OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
24 JUNE 2021 IA-52111-21

CYBERSECURITY

(U//FOUO) Ransomware Attacks in United States Likely to Increase

(U//FOUO) ***We assess that ransomware attacks targeting US networks are likely to increase in the near and long term because cybercriminals have developed effective business models to increase their financial gain, likelihood for operational success, and anonymity.*** Growing demand for ransomware-as-a-service (RaaS) and the use of initial access brokers (IAB) probably have helped cybercriminals reduce overhead costs and deepen their technical expertise. We assume global environmental factors also serve to sustain these operations, including broadly available vulnerabilities in networks, cybercriminals operating in permissive environments, and the ability for financially driven actors to act with at least some anonymity, including through the use of cryptocurrency.

- *(U)* During the last year, there was an increase in the number of ransomware incidents perpetrated by RaaS operators, as well as an increase in networks compromised by IABs. Operators using the RaaS model represented more than half of all ransomware attacks in 2020, according to media reporting. Ransomware variants such as Ryuk, Maze, REvil, DoppelPaymer and most other top variants also used the RaaS model throughout 2020, according to multiple cybersecurity reports.
- *(U)* Since at least early 2020, ransomware actors have increasingly used IABs to gain initial access and maintain persistence on target networks, according to multiple cybersecurity firm reports. This relationship reduces the time and resources needed to gain a foothold in a network that can be used to deploy ransomware, according to the same reports.

(U) Use of Cryptocurrency as Payment Helping to Minimize Risk

(U) Requesting ransoms in cryptocurrency like Bitcoin and Monero gives cybercriminals a stateless, decentralized, and anonymized method of transferring funds. This makes payments easier to facilitate than a wire transfer or international payment in fiat currencies and reduces the risk of apprehension. Unlike bank accounts, crypto wallets can be anonymously created and accessed by anyone who holds the wallet's private key, and use of multiple wallets to transfer funds allows cybercriminals to further cover their tracks.

(U) Prepared by the Cyber Mission Center, Field Operations Division-Northeast Region, and the Multi-State Information Sharing and Analysis Center. Coordinated within the DHS Intelligence Enterprise (CBP, CIMC, CWMD, and USCG ICC). For questions, contact DHS-SPS-RFI@hq.dhs.gov

(U//FOUO) ***We assess that recent compromises, including ransomware attacks, on US business networks likely will result in the degradation of physical operations, including inadvertent impacts caused by victims shutting down operational technology (OT) networks to prevent the spread of ransomware.*** Operational downtime also disrupts supply chains of dependent industries and infrastructure, and may cause additional effects such as increased prices, reduced supply, and create panic among the public. We base this assessment on recent compromises against JBS SA, Colonial Pipeline[USPER], and the New York Metropolitan Transit Authority[USPER], which demonstrate how the targeting of such networks affects operations.

- *(U)* In June 2021, REvil cybercriminals conducted a ransomware attack against business networks owned by meat processor JBS SA and received a ransom of $11 million dollars in cryptocurrency, according to media reporting. The attack forced JBS SA to shut down global business networks, directly impacting their operations. The shutdown degraded services on the network, such as tagging meat and scheduling shifts, which in turn degraded meat production, according to the same source.
- *(U)* Cybercriminals known as "DarkSide" in May 2021 conducted a ransomware attack against Colonial Pipeline's corporate network and received $4.3 million dollars in cryptocurrency—some of which was later recovered—according to media reporting and a Cybersecurity and Infrastructure Security Agency alert. The company shut down its OT networks to contain and mitigate the ransomware's spread. This disabled all pipeline operations and halted the majority of fuel distribution across the mid-Atlantic and Southern United States for a week, according to the same source.
- *(U)* In April 2021, unknown malicious cyber actors with suspected ties to the Chinese Government compromised 3 of 18 computer systems used by the New York City Metropolitan Transit Authority, according to media reporting. Although the cyber actors did not compromise the OT network that controls the train cars, network defenders were concerned that the cyber actors may have established a backdoor on the network to allow persistent access, enabling future attacks.

Source, Reference, and Dissemination Information	
Source Summary Statement	*(U//FOUO)* We assess that ransomware attacks targeting US networks are likely to increase in the near and long term because cybercriminals have developed effective business models to increase their financial gain, likelihood for operational success, and anonymity. We have **medium confidence** in this assessment based on information obtained from US cybersecurity companies as this information consists of verifiable, firsthand accounts or secondhand accounts corroborated by additional government or press reporting. We have **medium confidence** in the information obtained from open source reporting because some of it is corroborated by other reporting. *(U//FOUO)* We assess that recent compromises, including ransomware attacks, on US business networks will likely result in the degradation of physical operations, including inadvertent impacts caused by victims shutting down operational networks (OT) to prevent the spread of ransomware. We have **medium confidence** in this assessment based on information obtained from US cybersecurity companies and joint cybersecurity advisories from US Government agencies, as this information consists of verifiable, firsthand accounts or secondhand accounts corroborated by additional government or press reporting. We have **medium confidence** in the information obtained from open source reporting because some of it is corroborated by other reporting. *(U//FOUO)* While reporting on ransomware and cyber criminal activity is often incomplete, we maintain our **medium confidence** in our assessment because of the breadth and depth of sources that we incorporated into these assessments. Additional reporting about the scope, size, and tactics, techniques, and procedures utilized by IABs working in conjunction with ransomware actors would bolster our confidence in our assessment.
Definitions	*(U)* **Ransomware as-a service:** The ransomware economy includes a community of major malware developers, affiliates, and those that provide adjacent services such as selling network access, according to a news media. *(U)* **Initial Access Brokers (also known as Initial Access Sellers):** Opportunistic actors supplying affiliates with access-as-a-service. They obtain initial access to organizations and then offer it for sale on the same underground forums occupied by cybercriminals. *(U)* **Operational Technology:** A category of hardware and software that monitors and controls how physical devices perform. In the past, OT was used primarily in industrial control systems for manufacturing, transportation and utilities.
Dissemination	*(U)* Federal, state, local, and private sector network defenders.
Reporting Suspicious Activity	*(U)* To report a computer security incident please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form. The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail

	DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Warning Notices & Handling Caveats	*(U)* **Warning**: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials **may share** this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures.