kindred

# Security Newsletter

20 April 2020

Subscribe to this newsletter

# Zoom Caught in Cybersecurity Debate — Here's Everything You Need To Know

Over the past few weeks, the use of Zoom video conferencing software has exploded ever since it emerged the platform of choice to host everything from cabinet meetings to yoga classes amidst the ongoing coronavirus outbreak and work from home became the new normal.

Zoom's rapid sudden ascendance as a critical communications service has led to it drowning in a sea of privacy and security flaws. But is Zoom a malware? As the Guardian reported, some experts believe so. But no, Zoom is not malware. Rather, it's a piece of legitimate software that's, unfortunately, just full of security vulnerabilities and we're just now getting to know about it as the app was never scrutinized this thoroughly before

To give credit where it's due, Zoom largely responded to these disclosures swiftly and transparently, and it has already patched a number of issues highlighted by the security community.

Read More

# Gambling company to set aside $30 million to deal with cyber-attack fallout

Online betting company SBTech will have to place $30 million in escrow as insurance for covering the fallout from a cybersecurity incident that took place last month. The company agreed to do so as part of re-negotiated acquisition terms with Diamond Eagle Acquisition Corporation (DEAC), a blank-check company that acquired SBTech and rival platform DraftKings and is planning on merging the two later this year.

The funds will be used to deal with any expenses caused by a "cybersecurity incident" that took place on March 27. The SBTech was down for almost a week before it resumed service with international partners, but not with its US customers. The company is still waiting for approval from US gambling regulators before returning service to US partners.

Read More

## More #News

- Balancing public safety and privacy during COVID-19: The rise of mass surveillance
- WordPress WooCommerce sites targeted by card swiper attacks
- Google and Apple Plan to Turn Phones into COVID-19 Contact-Tracking Devices
- Microsoft and Google delay online authentication change
- Google reenables FTP support in Chrome due to pandemic
- US Offers $5 Million Reward for N. Korea Hacker Information
- Microsoft Office security updates may break VBA programs, how to fix
- Rapid7 launches AttackerKB, a service for crowdsourcing vulnerability assessments
- Over 500,000 Zoom accounts sold on hacker forums, the dark web
- Google removes 49 Chrome extensions caught stealing crypto-wallet keys
- Some Bug Bounty Programs Are Being Used to Buy Silence
- Discord Turned Into an Account Stealer by Updated Malware
- Microsoft Launches Free Zero Trust Assessment Tool
- 600,000 people affected in email provider breach

- Tech debt of remote working

# #Patch Time!

- Microsoft Issues Patches for 3 Bugs Exploited as Zero-Day in the Wild
- Microsoft Office April security updates fix critical RCE bugs
- Visa urges merchants to migrate e-commerce sites to Magento 2.x
- Microsoft delays end of support for older Windows, software versions
- Adobe Patches Flaws in ColdFusion, After Effects, Digital Editions
- Microsoft Patch Tuesday, April 2020 Edition
- Firefox gets fixes for two zero-days exploited in the wild
- 80% of all exposed Exchange servers still unpatched for critical flaw
- Google Patches Critical RCE Vulnerabilities in Android's System Component

# #Tech and #Tools

- PEASS - Privilege Escalation Awesome Scripts SUITE
- JSON Web Token Validation Bypass in Auth0 Authentication API
- Over 700 Malicious Typosquatted Libraries Found On RubyGems Repository
- Osquery Handout – Query Performance
- Breaking LastPass: Instant Unlock of the Password Vault
- Maza ad blocking - Like Pi-hole but local and using your operating system
- The Sandboxie Windows sandbox isolation tool is now open-source!
- New Stealth Magecart Attack Bypasses Payment Services Using Iframes
- A Quick Look at the Confidentiality of Zoom Meetings
- The ATT&CK Rainbow of Tactics
- Bypassing AV Detections: The Dumb Way (Part 1)
- Universally Evading Sysmon and ETW
- COVID-19 Free Autopsy Training
- XSSI - Exploiting the unexploitable
- Building Secure & Reliable Systems - PDF eBook
- VulnFanatic: Binary Ninja plugin for vulnerability research
- Targeting a macOS Application? Update Your Path Traversal Lists
- Building a Splunk Dashboard for pfSense
- Pwndrop - Self-hosting Your Red Team Payloads
- RedELK – Achieving operational oversight
- ThreatMapper: Identify vulnerabilities in running containers, images, hosts and repositories

This content was created by Kindred Group Security. Please share if you enjoyed!

## Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us