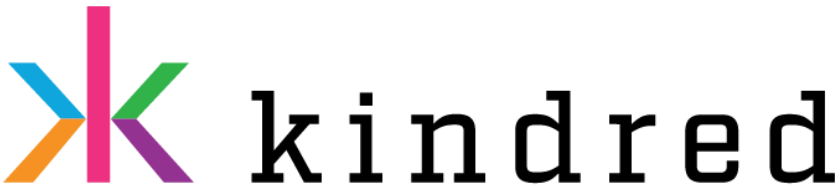


Security Newsletter

8 Nov 2021

Subscribe to this newsletter

Europol: Seven REvil/GandCrab ransomware affiliates were arrested in 2021

Europol has announced today the arrests of seven suspects who worked as “affiliates” (partners) for a major ransomware cartel and have helped carry out more than 7,000 attacks since early 2019.

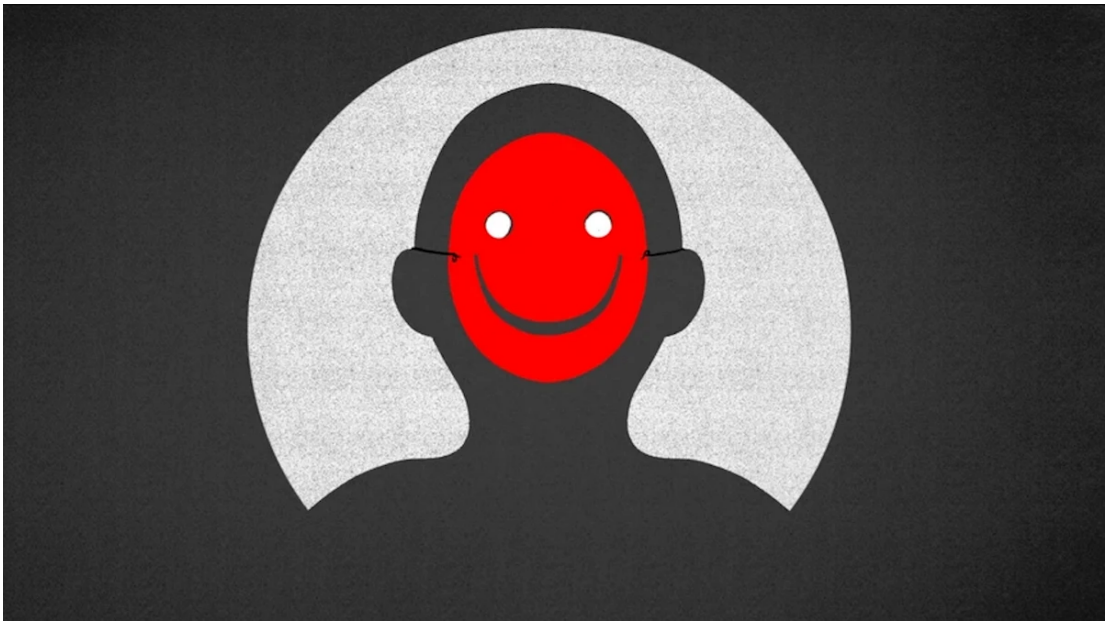
The suspects worked part of the REvil (Sodinokibi) and GandCrab Ransomware-as-a-Service (RaaS) operations. Both REvil and GandCrab, believed to be operated by the same individuals, created ransomware code that they offered to other cybercriminals for rent.

Europol says that since 2019, the seven suspects carried out attacks in which they collectively asked for more than €200 million ($230 million) in ransom demands.

Read More on The Record

Even More in Europol's press release

The Booming Underground Market for Bots That Steal Your 2FA Codes



The call came from PayPal's fraud prevention system. Someone had tried to use my PayPal account to spend $58.82, according to the automated voice on the line. PayPal needed to verify my identity to block the transfer.

"In order to secure your account, please enter the code we have sent your mobile device now," the voice said. PayPal sometimes texts users a code in order to protect their account. After entering a string of six digits, the voice said, "Thank you, your account has been secured and this request has been blocked."

But this call was actually from a hacker. The fraudster used a type of bot that drastically streamlines the process for hackers to trick victims into giving up their multi-factor authentication codes or one-time passwords (OTPs) for all sorts of services, letting them log in or authorize cash transfers.

Read More on Vice

More #News

- CISA creates catalog of known exploited vulnerabilities, orders agencies to patch
- GitLab servers are being exploited in DDoS attacks in excess of 1 Tbps
- US Sanctions Could Cut Off NSO From Tech It Relies On
- REvil Ransom Arrest, $6M Seizure, and $10M Reward
- Malware found in coa and rc, two npm packages with 23M weekly downloads
- Criminal group dismantled after forcing victims to be money mules

- State hackers breach defense, energy, healthcare orgs worldwide
- Pwn2Own: Printer plays AC/DC, Samsung Galaxy S21 hacked twice
- Alleged Twitter hacker charged with theft of $784K in crypto via SIM swaps
- CERT-FR warns of Lockean ransomware attacks against French companies
- Search engine phishing campaign targeting crypto wallet users

#Breach Log

- Robinhood Says It Was Hacked and Extorted But Nobody Lost Any Money
- Hacker steals $55 million from bZx DeFi platform
- 'Destructive' cyberattack hits National Bank of Pakistan
- Ransomware attack disrupts Toronto's public transportation system
- MediaMarkt hit by Hive ransomware, initial $240 million ransom
- US defense contractor Electronic Warfare hit by data breach
- UK Labour Party discloses data breach after ransomware attack
- BlackShadow hackers breach Israeli hosting firm and extort customers
- Newfoundland and Labrador healthcare system has suffered a cyberattack

#Patch Time!

- Sitecore XP RCE flaw patched last month now actively exploited
- Philips healthcare infomatics solution vulnerable to SQL injection
- Mozilla Thunderbird 91.3 released to fix high impact flaws
- Cisco fixes hard-coded credentials and default SSH key issues
- Over 30,000 GitLab servers still unpatched against critical bug
- Android November patch fixes actively exploited kernel bug

#Tech and #Tools

- Experts Detail Malicious Code Dropped Using ManageEngine ADSelfService Exploit
- Critical RCE Vulnerability Reported in Linux Kernel's TIPC Module
- Sitecore Experience Platform Pre-Auth RCE - CVE-2021-42237
- CVE-2021-43267: Remote Linux Kernel Heap Overflow | TIPC Module Allows Arbitrary Code Execution
- From Zero to Domain Admin
- Escalating XSS to Sainthood with Nagios
- Threat Hunting Certificate Account Persistence
- More Proactive SIMs
- A Kubeconfig Canarytoken
- Simple Storage Scanner
- Minimum Viable Secure Product

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 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 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