kindred

Security Newsletter

16 November 2020

Subscribe to this newsletter

FTC Settlement With Zoom Sets Security Requirements

As part of a settlement of allegations that Zoom "engaged in a series of deceptive and unfair practices that undermined the security of its users," the U.S. Federal Trade Commission is requiring video conferencing provider to implement and maintain a comprehensive security program within the next 60 days. The 17-page agreement announced Monday comes after allegations that Zoom did not maintain a high level of cybersecurity and misled its customers concerning the level of encryption provided for meetings, saying it was AES 256 when it was actually AES 128.

The FTC settlement describes the steps Zoom must take, including:

- Assess and document on an annual basis any potential internal and external security risks and develop ways to safeguard against such risks;
- Implement a vulnerability management program;
- Deploy safeguards such as multifactor authentication to protect against unauthorized access to its network, institute data deletion controls and take steps to prevent the use of known compromised user credentials;
- Require Zoom personnel to review any software updates for security flaws and ensure the updates will not hamper third-party security features.

Although no financial penalties were issued with the settlement, the FTC says any future violations could cost Zoom up to $43,280 for each.

As part of the New York settlement, Zoom agreed to implement "reasonable encryption and security protocols," for customer and corporate data. This includes the use of end-to-end encryption for all data as well as deploying industry-standard AES-256 encryption.

Read More on BankInfoSecurity

New ModPipe Point of Sale (POS) Malware Targeting Restaurants, Hotels

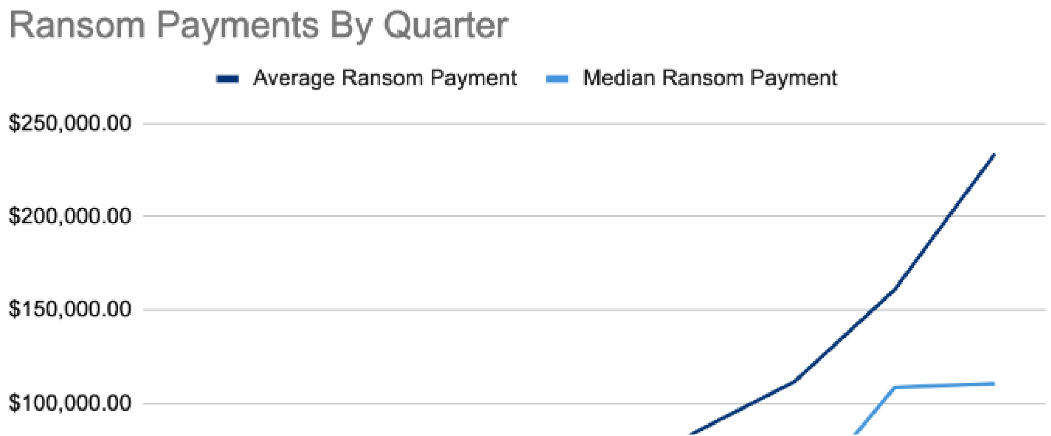
Cybersecurity researchers today disclosed a new kind of modular backdoor that targets point-of-sale (POS) restaurant management software from Oracle in an attempt to pilfer sensitive payment information stored in the devices. The backdoor — dubbed "ModPipe" — impacts Oracle MICROS Restaurant Enterprise Series (RES) 3700 POS systems, a widely used software suite in restaurants and hospitality establishments to efficiently handle POS, inventory, and labor management. A majority of the identified targets are primarily located in the US.

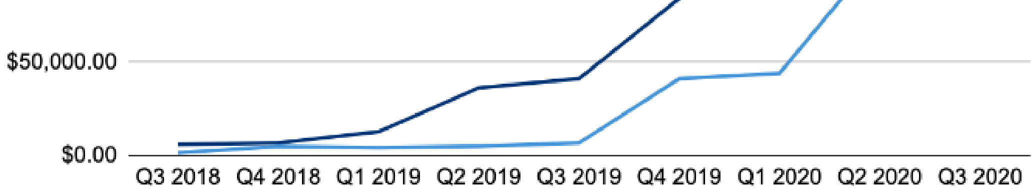
Businesses in the hospitality sector that are using the RES 3700 POS are advised to update to the latest version of the software as well as use devices that run updated versions of the underlying operating system.

