kindred

Security Newsletter

30 November 2020

Subscribe to this newsletter

Sopra Steria expects €40 to €50 million loss after Ryuk ransomware attack

French IT services giant Sopra Steria said today in an official statement that the October Ryuk ransomware attack will lead to a loss of between €40 million and €50 million. Sopra Steria is a European information technology firm with 46,000 employees in 25 countries providing a large array of IT services, including consulting, systems integration, and software development.

Sopra Steria published a statement on October 21st regarding a cyberattack that hit its network on the evening of October 20th but did not provide details on who was behind the attack.The ransomware attack was blocked by Sopra Steria's in-house security and IT teams which contained the ransomware to "a limited part of the Group's infrastructure" thus protecting the company's data, as well as its customers and partners. The recovery process started by the company on October 26th is almost complete, with access restored to nearly all "workstations, R&D and production servers, and in-house tools and applications." How was it that the French IT services firm got hit by a version of Ryuk that had not been previously seen by security researchers? Experts say the cybercrime gang behind Ryuk continually refines and updates the crypto-locking malware, sometimes customizing it for individual targets, to better try and evade security defenses

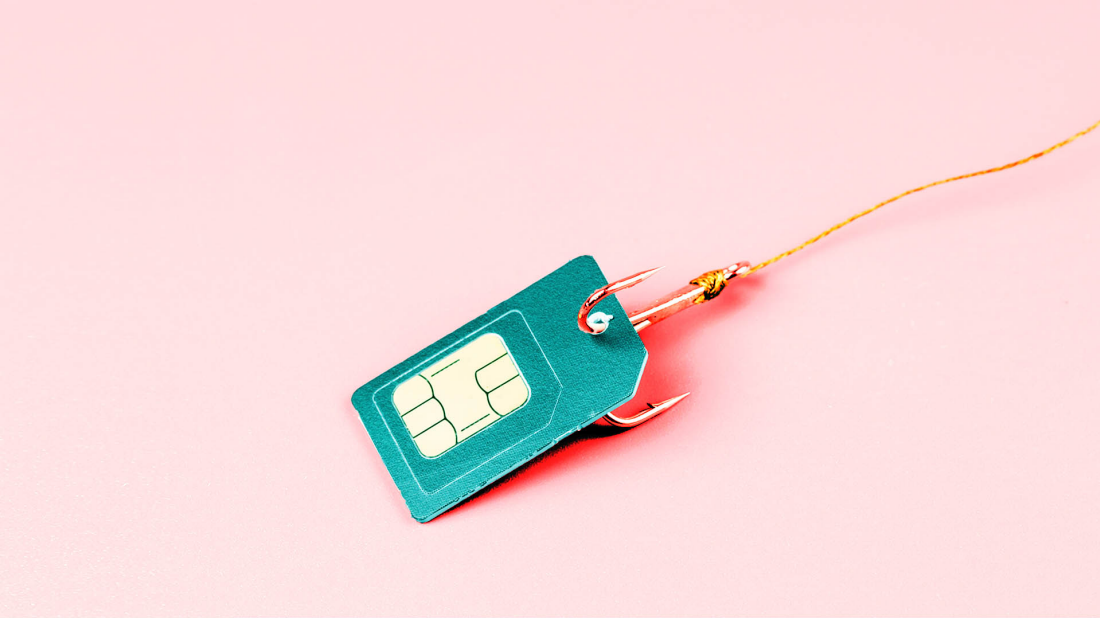
In a statement issued on Wednesday, the firm also says it expects to receive an insurance payout of $35 million. The company notes, however, that it does not expect the ransomware outbreak to impact its fourth quarter sales results, and says its cleanup efforts have nearly concluded. "After including the items mentioned above, for financial year 2020 Sopra Steria expects to see negative organic revenue growth of between 4.5% and 5.0% (previously 'between -2% and -4%'), an operating margin on business activity of around 6.5% (previously 'between 6% and 7%'), and free cash flow of between €50 million and €100 million (previously 'between €80m and €120m')," the company added.

Cognizant, one of the largest IT managed services company worldwide, also said it expected losses of between $50 million to $70 million after a Maze ransomware attack from April 2020.

