US Coast Guard Cyber Command
Maritime Cyber Alert 02-23

June 15, 2023

Information Sharing Protocol: TLP: CLEAR (https://www.us-cert.gov/tlp)

BlackBasta Ransomware Group

Summary:

Coast Guard Cyber Command (CGCYBER) recently observed a surge in BlackBasta Group ransomware campaigns targeting the Marine Transportation System (MTS). These campaigns include, but are not limited to, the publicized attack in May 2023 impacting ABB Ltd., a leading automation technology provider known in the MTS for its role supporting critical infrastructure sectors including maintenance services offered for ship-to-shore cranes.[1] This incident, along with several less publicized incidents, provide a reminder for organizations to be cognizant of the connections their systems have with third-party providers. Dependence on third-party providers calls for organizations to ensure they maintain access control of their networks and to ensure contingencies are in place.

The Ransomware as-a-Service (RaaS) group known as BlackBasta is a financially motivated criminal organization specializing in double extortion tactics, exfiltrating and encrypting data to profit from its victims.[2] The group's modus operandi involves deploying ransomware on victim networks to encrypt critical files and exfiltrate sensitive data, which it then threatens to release publicly as part of the "name and shame" tactic if the impacted entity refuses to pay the ransom. The Maritime Cyber Readiness Branch has seen an influx of reports involving BlackBasta since September 2022.

BlackBasta in the MTS:

BlackBasta first became known in April 2022 and is believed to be a rebrand of the previously established groups Herms, Ryuk, and Conti. Organizations of various sizes and industries, including energy, manufacturing, transportation, and government, have reported incidents of malicious activity attributed to BlackBasta, demonstrating the group's broad impact.

---

[1] Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com)
[2] Double extortion- (one) encrypt sensitive data to restrict access unless ransom is paid and (two) exfiltrate sensitive data and threaten to publish or sell it on the dark web unless the ransom is paid.

In CGCYBER's assessment of recently investigated incidents, phishing is the most common initial access vector. Phishing incidents often begin by targeting either third-party service providers or other trusted business partners. After successfully infiltrating these partners, BlackBasta threat actors craft convincing phishing emails with embedded malicious attachments and send them to the intended victim using a compromised email. This technique, known as Business Email Compromise (BEC), allows the threat actors to send malicious phishing emails from a legitimate source, thereby evading detection by security monitoring tools. Once opened, the malware embedded in these attachments typically provide the attackers initial access to the network. On some occasions, the malicious emails are used to steal credentials from the target organization. In at least one case, the malicious actors were able to trick an employee to submit credentials and acknowledge a Multi-Factor Authentication (MFA) prompt, thereby granting them full access to their account.

Mitigation Measures:

Prepare

- **Maintain Offline Back-Ups:** Maintain offline, encrypted data backups and regularly test them. Backup procedures should be conducted on a regular basis. It is important to maintain backups offline because many ransomware variants attempt to find and delete any accessible backups.

- **Maintain "Gold Images":** Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.

- **Exercise Incident Response Plan:** Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.

- **Understand Cyber Hygiene of Third-Party and Managed Service Providers:** Understand the cyber hygiene practices of third-parties or managed service providers (MSPs) your organization uses, especially for your most critical systems. As stated previously, BlackBasta has been known to exploit third-party vendors and BEC as an attack vector against target organizations.

Defend

- **Phishing-** Most common initial access vector utilized by BlackBasta

    - Implement a **cybersecurity user awareness and training program** that includes organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.

    - Implement **filters at the email gateway** to filter out emails with known malicious indicators, such as known malicious subject lines, and suspicious Internet Protocol (IP) addresses at the firewall.

    - Implement **Domain-based Message Authentication, Reporting and Conformance (DMARC)** to help ensure all emails that appear legit pass the Sender Policy Framework/Domain Keys Identified Mail (SPF/DKIM)

checks to confirm origin. DMARC is designed to fit into an organization's existing inbound email authentication process and protect against direct domain spoofing. It includes a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.

- **Precursor Malware-** Malware is often deployed as part of phishing campaigns to gain access to the target network.
    - Ensure antivirus and anti-malware software and signatures are up to date.
    - Use application directory allowlisting to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
    - Implement intrusion detection system to detect suspicious activity such as command and control actions.

If your organization has any questions related to this alert, please contact the U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.

Appendix A: Indicators of Compromise

Indicators of Compromise

Type	Indicator	Description
IPv4 Address	99.253.251.74	IP address using TTPs similar to BlackBasta.
IPv4 Address	99.232.140.205	IP address using TTPs similar to BlackBasta.
IPv4 Address	98.180.234.228	IP address using TTPs similar to BlackBasta.
IPv4 Address	95.136.41.50	IP address using TTPs similar to BlackBasta.
IPv4 Address	94.99.110.157	IP address using TTPs similar to BlackBasta.
IPv4 Address	91.116.160.252	IP address using TTPs similar to BlackBasta.
IPv4 Address	89.211.223.138	IP address using TTPs similar to BlackBasta.
IPv4 Address	89.211.217.38	IP address using TTPs similar to BlackBasta.
IPv4 Address	88.251.38.53	IP address using TTPs similar to BlackBasta.
IPv4 Address	88.246.170.2	IP address using TTPs similar to BlackBasta.
IPv4 Address	88.245.168.200	IP address using TTPs similar to BlackBasta.
IPv4 Address	88.242.228.16	IP address using TTPs similar to BlackBasta.
IPv4 Address	88.232.207.24	IP address using TTPs similar to BlackBasta.
IPv4 Address	88.232.207.24	IP address using TTPs similar to BlackBasta.
IPv4 Address	88.231.221.198	IP address using TTPs similar to BlackBasta.
IPv4 Address	87.75.195.211	IP address using TTPs similar to BlackBasta.
IPv4 Address	87.243.113.104	IP address using TTPs similar to BlackBasta.
Domain	Zedorocop[.]com	Malicious domain associated with BlackBasta.
Domain	Gerhiles[.]com	Malicious domain associated with BlackBasta.
Domain	Danimos[.]com	Malicious domain associated with BlackBasta.