Security Newsletter

13 Jun 2022

Subscribe to this newsletter

How a Saxophonist Tricked the KGB by Encrypting Secrets in Music

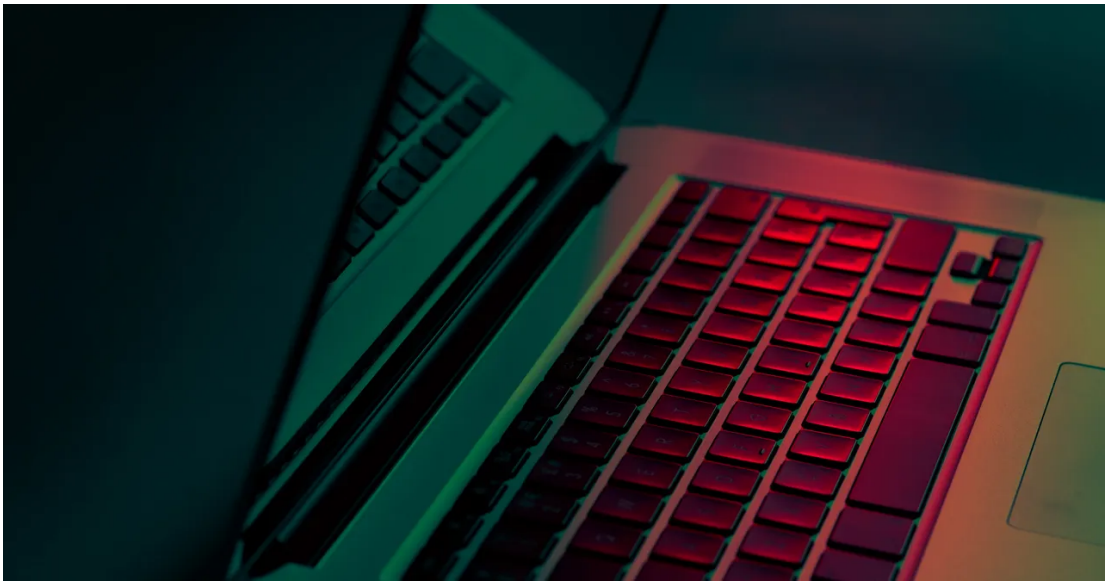
In 1985, saxophonist Merryl Goldberg found herself on a plane to Moscow with three fellow musicians from the Boston Klezmer Conservatory Band. She had carefully packed sheet music, reeds, and other woodwind supplies, along with a soprano saxophone, to bring into the USSR. But one of her spiral-bound notebooks, lined with staves for hand-notating music, contained hidden information.

Using a code she had developed herself, Goldberg had obscured names, addresses, and other details the group would need for their trip in handwritten compositions that looked, to an untrained eye, like the real melodies she'd written on other pages of the book. Goldberg and her colleagues didn't want to give Soviet officials details of who they planned to see and what they planned to do on their trip. They were going to meet the Phantom Orchestra.

The trip was a rare and special opportunity for American and Soviet players to meet in the USSR and make music together. It was also an opportunity for the American musicians to smuggle information about aid efforts and plans to the Phantom Orchestra, and for the ensemble to send updates out, including details about individuals looking to escape the Soviet Union.

Read More on Wired

Conti's Attack Against Costa Rica Sparks a New Ransomware Era



For the last two months, Costa Rica has been under siege. Two major ransomware attacks have crippled many of the country's essential services, plunging the government into chaos as it scrambles to respond. Officials say that international trade ground to a halt as the ransomware took hold and more than 30,000 medical appointments have been rescheduled, while tax payments have also been disrupted. Millions have been lost due to the attacks, and staff at affected organizations have turned to pen and paper to get things done.

Costa Rica's government, which changed midway through the attacks after elections earlier this year, has declared a "national emergency" in response to the ransomware—marking the first time a country has done so in response to a cyberattack. Twenty-seven government bodies were targeted in the first attacks, which ran from mid-April until the start of May, according to new president Rodrigo Chaves. The second attack, at the end of May, has sent Costa Rica's health care system into a spiral. Chaves has declared "war" on those responsible.

At the heart of the hacking spree is Conti, the notorious Russia-linked ransomware gang. Conti claimed responsibility for the first attack against Costa Rica's government and is believed to have some links to the ransomware-as-a-service operation HIVE, which was responsible for the second attack impacting the health care system.

Read More on Wired

More #News

- WiFi probing exposes smartphone users to tracking, info leaks
- Dark web sites selling alleged Western weapons sent to Ukraine

- Chinese hacking group Aoqin Dragon quietly spied orgs for a decade
- Massive Facebook Messenger phishing operation generates millions
- Surfshark, ExpressVPN pull out of India over data retention laws
- US seizes SSNDOB market for selling personal info of 24 million people
- US: Chinese govt hackers breached telcos to snoop on network traffic
- Why Netflix isn't the Only One Bummed About Password Sharing
- What Counts as “Good Faith Security Research?”
- Americans report losing over $1 billion to cryptocurrency scams
- Clipminer malware gang stole $1.7M by hijacking crypto payments
- Ransomware attacks need less than four days to encrypt systems
- Hackers steal WhatsApp accounts using call forwarding trick
- Aligning Your Password Policy enforcement with NIST Guidelines
- Vodafone plans carrier-level user tracking for targeted ads
- Three Nigerians arrested for malware-assisted financial crimes
- Even the Most Advanced Threats Rely on Unpatched Systems

#Breach Log

- Confluence servers hacked to deploy AvosLocker, Cerber2021 ransomware
- Vice Society ransomware claims attack on Italian city of Palermo
- Shields Health Care Group data breach affects 2 million patients
- Novartis says no sensitive data was compromised in cyberattack
- Costa Rica’s public health agency hit by Hive ransomware

#Patch Time!

- Android June 2022 updates bring fix for critical RCE vulnerability
- Exploit released for Atlassian Confluence RCE bug, patch now
- GitLab security update fixes critical account take over flaw

#Tech and #Tools

- New PACMAN hardware attack targets Macs with Apple M1 CPUs
- Using CloudTrail to Pivot to AWS Accounts
- Technical Advisory – FUJITSU CentricStor Control Center
- Aoqin Dragon | Newly-Discovered Chinese-linked APT Has Been Quietly Spying On Organizations For 10 Years
- Managed Identity Attack Paths, Part 3: Function Apps
- Shining the Light on Black Basta
- Vulnerability within the UNISOC baseband opens mobile phones communications to remote hacker attacks

remote hacker attacks

- ripgen: Taking the Guesswork Out of Subdomain Discovery
- DeepPass—Finding Passwords With Deep Learning

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- Are you a developer with a strong security passion? Be part of our Cyber Security team

Kindred is one of the largest online gambling companies in the world with over 30 million customers. You can find all our open vacancies on our career page.

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

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

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