Read More on BleepingComputer

Even More on BankInfoSecurity

SIM swap scam: What it is and how to protect yourself



SIM swap scams have been a growing problem, with fraudsters targeting people from various walks of life, including tech leaders, and causing untold damage to many victims. Commonly, the point of this type of attack is to gain access to one, or more, of the target's online accounts. The cybercriminal behind the attack is also banking on the assumption that the victim uses phone calls and text messages as a form of two-factor authentication (2FA). Here's why you should be on the lookout for attacks where someone can upend your life by first hijacking your mobile phone number.

Also known as SIM hijacking and SIM splitting, SIM swapping can be described as a form of account takeover fraud. To make the attack work, the cybercriminal will first gather information on their mark, often through trawling the web and searching for every tidbit of data the potential victim may have (over)shared. The victim's personal information can also be gleaned from known data breaches or leaks, or via social engineering techniques, such as phishing and vishing, where the fraudster wheedles the information directly out of the target. With enough information in their hands, the fraudster will contact the target's mobile phone provider and trick its customer service representative into porting their telephone number to a SIM card owned by the criminal. More often than not, the scammer's story will be something along the lines that the switch is needed due to the phone being stolen or lost. Once the process is done, the victim will lose access to the cellular network and phone number, while the hacker will now receive the victim's calls and text messages.

While SIM swap scams are ever-present and a threat to everybody, there are ways to protect yourself. Taking one or more of the several steps outlined in the article can help you lower your chances of falling victim to such an attack. Additionally, you can contact your bank and telecommunications providers to inquire about any supplementary security services you can enable to lock down your accounts.

Read More on WeLiveSecurity

More #News

- Home Depot agrees to $17.5 million settlement over 2014 data breach
- China's Baidu Android Apps Caught Collecting Sensitive User Data
- Study finds 31% of third-party vendors could cause significant damage to organizations if breached
- Major Power Outage in India Possibly Caused by Hackers: Reports
- LightBot: TrickBot's new reconnaissance malware for high-value targets
- Manchester United Unable to Fully Restore Systems A Week After Cyberattack
- Spotify launches 'rolling reset' on customer accounts, passwords linked to data leak
- Security flaws in smart doorbells may open the door to hackers
- Tesla Model X hacked and stolen in minutes using new key fob hack
- Malware creates scam online stores on top of hacked WordPress sites
- New 'LidarPhone' Attack Uses Robot Vacuum Cleaners for Eavesdropping
- A hacker is selling access to the email accounts of hundreds of C-level executives

#Breach Log

- Sophos alerts customers of info exposure after security breach
- Canon publicly confirms August ransomware attack, data theft
- Networking equipment vendor Belden discloses data breach
- Truck routing provider Rand McNally hit by cyberattack
- Ransomware Attack Targets Baltimore County Public Schools
- Ransomware hits largest US fertility network, patient data stolen
- Passwords exposed for almost 50,000 vulnerable Fortinet VPNs
- Skimmer Compromised Website of Boom! Mobile In October

#Patch Time!

- Unofficial Patch Released for Windows 7 Zero-Day Vulnerability
- cPanel 2FA bypassed in minutes via brute-force attacks, patch available
- Drupal Releases Out-of-Band Security Updates Due to Availability of Exploits
- Drupal sites vulnerable to double-extension attacks
- Critical Unpatched VMware Flaw Affects Multiple Corporates Products

#Tech and #Tools

- Code Security Advent Calendar 2020
- Protect domains that don't send email with SPF and DMARC
- Introducing another free CA as an alternative to Let's Encrypt
- CyberAlarm: An independent security review... and why you should avoid it.
- A Fresh Outlook on Mail Based Persistence
- Bento Toolkit: Minimal docker container for Pentest and CTF

- Architecture of a ransomware (1/2)
- DFIR Report: PYSA/Mespinoza Ransomware
- URLHunter recon tool: search URLs exposed by shortener services
- Inside the Cit0Day Breach Collection
- S3 Objects Check: Whitebox evaluation of effective S3 object permissions
- Mitre ATT&CK® Mappings for Amazon GuardDuty

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us