UTAH VALLEY UNIVERSITY W0LV3R1NES:
MARK DRIGGS, ALEC HEITZMANN, ANDREW JENSEN, HUNTER KARR

23 MARCH 2021

Situation Summary:

On 23 March 2021, the W0LV3R1NES Cybersecurity Task Force (WCTF) received notice of a cyberattack composed of both a ransomware and malware that targets global shipping software. The ransomware, codenamed BASKERVILLE, and the malware, codenamed CHIMERA, have been described as follows:

- BASKERVILLE: Ransomware that affects email software, access control, and cargo manifests at shipping ports.
- CHIMERA: Malware that allows actors to edit bills of lading and container tags at shipping ports.

The WCTF has a high level of confidence, based on HUMINT and SIGINT reporting, that BASKERVILLE has been deployed at several ports in the United States and abroad and works tangentially with CHIMERA, allowing actors to camouflage data manipulation in TidalWaves, a port management system used by government agencies and private industry. The WCTF has a moderate level of confidence, based on reliable HUMINT, that the aim of the cyber-attackers is to disrupt global trade; however, escalation of the cyber incident is possible. Any escalation could severely impact U.S. economic interests domestically and abroad.

Key Takeaways & Analysis:

- On 8 March 2021, the Port of Houston reported irregularities in their shipping and distribution, ranging from oil refinery equipment to perishable goods.
- On 17 March 2021, the NSA reported that operatives from 1881 COLECTIV, a Romanian organized cyber-criminal group, met in a chatroom with members of MANTICORE, a suspected Iranian-sponsored APT, about a new type of malware that would allow cyber-actors to edit shipping data. The MANTICORE actor instructed that the 1881 COLECTIV member install a ransomware on key port systems to camouflage the data manipulation.
- On 19 March 2021, the Rabinara Group, a private maritime cyber-monitoring service, disclosed that the Port of Houston and Port of Corpus Christi in the United States, and the Port of Harcourt in Nigeria, had reported an ongoing ransomware attack, which the WCTF is confident, based on SIGINT and private sector intel, is the deployment of the BASKERVILLE ransomware. Rabinara Group and industry partners reported similar incidents in 4 ports in South America, Europe, Asia, and Australia. BASKERVILLE has been confirmed to affect whole port operations systems, specifically, email services and access management software. More critically, BASKERVILLE has compromised the cargo manifest systems in the identified ports, including digital backups.
- On 23 March 2021, MANTICORE launched CHIMERA as a supply-chain attack against the TidalWaves port management system. The WCTF is confident, based on SIGINT and HUMINT, that BASKERVILLE has been deployed to cover the tracks of CHIMERA. Earlier, on 23 October 2020, the CIA reported that MANTICORE members, communicating on a video game chat, confirmed that their new malware, codenamed CHIMERA, had infected the BitHub repository of TidalWaves. The CIA report detailed that MANTICORE designed CHIMERA to edit shipping data in the TidalWaves network, which operates across multiple technological service platforms and ports operations systems globally. The CIA report further detailed that the MANTICORE group has also infiltrated the cybersecurity protections of “PoH,” which likely refers to either the Port of Houston or the Port of Harcourt.

We assess that it is possible that MANTICORE used this infiltration to directly edit shipping data in the Port of Houston, paving the way for 1881 COLECTIV to deploy BASKERVILLE. However, it is also likely that the infiltration of the Port of Houston is more substantial than the initial malware or ransomware attack, which the WCTF believes could point to an escalation of hostilities, hereby referenced as POSSIBLE CYBER INCIDENT (PCI). We assess that the CHIMERA cyberattacks, based on SIGINT and HUMINT, are actively allowing cyber-actors to manipulate shipping manifests and possibly divert shipped contents to currently unknown locations. Based on combined available intelligence, the indication is that the BASKERVILLE cyberattack is covering the tracks of the CHIMERA cyberattack by collecting cargo manifests and digital backups. The BASKERVILLE, CHIMERA, and PCI attacks point to a combined cybercriminal and state-sponsored APT syndicate bent on disrupting U.S. and global trade.

Response Goals:

The WCTF recommends that policies approved by the NSC follow a framework that includes several primary goals:

- Determine immediate mitigation plan for both Texas ports.
- Assess the damage of BASKERVILLE and CHIMERA on ports, government agencies, and private industry.
- Coordinate with affected countries to assess and mitigate the impacts of BASKERVILLE and CHIMERA to global trade.
- Maintain contingency plans for escalation of software deployment.

Policy & Response Options:

NATIONAL RESPONSE

- FBI and DHS will coordinate intelligence gathering with local law enforcement.
  - FBI Houston Field Office and Field Intelligence Group will work with the Houston DHS Fusion Center, local law enforcement, and Maritime ISAC and Maritime Transportation System ISAC to collect information at the Port of Houston and Port of Corpus Christi and assess the impact of BASKERVILLE and CHIMERA.
- Issue CISA Traffic Light Protocol: AMBER (TLP: AMBER) to Maritime ISAC and Maritime Transportation System ISAC members. This alert will include:
  - Warning regarding BASKERVILLE and CHIMERA, and potential severity and implications.
  - Identification of CHIMERA as a malware dropper launched by an APT on TidalWaves port management system.
- Establish national cyber taskforce including IT/IS staff from Port of Houston and Port of Corpus Christi, cyber specialists from the Rabinara Group, TidalWaves, Maritime ISAC, Maritime Transportation System ISAC, the FBI National Cyber Investigative Joint Task Force, and CISA to address the ransomware and malware attacks.
  - Assess damage and implement immediate mitigation plan for Port of Houston and Port of Corpus Christi.
  - Establish working groups to prioritize analysis of CHIMERA lateral movement potential, reverse-engineer BASKERVILLE and CHIMERA, and identify actors for attribution.
- Prioritize intelligence collection on 1881 COLECTIV and MANTICORE within the NSA, CIA, and FBI.
  - Contact Romanian and Interpol authorities through the FBI Legal Attaché in Bucharest, which covers Romania, in order to question 1881 COLECTIV SUBJECT in custody. Coordinate with DOJ's Office of International Affairs to request Romanian assitance via MLAT, if needed.

INTERNATIONAL RESPONSE

- Establish an international cyber taskforce with Nigeria, Australia, Brazil, France, and India to assess and mitigate the international impact from BASKERVILLE and CHIMERA.
  - Establish collaboration between USAID and the Ministry of Foreign Affairs in Nigeria to coordinate and address ongoing needs due to the situation at the Port of Harcourt.
- Establish international lines of communication with relevant partners.
  - Send high-priority diplomatic cable notifying international partners of malicious indicators of compromise (IOCs).
  - Coordinate with State Department RSO to notify OSAC members of malicious IOCs.
- Create economic outlook report that describes potential outcomes of a disruption of global trade as a result of the cyberattack, collaborating with the WTO and Financial Services ISAC.

ESCALATION CONTINGENCIES

- Put CYBERCOM on alert to develop potential OCO response options in the event the situation escalates.
- Prepare a public statement in order to mitigate negative PR, acknowledging that the U.S. Federal Government is coordinating with local Texas government, state Texas government, and private sector actors in order to assess and mitigate the impact of BASKERVILLE and CHIMERA.
  - Establish a PR strategy with DOJ Office of Public Affairs, CISA, social media, and news media companies to counter misinformation and potential disinformation.

Policy Recommendation:

The task force recommends implementing the National Response and International Response immediately. Additionally, the NSC should consider implementing the Escalation Contingencies should the CHIMERA software be detected *en masse* across the USG and private sector.