Read More on TheHackerNews

Even More on BleepingComputer

Ransomware Demands continue to rise as Data Exfiltration becomes common





COVEWARE

The Coveware Quarterly Ransomware Report describes ransomware incident response trends during Q3 of 2020. Ransomware groups continue to leverage data exfiltration as a tactic, though trust that stolen data will be deleted is eroding as defaults become more frequent when exfiltrated data is made public despite the victim paying.

The average ransom payment increased to $233,817 in Q3 of 2020, up 31% from Q2. The median payment in Q3 rose slightly from $108,597 to $110,532, reflecting how large, big game payments continue to drag the averages up. The disequilibrium within the cyber extortion industry was evident when attackers discovered that the same tactics, techniques, and procedures (TTPs) that work on a 500 person company can work on a 50,000 person company and the potential payoff is substantially higher. The dramatic increase in ransom amounts may imply a higher degree of sophistication as attackers go upmarket, but Coveware does not believe that the attacks are more sophisticated.

The biggest change over the past 6 quarters is threat actors now realize that their tactics scale to much larger enterprises without much of an increase in their own operating costs. The profit margins are extremely high and the risk is low. This problem will continue to get worse until pressure is applied to the unit economics of this illicit industry. It is also possible that the influx of remote and work-from-home setups using RDP and other remote technologies allowed threat actors to leverage attack vectors that previously didn't exist.

Almost 50% of ransomware cases included the threat to release exfiltrated data along with encrypted data. The threat to release exfiltrated data was used as a monetization conversion kicker. Previously, when a victim of ransomware had adequate backups, they would just restore and go on with life; there was zero reason to even engage with the threat actor. Now, when a threat actor steals data, a company with perfectly restorable backups is often compelled to at least engage with the threat actor to determine what data was taken.

Downtime is still the most dangerous aspect of a ransomware attack, and one of the reasons data exfiltration should not present as much of a challenge to victims as business interruption. In Q3 of 2020, the average firm experienced roughly 19 days of downtime. Downtime can range on a spectrum from having a business be at a total standstill, to being just mildly affected by non-available machines.

Read More on Coveware blog

The State of Ransomware in 2020

Data-Exfiltrating Ransomware Gangs Pedal False Promises

More #News

- Microsoft urges users to stop using phone-based multi-factor authentication
- Fake Microsoft Teams updates lead to Cobalt Strike deployment
- DDoS attacks: How to combat the latest tactics
- Ubuntu's Gnome desktop could be tricked into giving root access
- New Platypus attack can steal data from Intel CPUs
- Why you should keep your Netflix password to yourself
- MISSIONS — The Next Level of Interactive Developer Security Training
- CyberEdBoard CISO Community Debuts
- Probing Marriott's Mega-Breach: 9 Cybersecurity Takeaways

#Breach log

- Luxottica data breach exposes 820K EyeMed, LensCrafters patients
- Laptop maker Compal hit by ransomware, $17 million demanded
- Data on millions of hotel guests exposed in cloud storage leak
- Info of 27.7 million Texas drivers exposed in Vertafore data breach
- The North Face resets passwords after credential stuffing attack
- How a Game Developer Leaked 46 Million Accounts
- Popular stock photo service hit by data breach, 8.3M records for sale
- Steelcase furniture giant down for 2 weeks after ransomware attack

#Patch Time!

- Vulnerability Descriptions in the New Version of the Security Update Guide
- Patch Tuesday, November 2020 Edition
- Apple patches three actively exploited zero–day flaws in iOS
- WordPress plugin bugs can let attackers hijack up to 100K sites
- Recent WebLogic Vulnerability Likely Exploited by Ransomware Operators
- Adobe releases security update for Adobe Reader for Android
- Windows 10 Intel microcode released to fix new CPU security bugs
- Office November security updates fix remote code execution bugs
- Two New Chrome 0-Days Under Active Attacks – Update Your Browser

#Tech and #Tools

- Kubernetes Security Is Not Container Security
- Osctrl: TLS endpoint for OsQuery
- The Internet is Getting Safer: Fall 2020 RPKI Update
- How to get root on Ubuntu 20.04 by pretending nobody's /homeut4
- A new skimmer uses websockets and a fake credit card form to steal sensitive data

- Fixing leaky logs: how to find a bug and ensure it never returns
- Red Team KubeCTL Cheat Sheet
- Pigasus: Intrusion Detection and Prevention System using FPGA fto achieve 100GBPS
- Sharing the Myth
- Npm package caught stealing sensitive Discord and browser files
- Open Source project Security Scorecards
- Damn-Vulnerable-Bank

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