Threat Image

As we enter the month of July, some countries have already begun their holiday season, while others are eagerly awaiting August. However, regardless of the vacation plans, it is important to remain vigilant against phishing attacks and malware. LinkedIn is abuzz with advice and tips on how to protect oneself from these threats. It is crucial to stay informed and take proactive measures to safeguard personal and professional information.

Phishing is one of the primary delivery methods for ransomware. Rather than specifically stealing data with ransomware through phishing, the main aim of the initial phishing attack is to steal credentials. Using credentials means hackers can access internal networks as a 'legitimate' user. They can potentially escalate their attack undetected and deliver ransomware from within the network, encrypting and removing data before internal teams can respond. (1)

A notable addition to this year's ransomware landscape is MalasLocker, a new ransomware gang that gained prominence in May for securing the top spot on Marcelo Rivero's list of known ransomware attacks by gang. Rivero is Malwarebytes' ransomware specialist, monitors information published by ransomware gangs on their Dark Web sites, and maintains a list of known ransomware attacks perpetrated by various gangs. What sets MalasLocker apart, however, is its unique approach. Unlike traditional ransomware groups, MalasLocker doesn't demand ransoms from its victims. Instead, it asks them to donate to approved charitable organizations. The ransom note README.txt from MalasLocker states, "Unlike traditional ransomware groups, we're not asking you to send us money. We just dislike corporations and economic inequality." It is highly unusual for a ransomware gang to claim to attack organizations for altruistic reasons. While one might assume that a gang with such stated principles would primarily target larger and wealthier organizations, this doesn't seem to be the case. The gang's blog suggests that it is open to targeting businesses of all sizes, as long as they are not located in "Latin America, Africa, or other colonized countries. " (It is worth noting, however, that ransomware gangs, and cybercriminals in general, have a long and storied history of writing long and tedious tracts justifying their criminal activity with grandiose claims. It doesn't impress us.) (2)

Vacation time provides an opportunity for reflection, and this message is specifically addressed to the C-Suite. In April, Helsinki District Court handed a three-month suspended sentence to the former CEO of a psychotherapy firm targeted in a major data breach, according to the Finnish Broadcasting Company (Yle). The court found the ex-CEO of Vastaamo, Ville Tapio, guilty of a data protection crime because he did not fulfil General Data Protection Regulation (GDPR) requirements, in terms of the pseudonymisation and encryption of patient data handled by the center. (3)

Latest Cyberthreats and Advisories (4)

- NCSC Publishes Report About Cyberthreats in the Legal Sector
- Super Mario Malware Attacks Windows' Users
- Southwest and American Airlines Breached Due to Third-Party Vendor Hack
- 6,558 Arrests and €740 Million in Confiscated Cash Highlight EncroChat Bust
- Siemens Energy and 45,000 Students Impacted as MOVEit Transfer Fallout Continues
- U.S. Cyber Talent Shortage Addressed in Recent Washington Hearing

(1) https://aag-it.com/the-latest-ransomware-statistics/
(2) https://www.malwarebytes.com/blog/threat-intelligence/2023/06/ransomware-review-june-2023
(3) https://yle.fi/a/74-20027665
(4) https://blog.isc2.org/