Security Newsletter

3 August 2020

Subscribe to this newsletter

Garmin confirms ransomware attack

Garmin broke its silence Monday, acknowledging that a hack attack that encrypted several of its systems last week led to outages that affected several of the company's fitness and aviation products along with knocking its homepage and customer service centers offline, confirming a ransomware attack. Last week, Garmin suffered a worldwide outage that affected their Garmin Connect, Strava, inReach, and flyGarmin services.

It is common for companies not to mention the ransomware family used in an attack while law enforcement is conducting an investigation.The WastedLocker Ransomware is attributed to the Evil Corp cybercrime group who is best known for their use of the Dridex banking and downloader trojan in hacking operations. After the indictment of Evil Corp members by the USA, the hacking group restructured their tactics and techniques to include a new ransomware called WastedLocker that is used to target and extort enterprise organizations.

Garmin reiterated that it doesn't believe hackers exfiltrated any data from its network.

Read More on BleepingComputer

Even More on BankInfoSecurity

Zoom Bug Allowed Snoopers Crack Private Meeting Passwords in Minutes

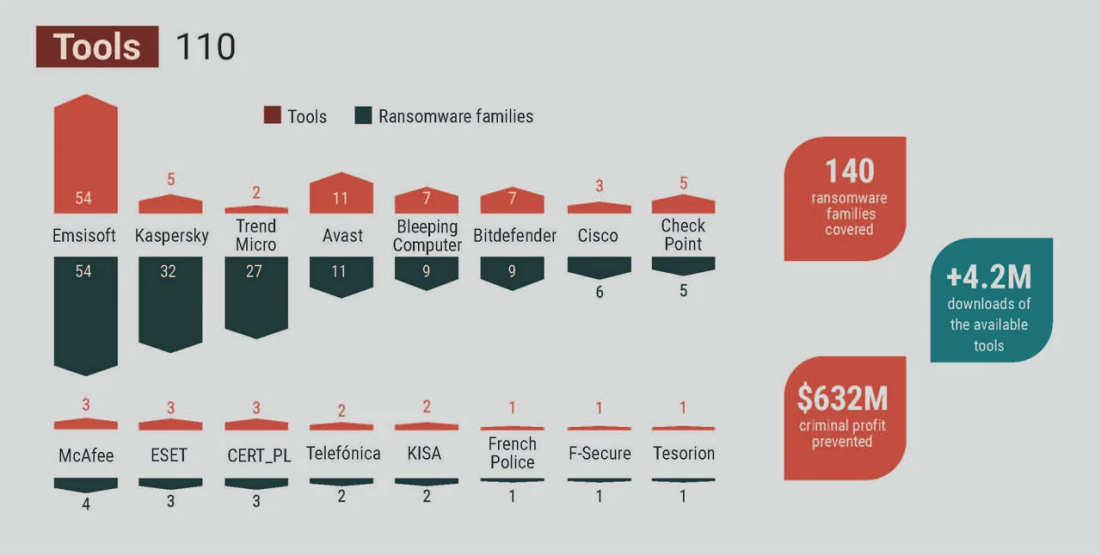
Popular video conferencing app Zoom recently fixed a new security flaw that could have allowed potential attackers to crack the numeric passcode used to secure private meetings on the platform and snoop on participants. Zoom meetings are by default protected by a six-digit numeric password, but the lack of rate limiting enabled "an attacker to attempt all 1 million passwords in a matter of minutes and gain access to other people's private (password protected) Zoom meetings."

It's worth noting that Zoom began requiring a passcode for all meetings back in April as a preventive measure to combat Zoom-bombing attacks, which refers to the act of disrupting and hijacking Zoom meetings uninvited to share obscene and racist content.

The researcher also found that the same procedure could be repeated even with scheduled meetings, which have the option to override the default passcode with a longer alphanumeric variant, and run it against a list of top 10 million passwords to brute-force a login. Following the findings, Zoom took the web client offline to mitigate the issues on April 2 before issuing a fix a week later. Just earlier this month, the company addressed a zero-day vulnerability in its Windows app that could allow an attacker to execute arbitrary code on a victim's computer running Windows 7 or older.

Read More on TheHackerNews

No More Ransom turns 4: Saves $632 million in ransomware payments



The No More Ransom Project celebrates its fourth anniversary today after helping over 4.2 million visitors recover from a ransomware infection and saving an estimated $632 million in ransom payments. Over the past four years, The No More Ransom project estimates that they have saved $632 million in ransom payments through its partners' cooperation and the decryptors that were released.

