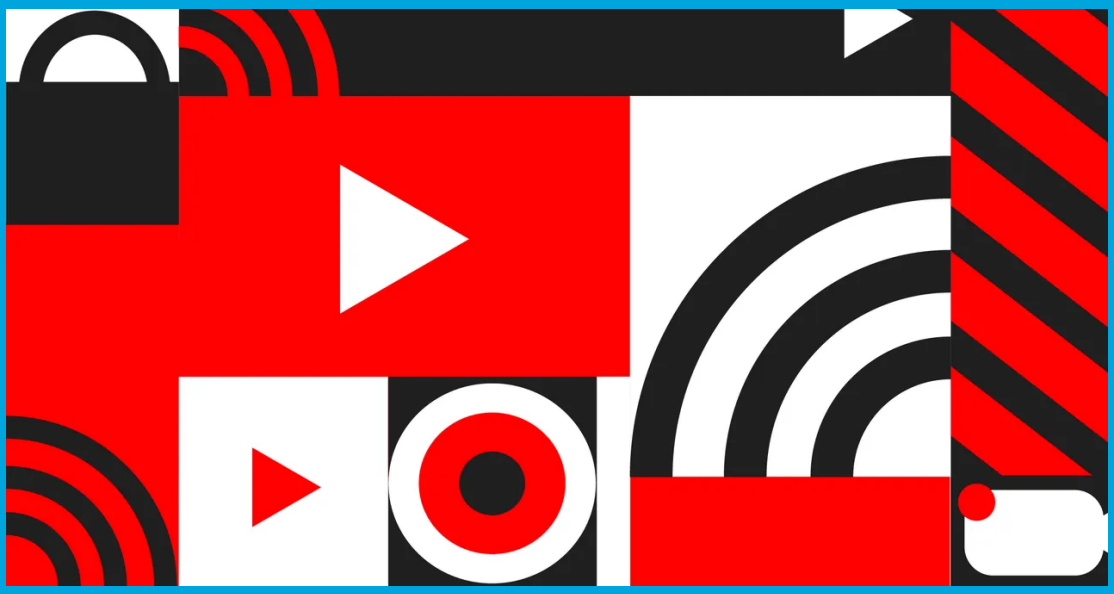
kindred

Security Newsletter

25 Oct 2021

Subscribe to this newsletter

How Hackers Hijacked Thousands of High-Profile YouTube Accounts



Since at least 2019, hackers have been hijacking high-profile YouTube channels. Sometimes they broadcast cryptocurrency scams, sometimes they simply auction off access to the account. Now, Google has detailed the technique that hackers-for-hire used to compromise thousands of YouTube creators in just the past couple of years.

Cryptocurrency scams and account takeovers themselves aren't a rarity; look no further than last fall's Twitter hack for an example of that chaos at scale. But the sustained assault against YouTube accounts stands out both for its breadth and for the methods hackers used, an old maneuver that's nonetheless incredibly tricky to defend against.

It all starts with a phish. Attackers send YouTube creators an email that appears to be from a real service—like a VPN, photo editing app, or antivirus offering—and offer to collaborate. They propose a standard promotional arrangement: Show our product to your viewers and we'll pay you a fee. It's the kind of transaction that happens every day for YouTube's luminaries, a bustling industry of influencer payouts.

Read More on Wired

FIN7 Recruits Talent For Push Into Ransomware

The financially motivated FIN7 cybercrime gang has masqueraded as yet another fictitious cybersecurity company called "Bastion Secure" to recruit unwitting software engineers under the guise of penetration testing in a likely lead-up to a ransomware scheme.

"With FIN7's latest fake company, the criminal group leveraged true, publicly available information from various legitimate cybersecurity companies to create a thin veil of legitimacy around Bastion Secure," Recorded Future's Gemini Advisory unit said in a report.

"FIN7 is adopting disinformation tactics so that if a potential hire or interested party were to fact check Bastion Secure, then a cursory search on Google would return 'true' information for companies with a similar name or industry to FIN7's Bastion Secure."

Read More on The Hacker News

Even More on Gemini Advisory

More #News

- Man Pleads Guilty to Stealing Nude Photos From Hundreds of iCloud Accounts
- Sim Swapper Doxes and SWATs His Accomplice
- More than 100,000 people have had their eyes scanned for free cryptocurrency

- FTC: ISPs collect and monetize far more user data than you'd think
- Microsoft Teams adds end-to-end encryption for one-to-one calls
- CISA: GPS software bug may cause unexpected behavior this Sunday
- Massive campaign uses YouTube to push password-stealing malware
- Google launches Android Enterprise bug bounty program
- Nine arrested for impersonating bank clerks to steal from the elderly
- Bulletproof hosting admins sentenced for helping cybercrime gangs
- US govt to ban export of hacking tools to authoritarian regimes
- Zerodium wants zero-day exploits for Windows VPN clients
- Man gets 7 years in prison for hacking 65K health care employees
- FBI, CISA, NSA share defense tips for BlackMatter ransomware attacks
- New Gummy Browsers attack lets hackers spoof tracking profiles
- NYT Journalist Repeatedly Hacked with Pegasus after Reporting on Saudi Arabia
- Detecting anomalies with TLS fingerprints could pinpoint supply chain compromises
- Why Is the Majority of Our MFA So Phishable?
- Dutch forensic lab decrypts Tesla's driving safety data and finds a wealth of information
- Facebook sues Ukrainian who scraped the data of 178 million users

#Breach Log

- Sinclair Broadcast 'Disrupted' by Ransomware Attack
- Microsoft: Russian SVR hacked at least 14 IT supply chain firms since May
- Popular NPM library hijacked to install password-stealers, miners
- Hacker sells the data for millions of Moscow drivers for $800
- SCUF Gaming store hacked to steal credit card info of 32,000 customers
- Evil Corp demands $40 million in new Macaw ransomware attacks
- Acer hacked twice in a week by the same threat actor
- LightBasin hacking group breaches 13 global telecoms in two years
- Hackers Exploited Popular BillQuick Billing Software to Deploy Ransomware
- Tesco's website restored after suspected cyberattack

#Patch Time!

- CISA urges admins to patch critical Discourse code execution bug
- Bug in Popular WinRAR Software Could Let Attackers Hack Your Computer
- Cisco SD-WAN Security Bug Allows Root Code Execution
- Squirrel Bug Lets Attackers Execute Code in Games, Cloud Services
- Patch PowerShell 7

#Tech and #Tools

- Researchers Break Intel SGX With New 'SmashEx' CPU Attack Technique

- Cracking RDP NLA Supplied Credentials for Threat Intelligence
- Life is Pane: Persistence via Preview Handlers
- Karma Ransomware | An Emerging Threat With A Hint of Nemty Pedigree
- AlphaGolang | A Step-by-Step Go Malware Reversing Methodology for IDA Pro
- Detecting and Protecting when Remote Desktop Protocol (RDP) is open to the Internet
- A Snapshot of CAST in Action: Automating API Token Testing
- Digital banking fraud: how the Gozi malware works
- Discourse SNS webhook RCE

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