Virtual Machines targeted by a Sophisticated Ransomware

Negligence in an organization's cloud infrastructure as well as flaws in cloud networks can only add significant challenges to security teams managing virtual resources and services.

Modus Operandi

Scientists recently discovered a sophisticated ransomware, though at its early stage, using advanced techniques to compromise Windows virtual machines.

- RegretLocker sports features that allow it to encrypt virtual hard drives and close open files to encrypt them.
- To communicate with its victims, attackers prefer to send e-mail notes instead of a Tor payment site.
- Hackers' email address is apparently hosted on CTemplar, an Iceland-based anonymous email hosting service.

How it works

Normally, it is an uphill task to encrypt virtual hard disk files because of their enormous size as encryption takes time.

- The actors behind RegretLocker uses OpenVirtualDisk, AttachVirtualDisk, and GetVirtualDiskPhysicalPath functions to mount virtual disks for encryption, speeding up the process.

- The ransomware tampers with Windows Restart Manager API to terminate active programs or Windows services that keep files open.
- When encrypting files, it appends the. mouse extension to encrypted file names.

Recommendation

Virtual machine-related security issues occur because of the difference between security tools designed to protect hosted software and those safeguarding physical devices. Cyber Experts recommend to segregate and protect hosted elements inside a private subnetwork, allowing only tested and trusted virtual features and functions, and deploying separate infrastructure management and orchestration to protect the network.

References

https://www.scmagazine.com/home/security-news/ransomware/attackers-use-of-virtual-machine-to-hide-ransomware-is-a-first-say-researchers/

https://cyware.com/news/regretlocker-ransomware-meddles-with-your-virtual-machines-a5dbe043

https://security.stackexchange.com/questions/171649/is-a-vm-safe-to-run-a-simple-virus-on

https://superuser.com/questions/289054/is-my-host-machine-completely-isolated-from-a-virus-infected-virtual-machine