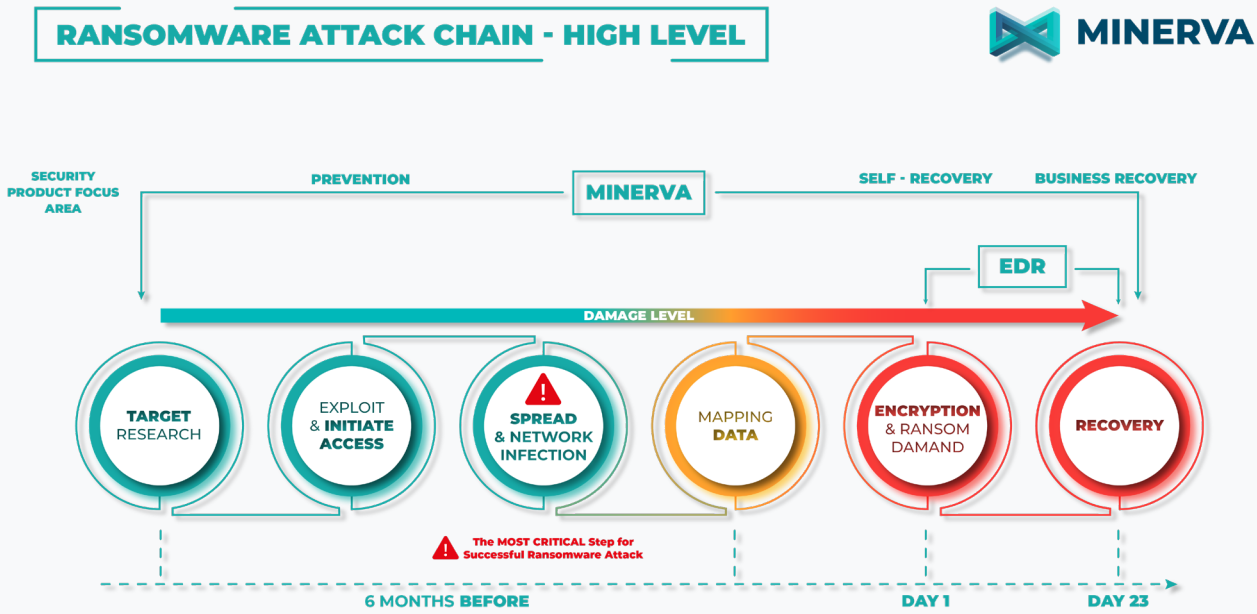
So, instead of just focusing on infecting a single computer, ransomware actors work on getting in and staying in as long as possible. In order to do this, they invest a lot of time and effort into making their ransomware as stealthy as possible in order to bypass security measures and remain undetected, allowing them to spread out through the network quietly without getting noticed.

In developing the ransomware with the security measures in mind, they implement many different techniques purpose build to bypass traditional security products and detect and response solutions. If they can't detect the ransomware, they can't stop it.

Encryption is the final step

The important part to understand is that the actual “ransom” part of the whole ransomware process, which includes exfiltrating and encrypting the victims’ files, and then demanding the ransomware, is the final stage of a long journey.

While this stage might appear to most people as “day 1”, and they’d say things along the lines of “we’ve just suffered a massive ransomware attack”, the reality is that their ransomware journey most likely started months months beforehand, but they are only now seeing it because the detonation stage is the most visible, and devastating stage.



The Ransomware Attack Chain

Once the ransomware has detonated, it will most likely then be discovered by the security solution. Its hash and behavior signature will then be added to the security solution database, making it easier to stop the next time.

This means we’re mainly talking here about unknown, or “zero day” ransomware attacks that are yet to be discovered and are therefore the most dangerous. Keep in mind that ransomware groups usually repack and change their ransomwares regularly, so even once a security solution has “detected” and added the signature to its database, the new version will have a different hash and therefore won’t be detected through the same means.

New methods require a new approach

With ransomware running rampart all over the world, it is clear that current solutions are not enough. While EDR/XDR/EPPs are all great at detecting and stopping traditional (known) threats that try to cause immediate harm without any real end-game, they are simply not able to keep up with a threat which has security solution evasion embedded so deeply within the core of its business model.

A completely different approach is needed on top of existing solutions to combat this historically malicious type of malware in order to keep organizations safe. One that is purpose built to manipulate the very core of what makes ransomware so effective, and turn its evasive properties against itself to not only stop the ransomware before it can spread inside the network and do any damage, but also protect the EDR/XDR/EPP agent itself from manipulation and disablement by the ransomware, and close the critical gap in the organization's security stack.

Minerva Anti-Ransomware bridges the gap

Minerva's ransomware prevention is the world's first pure dedicated ransomware prevention solution, which works alongside existing EDR/EPP/XDR solutions and actively prevents zero-day ransomware attacks without even needing to detect them first.

Contact us to learn how Minerva Labs can keep you safe from Ransomware