02 June 2023

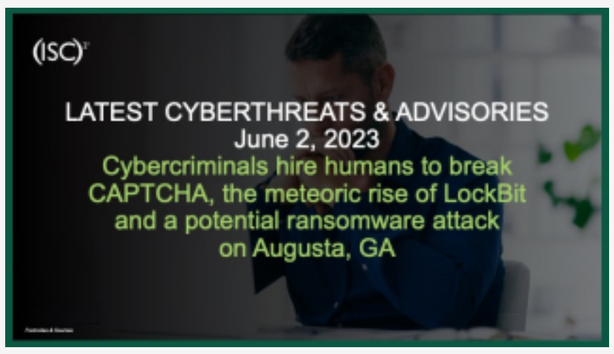
LATEST CYBERTHREATS AND ADVISORIES - JUNE 2, 2023

Cybercriminals hire humans to break CAPTCHAs, the meteoric rise of LockBit and a potential ransomware attack on the U.S. city of Augusta, Georgia. Here are the latest threats and advisories for the week of June 2, 2023.

By John Weiler

Threat Advisories and Alerts

China State-Sponsored Actor Infiltrates U.S. Critical Infrastructure



In a collaborative effort, cybersecurity authorities from the U.S., Canada, Australia, New Zealand and the U.K. have issued a joint advisory to highlight a series of events linked to a China state-sponsored threat actor known as Volt Typhoon. The cybercriminal's activity impacts the networks of critical infrastructure sectors across the U.S., prompting concerns that the bad actor might deploy similar tactics on a larger scale worldwide. A primary strategy of Volt Typhoon is a technique known as "living off the land," which utilizes pre-existing network administration tools to evade detection while conducting malicious activity.

The Meteoric Rise of LockBit Ransomware

Committing 913 ransomware attacks worldwide in 2022, the LockBit ransomware gang has become the kingpin of the cybercrime world. The Cyber Security Agency of Singapore (CSA) recently published an article tracking LockBit's meteoric rise, from the groups early days as the ABCD ransomware gang to its revolutionization of the cybercriminal affiliate model and its present day turmoil. Will the group soon come undone? With the U.S. Federal Bureau of Investigation (FBI) after them, the arrest of a LockBit affiliate in Canada and discontent potentially brewing among members—as evident by the recent internal leak of the gang's source code—LockBit's fall may be imminent. The full story can be read in the link above.

Emerging Threats and Research

Over 1 Million Customer Records Leaked in SimpleTire Database Error Debacle

A database configuration error at the Philadelphia-based business SimpleTire led to the exposure of 1TB of customer records. Over 2.8 million records are contained in the SimpleTire database, including more than a million order confirmations that reveal customer names, partial credit card details and expiration dates, phone numbers and other personal information. Security researcher Jeremiah Fowler, who reported the incident, warned, "The criminal could contact the victim and claim to work for SimpleTire or one of the installers and advise the customer that they need to update their payment details." In other words, cybercriminals could use the information to social engineer attacks on unsuspecting SimpleTire customers.

U.S. City of Augusta Reportedly Hit with Ransomware Attack

The U.S. city of Augusta, Georgia, has been hit by a cyber "incident," which began on Sunday, May 21, when some of the city's computer systems were disrupted. While the Augusta government has revealed little details about the incident, local TV station FOX54 has reported that it was a ransomware attack with a $50 million payment demand. The ransomware gang BlackByte has claimed responsibility for the attack, as well as theft of 10GB of "sensitive data."

Personal Data Swindled from Nearly 9 Million Patients in MCNA Dental Breach

Managed Care of North America (MCNA) Dental, one of the largest dental health insurers in the U.S., recently reported a ransomware breach, impacting 8.9 million patients. "We learned a criminal was able to see and take copies of some information in our computer system between February 26, 2023 and March 7, 2023," reads a notice published on MCNA's website this past Friday. Stolen information included Social Security numbers, driver's license numbers, email addresses, health insurance information and other sensitive data. The notorious LockBit ransomware gang is believed to be behind the attack.

Cybercriminals Employ Humans to Bypass CAPTCHA Security Controls

Researchers at cybersecurity company Trend Micro have reported an uptick in services that employ human CAPTCHA solvers, which help cybercriminals get around the security feature. How does it work? Bot operators use automation to collect the CAPTCHA and send it to a service provider where humans will solve it and send it back to the operator. While this maneuver may sound wild, an attack has already been experienced by the Poshmark social commerce marketplace.

To stay updated on the latest cybersecurity threats and advisories, look for weekly updates on the (ISC)² blog. Please share other alerts and threat discoveries you've encountered and join the conversation on the (ISC)² Community Industry News board.

Posted by (ISC)² Management on 02 June 2023 at 06:00 AM in IT Security, Ransomware, Risk | Permalink

Comments