kindred

Security Newsletter

24 Jan 2022

Subscribe to this newsletter

Sketchy ‘Account Recovery’ Services Are Trying to Scam Hacking Victims on Twitter

People often get locked out of their online accounts. Sometimes they may have lost access to the email address registered to the account. Or perhaps the site or social network’s process for getting back in is so convoluted or ineffective, like Instagram’s, that people pay thousands of dollars for help from semi-professionals.

This market of third-party account recovery services is a seemingly ballooning industry, with some legitimate players and likely some scams too. And now they’re fighting over potential clients who tweet about their hacked or otherwise inaccessible accounts, using bots to automatically reply to people on Twitter pointing people to their recovery services.

Read More on Vice

A Trip to the Dark Site — Leak Sites Analyzed

Gone are the days when ransomware operators were happy with encrypting files on-site and more or less discretely charged their victims money for a decryption key. What we commonly find now is encryption with the additional threat of leaking stolen data, generally called Double-Extortion (or, as we like to call it: Cyber Extortion or Cy-X).

This is a unique form of cybercrime in that we can observe and analyze some of the criminal action via 'victim shaming' leak sites.

Since January 2020, we have applied ourselves to identifying as many of these sites as possible to record and document the victims who feature on them. Adding our own research, analyzing, and enriching data scraped from the various Cy-X operators and market sites, we can provide direct insights into the victimology from this specific perspective.

Read More on The Hacker News

More #News

- IRS Will Soon Require Selfies for Online Access
- Crime Shop Sells Hacked Logins to Other Crime Shops
- FBI warns of malicious QR codes used to steal your money
- CISA adds 17 vulnerabilities to list of bugs exploited in attacks
- US sanctions former Ukrainian official for helping Russian cyberspies
- Biden signs memo to boost US national security systems' defenses
- Interpol arrests 11 BEC gang members linked to 50,000 targets
- Beijing 2022 Winter Olympics app bursting with privacy risks
- Europol shuts down VPN service used by ransomware groups

- Europe's Move Against Google Analytics Is Just the Beginning
- Nigerian police arrest members of SilverTerrier BEC gang
- Europol takes down VPNLab, a service used by ransomware gangs
- EU wants to build its own DNS infrastructure with built-in filtering capabilities
- UK Government to Launch PR Campaign Undermining End-to-End Encryption

#Breach Log

- Over 90 WordPress themes, plugins backdoored in supply chain attack
- Crypto.com confirms 483 accounts hacked, $34 million withdrawn
- Indonesia's central bank confirms ransomware attack, Conti leaks data
- Red Cross cyberattack exposes data of 515,000 people seeking missing family
- Marketing giant RRD confirms data theft in Conti ransomware attack
- Fashion giant Moncler confirms data breach after ransomware attack
- Indian Fashion Retailer Data Leaked on Darknet Marketplace

#Patch Time!

- WordPress plugin flaw puts users of 20,000 sites at phishing risk
- Microsoft: SolarWinds fixes Serv-U bug exploited for Log4j attacks
- Zoho plugs another critical security hole in Desktop Central
- Microsoft releases OOB updates for January Windows update issues

#Tech and #Tools

- Scammers are creating new fraudulent Crypto Tokens and misconfiguring smart contract's to steal funds
- Stealing administrative JWT's through post auth SSRF (CVE-2021-22056)
- New MoonBounce UEFI malware used by APT41 in targeted attacks
- Safari bug leaks your Google account info, browsing history
- Emotet Now Using Unconventional IP Address Formats to Evade Detection
- Chinese Hackers Spotted Using New UEFI Firmware Implant in Targeted Attacks
- What does the newest kernel exploit mean for Kubernetes users and how to detect it?

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