What are your thought on advanced malware and solutions out there to help stop them? You can comment on specific solutions that you researched for this week's deliverables, or choose different ones.

Advanced malware (usually refereed to Advanced Persistent Threats or APTs) are malware strains engineered with advanced capabilities for infection, communication and control, movement, or data exfiltration and payload execution (“What is an Advanced Persistent Threat? APT Definition | Digital ...”, n.d.). Advanced malware is commonly delivered in the malware introduction stage of an attack chain, and it can remain in the victim’s environment even after an attack or exfiltration of information is completed. Due to this need, they are usually built for long-lasting existence capability by avoiding detection by traditional antivirus or antimalware solutions.

Due to the significant rise of attacks that advanced malware caused on businesses, various security vendors have either came out with new security solutions or updated their existing ones to help encounter the risks these malware causes. However, most vendors have solutions that are tailored towards a specific type of assets and environments, which forces businesses to integrate various security solutions to have a more comprehensive visibility across their network and assets in order to protect themselves. Nevertheless, according to the research I conducted and my experience so far, Trend Micro’s Deep Security solution is more powerful in the identification, detection, and prevention of advanced threats caused by such malware. It is also unique because it is a hybrid solution (on-premise and cloud) for assets with antimalware, firewall, intrusion prevention, application control, web reputation, and log inspection security modules. It also has a virtual patching feature(to protect against zero-day exploit) that automatically gets applied to assets whenever a vulnerability is detected, but the manufacturer hasn’t provided a permanent patch yet. The pricing for this solution is also reasonable for all the protection it offers. Plus, organizations can choose the modules they want active in the environments to adjust the cost. Personally, I also used this tool even to remove a WannaCry ransomware on a virtual machine when doing a threat defense challenge.

That being said, it is still important to note that there isn’t one single solution that can protect business completely from current and emerging threats. That is, the human factor remains the number one security control to combat any breaches and damage that can occur. As a result, employee security awareness and technical knowledge for security professionals plays a critical role in stopping advanced malware.

References

What is an Advanced Persistent Threat? APT Definition | Digital . Retrieved March 23, 2020, from <https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition>

Trend Micro’s Solution Details: <https://www.trendmicro.com/en_us/business/products/hybrid-cloud/deep-security.html>