Sponsor SEC Consult: Resilience Rising: Countering the Threat Actors Behind Black Basta Ransomware

Published: 2023-11-15 · Archived: 2026-04-05 13:47:52 UTC

Resilience Rising: Countering the Threat Actors Behind Black Basta Ransomware By Angelo Violetti Senior Digital Forensics & Incident Response Consultant, SEC Consult (Schweiz) visit https://2023.swisscyberstorm.com/sche... & https://www.swisscyberstorm.com for more information The following summary was machine generated from the YouTube transcript and then reviewed by human eyes. If you spot any errors, please comment below. Summary Presenter: Angelo Violetti Title: Resilience Rising: Countering the Threat Actors Behind Black Basta Ransomware Category: SCS2023 Subcategory: Sponsor Video: • Sponsor SEC Consult: Resilience Rising: Co... Length: 33:14 Content: Angelo Violetti discusses the Black Basta ransomware group, focusing on their tactics, the human factors behind these attacks, and strategies for countering them. Key topics include ransomware as a service, the structure of attack groups, specific ransomware tactics, and recommendations for improving organizational resilience against such threats. Keywords:

- Ransomware
- Black Basta
- Threat Actors
- Cyber Security
- Human Factors

Ideas

- Ransomware groups are structured similarly to businesses, with various roles including initial access brokers, ransomware operators, affiliates, and money launderers.
- Ransomware attacks are highly profitable, so preventing financial gain by not paying ransoms is crucial.
- Understanding and countering the playbooks and tactics used by ransomware groups can significantly reduce the effectiveness of their attacks.
- Effective defenses involve minimizing misconfigurations and vulnerabilities, which ransomware actors exploit to gain quicker access and achieve their goals.
- Deception techniques, such as fake accounts and decoy files, can help in detecting and responding to attacks if the organization is prepared with proper logging and alerting mechanisms.

Quotes

- "Paying ransom means funding criminal actions because otherwise, if you do not pay, there is no financial gain for them."
- "In order to perform a successful attack, they have got playbooks that define every step an affiliate should take."
- "If you are able to detect the techniques used by this tool, you can cover pretty much all the ransomware groups that are out there."

- "Quack bot was their main malware used for gaining access into an infrastructure."
- "Strong password policies and least privilege principles are crucial to preventing credential compromise."

Facts

- Black Basta ransomware was first discovered in April 2022 and has rapidly gained notoriety due to its high number of victims.
- The group’s attack phases include initial access via brokers, deployment of malware, enumeration of infrastructure, and data exfiltration before encryption.
- Black Basta employs tools like Cobalt Strike and system BC to evade security measures and establish persistence.
- The FBI disrupted the Quack bot infrastructure in August 2023, impacting Black Basta’s operations and shifting their malware tactics.
- Strong password policies and using least privilege for service accounts are essential in preventing domain admin privilege escalation and compromising attacks.

Resources

- Quack Bot: Tool used by Black Basta for gaining initial access.
- Cobalt Strike: A common post-exploitation framework used by attackers for persistence and evasion.
- System BC: Malware used by Black Basta to facilitate communication and data exfiltration.

Recommendations

- Implement strong password policies and enforce the principle of least privilege for service accounts to reduce the risk of credential compromise.
- Use native Windows functionalities, such as restricted PowerShell usage and Windows Firewall, to minimize attack surfaces and block malicious activities.
- Regularly assess and update your security measures, including deploying EDRs, performing periodic assessments, and engaging in purple teaming exercises to improve detection and response capabilities.

Source: https://www.youtube.com/watch?v=iD_KZAqNDZ0