No More Ransom was created in 2016 through an alliance between Europol's European Cybercrime Centre, the National High Tech Crime Unit of the Netherlands' police, McAfee, and Kaspersky to battle ransomware and provide free decryption services and support to victims.

The amount of money saved is probably far more significant as it is common for other sites to host partner's decryptors, which would not allow the Project to keep track of their usage. Furthermore, as most decryptors do not include telemetry, they may have been used in far higher amounts than we know.

Read More on BleepingComputer

More #News

- Hacker gang behind Garmin attack doesn't have a history of stealing user data
- Critical GRUB2 Bootloader Bug Affects Billions of Linux and Windows Systems
- 'Keeper' Group Targeted Payment Card Data on 570 Sites
- Consumer VPNs: You May Be Fine Without
- The IRS asks tax professionals to enable multi-factor authentication
- T-Mobile announces free Scam Shield robocall and scam protection
- Magento adds 2FA to protect against card skimming attacks
- OkCupid Dating App Flaws Could've Let Hackers Read Your Private Messages
- Industrial VPN Flaws Could Let Attackers Target Critical Infrastructures
- What is Privileged Access Management (PAM)?

- Microsoft Double Key Encryption enters public preview
- Microsoft 365 adds endpoint data leak protection in public preview
- 'Crypto' Scammers Weren't the First to Crack Twitter
- CouchSurfing investigates data breach after 17m user records appear on hacking forum
- Google adds security enhancements to Gmail, Meet and Chat
- Apple sued for not taking action against iTunes gift card scams
- Source code from dozens of companies leaked online
- The Hacker Battle for Home Routers
- Netflix credential phishing hides behind working CAPTCHA
- Why security professionals are facing more work stress
- Linux Malware Targeting Docker Servers With Exposed APIs
- How to add fingerprint authentication to your Windows 10 computer
- FBI warns of new DDoS attack vectors: CoAP, WS-DD, ARMS, and Jenkins

#Patch Time!

- Adobe issues emergency fixes for critical vulnerabilities in Photoshop, Bridge, Prelude
- Critical Wordpress plugin bug lets hackers take over hosting account
- PoC exploits released for SAP Recon vulnerabilities, patch now!
- Cisco releases security fixes for critical VPN, router vulnerabilities
- Firefox 79 is out – it's a double-update month so patch now!
- Magento gets security updates for severe code execution bugs
- Critical SharePoint flaw dissected, RCE details now available
- ASUS routers could be reflashed with malware – patch now!
- 5 severe D-Link router vulnerabilities disclosed, patch now
- Multiple Tor security issues disclosed, more to come
- Here's Why Credit Card Fraud is Still a Thing
- 8 Tips for Crafting Ransomware Defenses and Responses
- Zoom patches zero–day flaw in Windows client

#Tech and #Tools

- Python Malware On The Rise
- Reducing TLS Certificate Lifespans to 398 Days
- HoneyPoC: The fallout data after I trolled the Internet...
- The Story of my first "Incident Response"
- Kubernetes Vulnerability Puts Clusters at Risk of Takeover (CVE-2020-8558)
- There's a Hole in the Boot
- SkyArk: detects shadow admin accounts in AWS and Azure environments
- OPNsense® 20.7 "Legendary Lion" released
- Pentesting User Interfaces: Tips to Phish Chrome, Outlook, or Thunderbird User
- Protecting Your Serverless Solution
- OWASP TOP 10 interractive training
- All Your SPF Belong to us: Exploring Trust Relationships Through Global Scale SPF Mining
- What's wrong with Cyber Threat Intelligence

- Sentinel ATT&CK: leverages Sysmon and MITRE ATT&CK on Azure Sentinel
- “EvilQuest” Rolls Ransomware, Spyware & Data Theft Into One
- Reversing and Evading EDRs: Part 1
- Top 16 Active Directory Vulnerabilities
- TrustJack - A UAC bypass based on Trusted folder abuse
- Sysmon Tools
- Bypassing AV (Windows Defender) … Cat vs. Mouse
- Zoom Security Exploit – Cracking private meeting passwords
- Offensive Security Acquires Cybersecurity Training Project VulnHub

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