Babuk Locker Ransomware (CSB21-04)

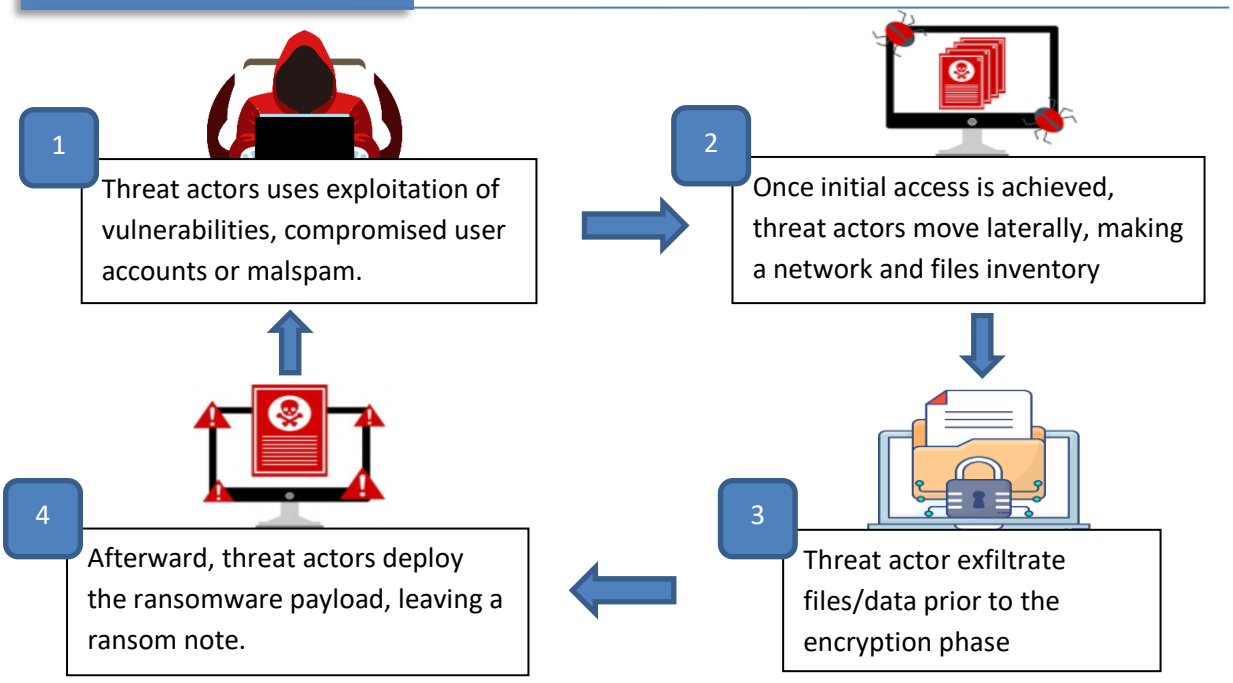
February 26, 2021

Babuk Locker Ransomware, also known as 'Babyk', is a new ransomware that was discovered early 2021. It is a ransomware threat to steal, encrypt and leak victim data in an attempt to extort payments. Since its discovery, Babuk Locker Ransomware has already impacted five big enterprises with double extortion ransomware attacks, demanding a ransom of $60,000 to $85,000 in Bitcoins from its victims.

Babuk Locker Ransomware website listed the organizations that are excluded from the group's scope of interest: such as hospitals (*except private plastic surgery clinics, and private dental clinics*), non-profit charitable foundations (*except the foundations who help LGBTQ and BLM*), schools (*except major universities*), and small business.

While not much is known about how the victims were initially compromised, similar ransomware campaigns have previously taken advantage of infrastructure vulnerabilities, such as exploits found in remote desktop protocol (RDP) and virtual private network (VPN) hosts, utilized stolen credentials, or malicious email (malspam) to gain initial access. Once the ransomware has been activated, it terminates Windows processes that prevent encryption before terminating a host of other programs on their victim's device, leaving a ransom note threatening to leak the stolen data if the ransom is not paid.

HOW IT WORKS



IMPACT

- Temporary or permanent loss of data.
- Potential harm to the organization's reputation.
- Interfere with the normal functioning of the computer system or prevent its utilization.

MITIGATIONS

- Do not pay the ransom.
- Remove infected computer within the network.
- Coordinate with IT Project Officer assigned in your office/unit.
- Perform a full system scan in safe mode to remove any infections.

PREVENTION

- Navigate directly to websites by typing the legitimate URL into the browser instead of clicking on links in messages/emails.
- Avoid auto-saving password, payment card numbers, or contact information.
- Use unique, complex passwords for all devices/accounts.
- Keep software up to date with the latest security patches and updates.
- Implement scheduled backups of data and conduct testing of backups regularly. Consider maintaining multiple backups in different locations for redundancy.
- Consider encrypting the data on your backup.
- Ignore all emails from unknown sender. Avoid opening or downloading files attached to spam emails.
- Do not use cracked or untrusted program
- Regularly run a complete scan to check the computer for present of malware.

REFERENCE

- https://www.cyber.nj.gov/alerts-advisories/ransomware-the-current-threat-landscape
- https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf
- https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html