K logix

BE CONFIDENT.

VOL 3 | JANUARY 2023 | THREAT INTEL NEWSLETTER

Cuba Ransomware and LockBit Ransomware

C-Suite level threat review by applicable business area addressing active threats.

Ransomware is a form of malware that encrypts data, rendering that data unusable to an organization until it pays the ransom. Ransomware attacks are costly and increasing in frequency. IBM found in its Cost of a Data Breach Report 2022 that the average cost of a ransomware attack in 2022 is $4.54 million USD, excluding the cost of the ransom itself. The report also found that the frequency of ransomware breaches has increased from 7.8% in 2021 to 11% in 2022.

Cuba Ransomware:

Cuba ransomware actors have been operative for a few years now, targeting critical infrastructure. Despite the name, there is no indication that Cuba ransomware is connected to the Republic of Cuba. The actors encrypt and exfiltrate data, compelling victims to pay the ransom to prevent the public release of that data. This is known as the double extortion technique.

LockBit Ransomware:

LockBit 3.0 is the newest edition of LockBit ransomware and has several improvements over its predecessor, some of which suggest an integration of capabilities with the now-deprecated ransomware BlackMatter. LockBit 3.0 employs triple-extortion, which targets the initial victim with the double-extortion technique and third parties who could be impacted by the data disclosure.

Cuba Ransomware

Threat Level: Medium

Attack:

To gain initial access, Cuba ransomware actors have conducted phishing campaigns and utilized known commercial software vulnerabilities. Palo Alto and Trend Micro recently observed Cuba ransomware actors operating with updated techniques. To evade detection, the ransomware actors have been observed terminating AV-related processes via a KillAV tool and leveraging a dropper called APCHelper.sys that targets and terminates security products (MITRE T1562). The actors have also utilized a technique called Kerberoasting to steal Kerberos tickets (MITRE T1558.003).

Remediation:

- Update operating systems, software and firmware with the latest patches and releases (cyber hygiene)
- Use an Endpoint Detection and Response (EDR) tool
- Enable multi-factor authentication (MFA) and contextual authentication via an Identity-as-a-Service (IDaaS) tool
- Audit user accounts with admin privileges
- Have just-in-time access for privileged accounts via a privilege access management (PAM) tool

LockBit Ransomware

Threat Level: High

Attack:

LockBit usually gains access through compromised servers, targeting Windows and Linux systems. LockBit 3.0 has worm-like capabilities giving it the ability to self-propagate within an organization. LockBit 3.0 improves upon LockBit 2.0 with increased anti-analysis techniques, such as debugger evasion (MITRE T1622) and the use of undocumented kernel-level Windows functions.

Remediation:

- Establish network segmentation
- Implement a Security Awareness and Training program, where employees are regularly training on pertinent threats
- Regularly scan for vulnerabilities
- Conduct penetration tests

Cuba Ransomware Details

- **Details on the MITRE techniques used:** https://attack.mitre.org/software/S0625/
- **Cybersecurity advisory by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA):** https://www.cisa.gov/uscert/ncas/alerts/aa22-335a

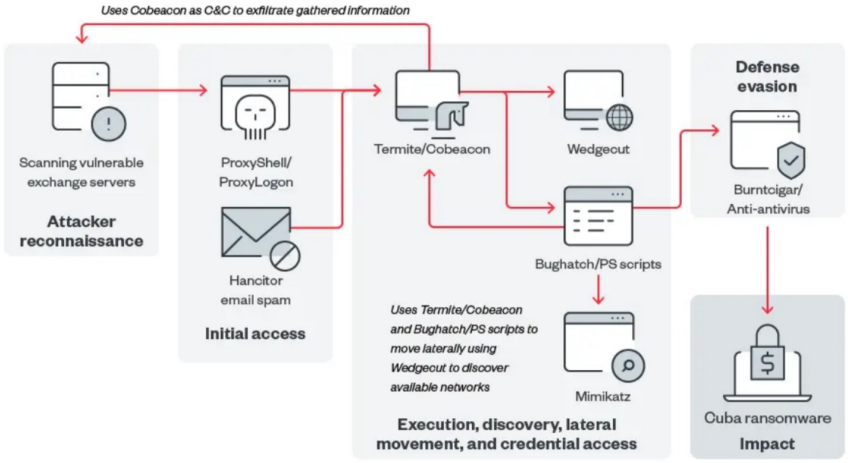
LockBit Details

- **Details on the similarities to BlackMatter ransomware:** https://news.sophos.com/en-us/2022/11/30/lockbit-3-0-black-attacks-and-leaks-reveal-wormable-capabilities-and-tooling/
- **Department of Health and Human Services Office of Information Security Report on LockBit 3.0 Ransomware:** https://www.hhs.gov/sites/default/files/lockbit-3-analyst-note.pdf

How K logix Can Help

- Technology Advisory
  - Endpoint Detection and Protection
  - Identity and Access Management
  - Threat Management/Intelligence
  - File Integrity Monitoring
- Programmatic Advisory
  - Identity and Access Management
  - Threat Intelligence Program Maturity
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI)
  - Penetration testing

Cuba Ransomware Infection Chain



Source for graph: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-cuba