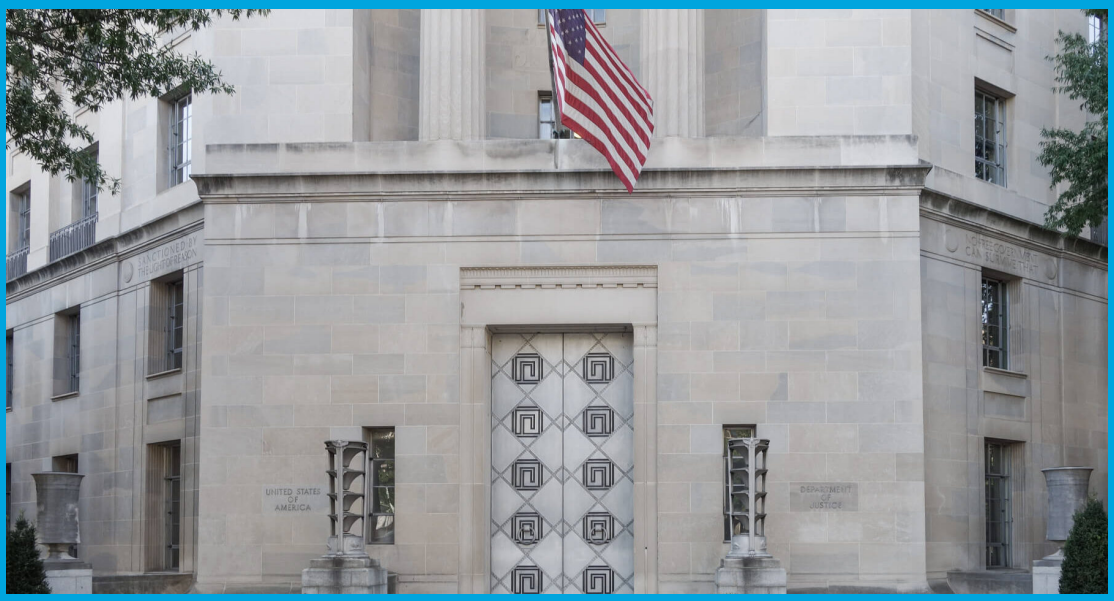
kindred

Security Newsletter

30 May 2022

Subscribe to this newsletter

Man who helped Infraud cybercrime cartel steal millions of credit cards sentenced



A Brooklyn resident was sentenced to four years in federal prison this week after pleading guilty to being an integral member of the Infraud Organization, a cybercrime cartel that stole over four million credit and debit card numbers and cost victims more than $568 million dollars.

John Telusma – a 37-year-old who went by “Peterelliot” online – is the 14th member of the Infraud gang to be charged in connection to the group’s activities, which the Justice Department said involved the “mass acquisition and sale of fraud-related goods and services, including stolen identities, compromised credit card data, computer malware, and other contraband.”

The group had members across the globe and the DOJ has already sentenced several members to lengthy prison sentences. After several undercover operations, U.S. officials partnered with law enforcement agencies across Europe, Australia and Asia to arrest 13 members of the group and shut down the Infraud website in February 2018.

Read More on The Record

DuckDuckGo has a tracker blocking carve-out linked to Microsoft contract

DuckDuckGo, the self-styled “internet privacy company” — which, for years, has built a brand around a claim of non-tracking web search and, more recently, launched its own ‘private’ browser with built-in tracker blocking — has found itself in hot water after a researcher found hidden limits on its tracking protection that create a carve-out for certain advertising data requests by its search syndication partner, Microsoft.

The researcher in question, Zach Edwards, tweeted the findings of his audit — saying he had found DDG’s mobile browsers do not block advertising requests made by Microsoft scripts on non-Microsoft web properties.

Edwards had some Twitter back and forth with DDG’s founder and CEO Gabe Weinberg, who initially appeared to be attempting to play down the finding by emphasizing all the stuff he said DDG’s browser does block (e.g., third-party tracking cookies, including those from Microsoft).

Read More on TechCrunch

More #News

- New Yorker imprisoned for role in carding group behind $568M damages

- FBI warns of hackers selling credentials for U.S. college networks
- Microsoft finds severe bugs in Android apps from large mobile providers
- Microsoft to force better security defaults for all Azure AD tenants
- FTC fines Twitter $150M for using 2FA info for targeted advertising
- Hacker says hijacking libraries, stealing AWS keys was ethical research
- Interpol arrests alleged leader of the SilverTerrier BEC gang
- DuckDuckGo browser allows Microsoft trackers due to search agreement
- Microsoft: Credit card stealers are getting much stealthier
- CISA adds 41 vulnerabilities to list of bugs used in cyberattacks
- Photos of abused victims used in new ID verification scam
- Hackers can hack your online accounts before you even register them
- Attackers Can Use Electromagnetic Signals to Control Touchscreens Remotely
- Remote bricking of Ukrainian tractors raises agriculture security concerns

#Breach Log

- Clop ransomware gang is back, hits 21 victims in a single month
- GitHub: Attackers stole login details of 100K npm user accounts
- BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state
- SpiceJet airline passengers stranded after ransomware attack
- General Motors credential stuffing attack exposes car owners info

#Patch Time!

- OAS platform vulnerable to critical RCE and API access flaws
- Exploit released for critical VMware auth bypass bug, patch now
- Microsoft shares mitigation for Windows KrbRelayUp LPE attacks
- Mozilla fixes Firefox, Thunderbird zero-days exploited at Pwn2Own
- Cisco Issues Patch for New IOS XR Zero-Day Vulnerability Exploited in the Wild
- Zoom Patches 'Zero-Click' RCE Bug

#Tech and #Tools

- Automating Azure Abuse Research—Part 1
- Understanding CVE-2022-22972 (VMWare Workspace One Access Auth Bypass)
- Use of Obfuscated Beacons in 'pymafka' Supply Chain Attack Signals a New Trend in macOS Attack TTPs
- Call of DeFi: The Battleground of Blockchain
- npm security update: Attack campaign using stolen OAuth tokens
- Orange-Cyberdefense/arsenal: An inventory and launcher for hacking programs
- ForceAdmin: Create infinate #UAC prompts forcing a user to run as admin

- grsecurity - Tetragone: A Lesson in Security Fundamentals
- How Defenders Can Hunt for Malicious JScript Executions
- Cloudflare's approach to handling BMC vulnerabilities

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