Microsoft

Ransomware ve zdravotnictví v roce 2020 v době pandemie

Jan Pilař | Senior Program Manager @ Microsoft

- V samotných Spojených Státech, **764** poskytovatelů zdravotních služeb muselo dočasně zastavit provoz kvůli ransomware.

- **45 procent** veřejných institucí bylo zasaženo ransomwarem.

- **Každých 14 vteřin** se veřejná organizace (například zdravotnické zařízení…) stane cílem útoku ransomware

Ransomware Statistics, Trends and Facts for 2020 and Beyond (cloudwards.net)

- 83 % dotázaných zdravotnických organizací uvedlo, že za poslední rok zaznamenaly nárůst kybernetických útoků.

- Dvě třetiny (66 %) dotázaných zdravotnických organizací uvedly, že se kybernetické útoky staly za poslední rok složitějšími.

- 45 % dotázaných zdravotnických organizací uvedla, že se setkaly s útoky, jejichž hlavním cílem bylo právě zničení dat

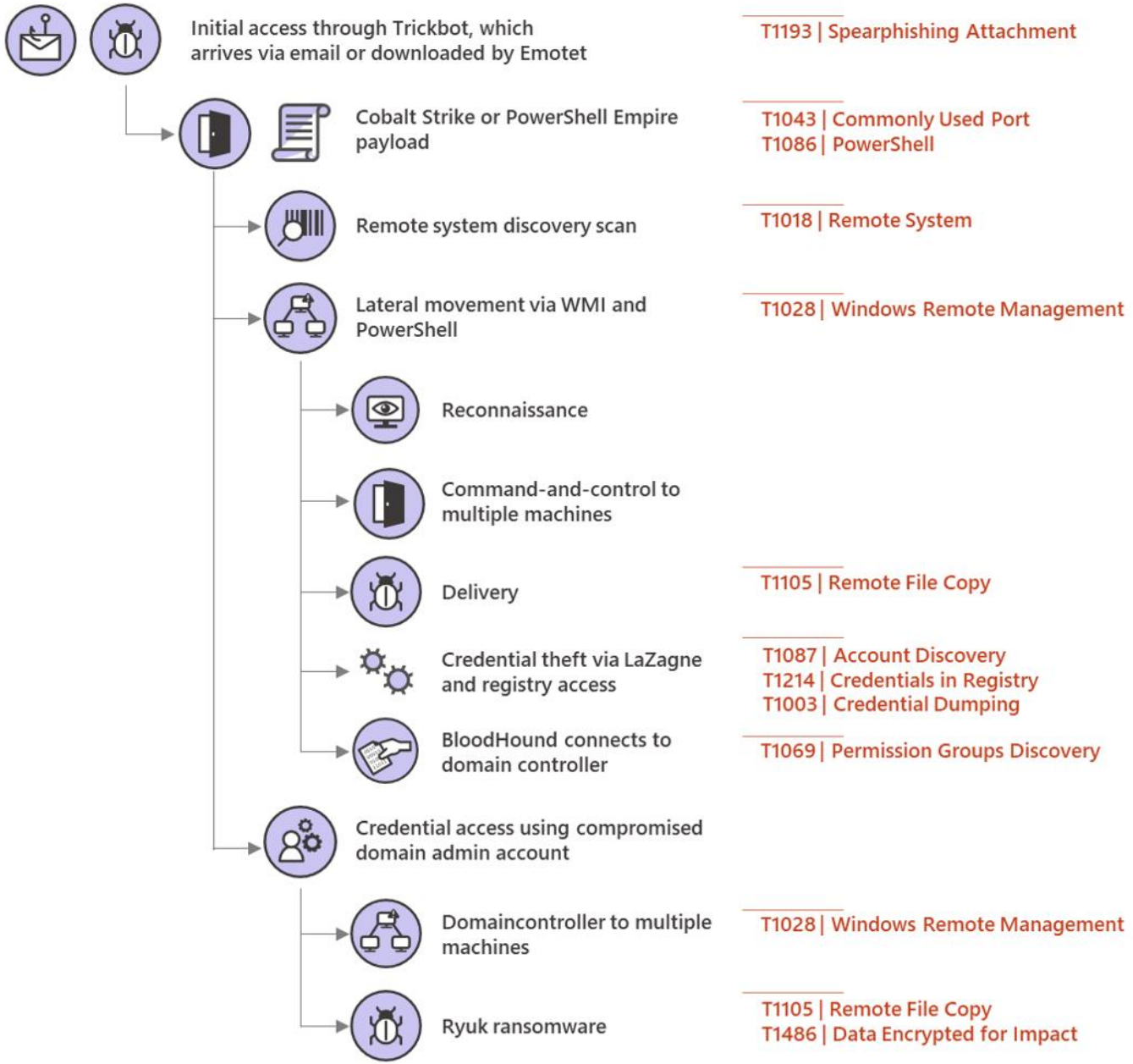
KYBEZ ZDRAVOTNICTVÍ | (egovernment.cz)

“Proč útočník používá ransomware?”

"...that the attackers behind the Revil (Sodinokibi) ransomware are actively scanning the internet for vulnerable systems.."

"In these attacks, adversaries typically persist on networks undetected, sometimes for months on end, and deploy the ransomware payload at a later time. This type of ransomware is more difficult to remediate because it can be challenging for defenders to go and extensively hunt to find where attackers have established persistence and identify email inboxes, credentials, endpoints, or applications that have been compromised."

Ryuk attack chain



Co s tím?

Human-operated ransomware attacks

Common attack techniques

Initial entry through misconfigured or outdated web servers
- RDP brute force

Deployment through commodity malware infection
- Initial entry through Trickbot or Dridex

Finding and exploiting poor security controls
- Thorough reconnaissance to discover and leverage security weaknesses
- Extensive knowledge of system and network misconfigurations

Credential theft and escalation of privilege
- Credential dumping through tools like Mimikatz, ProcDump, or LaZagne
- Privilege escalation through Sticky Keys attack
- Theft of financial credentials and LSA secrets in registry
- Data exfiltration through RDP
- Creating new accounts then granting remote desktop privileges

Human-operated lateral movement
- Network recon through scanning tools
- Manual spread though PsExec and GPO

Disabling of security controls
- Stopping security services
- Clearing event logs

Defenses

Secure internet-facing assets
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions
- Ensure collaboration among SecOps, SecAdmins, and IT admins to configure servers and other endpoints securely

Build credential hygiene
- Use MFA or NLA, and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege

Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event logs
- Analyze logon events

Harden infrastructure
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and AMSI for Office VBA

- Aplikujte všechny dostupné bezpečnostní aktualizace pro VPN a firewall konfigurace
- Důsledně monitorujte provoz a zvyšte obezřetnost u infrastruktury pro vzdálený přístup
- Jakékoliv detekce z bezpečnostních technologií nebo anomálie musí být vyšetřeny bezodkladně.
- V případě napadení se ujistěte, že jakémukoliv účtu použitému na daném zařízení byl proveden reset hesla. Přihlašovací údaje mohly být exfiltrovány.

- Zapněte ASR pravidla (HIPS technologie vašeho AV) pro blokování “credential theft” a “ransomware activity”.
- Zapněte “AMSI for Office VBA” pokud používáte Microsoft 365 Apps.
- Používejte TVM nástroje
- Používejte EDR / XDR technologie (offsite)
- Naučte se vyšetřovat útok a hunting
- Vícevrstvá úroveň zabezpečení proti škodlivému kódu (pozor na legitimní nástroje)
- Zero Trust – Assume Breach, Least Priviledge, Verify explicitly

Zdroje

- Human-operated ransomware attacks: A preventable disaster - Microsoft Security
- Cyberattacks targeting health care must stop - Microsoft On the Issues
- Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here's what to do - Microsoft Security
- Office VBA + AMSI: Parting the veil on malicious macros - Microsoft Security
- Ransomware Statistics, Trends and Facts for 2020 and Beyond (cloudwards.net)
- https://download.microsoft.com/download/7/5/1/751682ca-5aae-405b-afa0-e4832138e436/RansomwareRecommendations.pptx