THREAT BULLETINS

2021 Trends Show Increased Globalized Threat of Ransomware

TLP:WHITE

Feb 09, 2022

Health-ISAC is distributing a threat bulletin regarding the collaborative work of the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) provided in a Joint Cybersecurity Advisory (CSA) alert (AA22-040A).

In 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents targeting critical infrastructure organizations globally. Additionally, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 US critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors.

The Australian Cyber Security Centre (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities including the healthcare and medical, financial services and markets, higher education and research, and energy sectors. The United Kingdom's National Cyber Security (NCSC-UK) recognizes ransomware as the largest cyber threat facing the United Kingdom with education as one of the top UK sectors targeted by ransomware actors coupled with leveraging attacks against businesses, charities, the legal profession, and public services in the Local Government and Health Sectors.

Health-ISAC is sharing this alert due to the observed continuous evolution of ransomware tactics and techniques in 2021 which is indicative of threat actors' growing technological sophistication and an increased ransomware threat to organizations globally.

All members are encouraged to review 2021 Trends Show Increased Globalized Threat of Ransomware, which has been attached to this alert.

Cybersecurity authorities in the United States, Australia, and the United Kingdom observed the following behaviors and trends among cyber criminals in 2021:

- **Gaining access to networks via phishing, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting vulnerabilities.** Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware. Note: these infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.

- **Using cybercriminal services-for-hire.** The market for ransomware became increasingly "professional" in 2021, and the criminal business model of ransomware is now well established. In addition to their increased use of ransomware-as-a-service (RaaS), ransomware threat actors employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other

cyber criminals. NCSC-UK observed that some ransomware threat actors offered their victims the services of a 24/7 help center to expedite ransom payment and restoration of encrypted systems or data.

Cybersecurity authorities in the United States, Australia, and the United Kingdom assess that if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent. Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model. Additionally, cybersecurity authorities in the United States, Australia, and the United Kingdom note that the criminal business model often complicates attribution because there are complex networks of developers, affiliates, and freelancers; it is often difficult to identify conclusively the actors behind a ransomware incident.

- **Sharing victim information.** Eurasian ransomware groups have shared victim information with each other, diversifying the threat to targeted organizations. For example, after announcing its shutdown, the BlackMatter ransomware group transferred its existing victims to infrastructure owned by another group, known as Lockbit 2.0. In October 2021, Conti ransomware actors began selling access to victims' networks, enabling follow-on attacks by other cyber threat actors.

- **Shifting away from "big-game" hunting in the United States.**

    - In the first half of 2021, cybersecurity authorities in the United States and Australia observed ransomware threat actors targeting "big game" organizations—i.e., perceived high-value organizations and/or those that provide critical services—in several high-profile incidents. These victims included Colonial Pipeline Company, JBS Foods, and Kaseya Limited. However, ransomware groups suffered disruptions from U.S. authorities in mid-2021. Subsequently, the FBI observed some ransomware threat actors redirecting ransomware efforts away from "big-game" and toward mid-sized victims to reduce scrutiny.

    - The ACSC observed ransomware continuing to target Australian organizations of all sizes, including critical services and "big game," throughout 2021.

    - NCSC-UK observed targeting of UK organizations of all sizes throughout the year, with some "big game" victims. Overall victims included businesses, charities, the legal profession, and public services in the Education, Local Government, and Health Sectors.

- **Diversifying approaches to extorting money.** After encrypting victim networks, ransomware threat actors increasingly used "triple extortion" by threatening to (1) publicly release stolen sensitive information, (2) disrupt the victim's internet access, and/or (3) inform the victim's partners, shareholders,

or suppliers about the incident. The ACSC continued to observe “double extortion” incidents in which a threat actor uses a combination of encryption and data theft to pressure victims to pay ransom demands