kindred

Security Newsletter

31 Jan 2022

Subscribe to this newsletter

Scary Fraud Ensues When ID Theft & Usury Collide

What's worse than finding out that identity thieves took out a 546 percent interest payday loan in your name? How about a 900 percent interest loan? Or how about not learning of the fraudulent loan until it gets handed off to collection agents? One reader's nightmare experience spotlights what can happen when ID thieves and hackers start targeting online payday lenders.

The reader who shared this story (and copious documentation to go with it) asked to have his real name omitted to avoid encouraging further attacks against his identity. So we'll just call him "Jim." Last May, someone applied for some type of loan in Jim's name. The request was likely sent to an online portal that takes the borrower's loan application details and shares them with multiple prospective lenders, because Jim said over the next few days he received dozens of emails and calls from lenders wanting to approve him for a loan.

Read More on KrebsonSecurity

More #News

- Fake Investor John Bernard Sinks Norwegian Green Shipping Dreams
- Hacktivism and State-Sponsored Knock-Offs | Attributing Deceptive Hack-and-Leak Operations
- US bans major Chinese telecom over national security risks
- EU to create pan-European cyber incident coordination framework

- Finnish diplomats' phones infected with NSO Group Pegasus spyware
- 105 million Android users targeted by subscription fraud campaign
- White House wants US govt to use a Zero Trust security model
- UK govt releasing Nmap scripts to find unpatched vulnerabilities
- Russia arrests leader of "Infraud Organization" hacker group
- Apple Pays $100,500 Bounty to Hacker Who Found Way to Hack MacBook Webcam
- German Court Rules Websites Embedding Google Fonts Violates GDPR
- Microsoft Mitigated Record-Breaking 3.47 Tbps DDoS Attack on Azure Customers
- Biden administration launches initiative to protect U.S. water systems from cyberattacks
- Cybercriminals laundered $8.6 billion worth of cryptocurrency in 2021
- Tracking Secret German Organizations with Apple AirTags

#Breach Log

- Taiwanese Apple and Tesla contractor hit by Conti ransomware
- Segway store hacked to steal customers' credit cards
- Canada's foreign affairs ministry hacked, some services down
- Deadbolt ransomware hits more than 3,600 QNAP NAS devices
- Qubit Finance platform hacked for $80 million worth of cryptocurrency
- Unsecured AWS server exposed 3TB in airport employee records

#Patch Time!

- Windows vulnerability with new public exploits lets you become admin
- Apple fixes new zero-day exploited to hack macOS, iOS devices
- Linux system service bug gives root on all major distros, exploit released
- VMware: Patch Horizon servers against ongoing Log4j attacks!

#Tech and #Tools

- 3 Foundational Pillars for Attack Path Management: Pillar 2—Empirical Impact Assessment
- Solarwinds Web Help Desk: When the Helpdesk is too Helpful
- A story of leaking uninitialized memory from Fastly
- "Stratus Red Team": open-source adversary emulation for AWS

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