kindred

Security Newsletter

21 Mar 2022

Subscribe to this newsletter

Microsoft Investigating Claim of Breach by Extortion Gang

Microsoft is investigating claims that an extortion-focused hacking group that previously compromised massive companies such as Ubisoft and Nvidia has gained access to internal Microsoft systems, according to a statement from the company.

The hacking group, which goes by the self-designated name LAPSUS$, has successfully breached a wave of corporations recently. LAPSUS$ sometimes makes unusual ransom demands of its victims, including asking Nvidia to unlock aspects of its graphics cards to make them more suitable for mining cryptocurrency. The group has so far not made any public demands against Microsoft.

On Sunday, a Microsoft spokesperson told Motherboard in an email that “We are aware of the claims and are investigating.”

Read More on Vice

The Big, Baffling Crypto Dreams of a $180 Million Ransomware Gang

Not satisfied with extorting $180 million from companies last year, the Conti ransomware gang is investing its coerced cash in new moneymaking schemes. Since last summer, according to leaked details from the group, the Russia-linked cybercrime organization has been quietly developing its own social network and blockchain-based cryptocurrency platform. Its leader even suggested opening an online casino.

Conti's unconventional expansion plans were revealed in 60,000 of the group's chat messages and files, which were published by a Ukrainian cybersecurity researcher who infiltrated the group.

While many of the leaked chat messages detail the daily workings of the notorious ransomware group, they also show how it's planning to expand beyond corporate extortion.

Read More on Wired

More #News

- Pro-Ukraine ‘Protestware’ Pushes Antiwar Ads, Geo-Targeted Malware
- New Phishing toolkit lets anyone create fake Chrome browser windows
- CISA, FBI warn US critical orgs of threats to SATCOM networks
- New Unix rootkit used to steal ATM banking data
- Europe warns of aircraft GPS outages tied to Russian invasion
- FBI warns of MFA flaw used by state hackers for lateral movement
- FTC to fine CafePress for cover up of massive data breach
- New Backdoor Targets French Entities via Open-Source Package Installer
- SEC filings show hidden ransomware costs and losses
- MITRE and partners build insider threat knowledge base
- Why Vaccine Cards Are So Easily Forged

#Breach Log

- Thousands of Open Cloud Databases Exposing Data in the Wild
- TransUnion cyber attack – hackers demand R225 million ransom
- Hundreds of GoDaddy-hosted sites backdoored in a single day

#Patch Time!

- cr8escape: New Vulnerability in CRI-O allows for container brekout
- From XSS to RCE (dompdf 0day)
- Western Digital app bug gives elevated privileges in Windows, macOS
- OpenSSL cert parsing bug causes infinite denial of service loop

#Tech and #Tools

- Announcing Azure in BloodHound Enterprise
- The Art and Science of macOS Malware Hunting with radare2
- Tool Release – ScoutSuite 5.11.0
- A Primer on Proxies
- Validate all the things: improve your security with input validation!
- Browser In The Browser (BITB) Attack

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