kindred

Security Newsletter

1 Nov 2021

Subscribe to this newsletter

Hitting the BlackMatter gang where it hurts: In the wallet

Earlier this year, Emsisoft researchers discovered a critical flaw in the BlackMatter ransomware that allowed them to help victims recover their files without paying a ransom, preventing millions of dollars falling into the hands of cybercriminals.

The work has been conducted quietly and privately so as not to alert the BlackMatter operators to the flaw. For the reasons discussed below, we believe it is now safe to share the story without jeopardizing the operation.

Read More on Emsisoft blog

EU to adopt new cybersecurity rules for smartphones, wireless, IoT devices

The European Commission has ordered an update to the Radio Equipment Directive in order to introduce new cybersecurity guidelines for radio and wireless equipment sold on the EU market, such as mobile phones, tablets, fitness trackers, and other smart IoT devices.

The new standards, which are currently scheduled to enter into effect by mid-2024, were adopted following a delegated act to the Radio Equipment Directive (RED), a piece of 2014 EU legislation that acts as the regulatory framework that equipment vendors must follow in order to sell electronic equipment on the EU market.

The delegated act, which is a bureaucratic mechanism used by the European Commission to tell EU bodies to update legislation, lists three new security measures that device makers must incorporate in the design of their products in order to be allowed to sell products in the EU.

Read More on The Record

Even More in the press release

More #News

- Here's the FBI's Internal Guide for Getting Data from AT&T, T-Mobile, Verizon
- FBI Raids Chinese Point-of-Sale Giant PAX Technology
- US Citizens Sue Company That Processes Billions of Texts For Exposing Their Data
- FCC kicks China Telecom out of United States
- Microsoft warns over uptick in password spraying attacks

- Industry group warns of coordinated DDoS extortion campaign against VoIP providers
- Conti Ransom Gang Starts Selling Access to Victims
- South Korean telco KT suffers nationwide outage after routing error
- Millions of Android users targeted in subscription fraud campaign
- Mozilla blocks malicious add-ons installed by 455K Firefox users
- Money launderers for Russian hacking groups arrested in Ukraine
- German investigators unmask a core member of REvil ransomware gang
- NSA and CISA share guidance on securing 5G cloud infrastructure
- Police arrest criminals behind Norsk Hydro ransomware attack
- Hive ransomware now encrypts Linux and FreeBSD systems
- 'Trojan Source' Bug Threatens the Security of All Code
- Twitter employees required to use security keys after 2020 hack

#Breach Log

- Third-party data breach in Singapore hits healthcare provider
- Workers sent home after ransomware attack on major automotive parts manufacturer
- Hackers steal $130 million from Cream Finance; the company's 3rd hack this year
- Hackers used billing software zero-day to deploy ransomware
- Sensitive data of 400,000 German students exposed by API flaw
- EU investigating leak of private key used to forge Covid passes
- Malicious NPM libraries install ransomware, password stealer
- Iranian gas stations out of service after distribution network hacked
- North Korean state hackers start targeting the IT supply chain

#Patch Time!

- Google fixes 15th and 16th Chrome zero-day this year
- Microsoft finds Shrootless, a macOS bug that lets malware install rootkits
- WordPress plugin bug impacts 1M sites, allows malicious redirects
- All Windows versions impacted by new LPE zero-day vulnerability

#Tech and #Tools

- How to exploit a double free
- Common Threat Matrix for CI/CD Pipeline
- NGINX Custom Snippets CVE-2021-25742
- Spook Ransomware
- From Zero to Domain Admin
- Public Report – WhatsApp End-to-End Encrypted Backups Security Assessment
- Technical Advisory – Apple XAR – Arbitrary File Write (CVE-2021-30833)
- Microsoft Defender ATP adds live response for Linux and macOS

- Cracking WiFi at Scale with One Simple Trick
- FormatFuzzer: a framework for high-efficiency, high-quality generation and parsing of binary inputs
- Anatomy of a Linux Ransomware Attack | LinuxSecurity.com
- Impacket v0.9.24 Released
- Using Kerberos for Authentication Relay Attacks
- Agent 007: Pre-Auth Takeover of Build Pipelines in GoCD

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