Zoom - A trial by Fire

With a good part of the world working from home due to Covid-19, the need for a good and simple video conference solution was urgent. Zoom being intuitive and powerful enough to handle the onslaught of users, filled that need.

As millions of users flooded to Zoom so did the hackers and security researchers. They discovered an application riddled with vulnerabilities and an organization more interested in new users than fixing its problems. Just how many Zoom-calls routed trough China where intercepted, we may never know.

Timeline of vulnerabilities

- **July 31**

  British security researcher Tom Anthony learns he can break into any Zoom meeting in about half an hour. The meetings were protected by a 6-digit pin, but did not limit the number of login attempts a user could make.

  Limiting login attempts is standard practice in any security solution; this begs the question of Zoom ever took security seriously?

  Status: Fixed

- **July 10**

  An unnamed security researcher found a flaw in the Zoom client for Windows; the flaw would let a hacker take over any PC running Windows 7 or earlier.

  Status: Fixed

- **June 17**

  Zoom gives in to critics and offers end-to-end encryption to everyone, something that should have been there from the start.

  Status: Unknown

- **June 12**

  Zoom caves into the Chinese government and temporarily suspends the accounts of three Chinese dissidents. Any organization that suppresses free speech with censorship should not be trusted.

- **June 4**

  A Cisco information-security research firm, Talos, found two serious flaws in the Zoom client.

  The first flaw would let an attacker post a specially created GIF that would force the installation of malware on the victim's computer.

  The second flaw would let an attacker send malware in a compressed file to a Zoom-user; it would automatically open and infect the computer.

  Status: Fixed

- **May 21**

  Trend Micro researchers found two instances of corrupted Zoom installers. The first opens up a backdoor to the victim's PC letting hackers in. The second spies on the PC's owner with screenshots, keylogging, and webcam hijacking; it also drafts the PC into the Devil Shadow botnet.

  Status: Unknown

- **May 18**

  An unexplained outage rendered the service unavailable to thousands of users in the US and UK.

  Status: Unknown

- **May 12**

  Israeli security firm Check Point discovered that cybercriminals might have registred hundreds of Zoom-related website addresses in the past few weeks. These websites are used in phishing attacks, masquerading as legitimate Zoom-sites, and harvesting users usernames and passwords.

  Status: Unknown

- **May 8**

  Zoom bans free users from tech-support calls. Being overwhelmed with calls, Zoom opted to ban free users from support rather than hire more tech-support staffers.

- **May 8**

  New York State Attorney General Letitia James' office reached an agreement with Zoom following an investigation into their security and privacy practices. Basically, they forced Zoom to adhere to longstanding policies and security practices that are standard at many other online companies. Why this was not already standard policy at Zoom is beyond supprising.

- **May 7**

  Zoom buys the small New York City startup Keybase in a bid to implement true end-to-end encryption for Zoom meetings quickly. In March, Zoom had to admit that their "end-to-end" encryption was a lie. Zoom was always able to access the contents of the meetings.

- **April 30**

  Zoom stock shares dipped nearly 9% Thursday, April 30, the day the company joined the NASDAQ 100 stock index.

  The reason being Zoom once again lied, saying it had a peak of 300 million daily users in a blog post. In reality, they had a peak of 300 million daily "participants," not unique users. One user can attend several meetings on the same day.

- **April 29**

  Not surprisingly, the Departement of Homeland Security warned the US government that Zoom is a prime target for Chinese intelligence operatives, according to ABC News.

  "China's access to Zoom servers makes Beijing uniquely positioned to target US public and private sector users," ABC News quoted the DHS report as stating.

- **April 28**

  A new Zoom phishing scam sends an email that looks like it's from your employer's HR department, inviting you to join a Zoom meeting. The link to join the meeting takes you to a real-looking Zoom login page that harvests your login credentials when entered.

- **April 17**

  A security researcher, Phil Guimond, noticed that you could easily find recorded Zoom meetings stored in Zoom cloud servers. The structure of the URLs used was so easily predictable that Guimond could build a simple tool that automatically found them.

  Status: Mitigated with additional obstacles against attack, not fixed

- **April 15**

  Hackers are trying to sell two "zero-day" exploits for Zoom to the highest bidder, Vice reports.

  One exploit would apparently let the attacker get full control over the target computer. The other was a less severe MacOS exploit.

Open and unresolved issues

- **Accounts for sale**

  Over 500,000 Zoom accounts up for sale on criminal marketplaces. Hackers used login credentials from previous data breaches to unlock Zoom accounts. The accounts that were breached used the same password across multiple services.

- **2,300 sets of Zoom login credentials found online**

  IngSights researchers found that 2,300 Zooom login credentials where being shared in an online criminal forum.

- **Zero-Day exploits**

  According to Vice, security researchers know of several Zoom "zero-day" exploits for Zoom.

- **Zoom installer bundled with cryptocurrency-mining malware**

  Trend Micro researchers found a version of the Zoom installer that also installs malware that mines cryptocurrency on the user's computer.

- **Zoom lies about its encryption algorithm**

  Zoom says it's using AES-256 encryption for video and audio being sent from Zoom servers to Zoom clients. But in reality, Citizen lab reports, they are using a weaker in-house implementation of the AES-128 algorithm that's poorly coded.

- **Zoom software can easily be corrupted**

  A British computer student calling himself "Lloyd" wrote in a blog post that Zooms anti-tampering mechanisms can easily be thwarted. In other words, malware already presents on a computer could use Zoom's own anti-tampering mechanism to tamper with Zoom. This is yet another example of Zoom's poor coding and security practices.

- **Zoom Bombing**

  A Zoom meeting can be "bombed" by anyone if they know the meeting number. Bombing is when uninvited users connect to the meeting and use the file-sharing function to post shocking images, or make annoying sounds in the audio. Even the FBI warned about it.

- **Leaks of profile photos and email addresses**

  Everyone sharing the same email domain were automatically put in the same "company" folder, letting everyone see each other's information.

  Dutch Zoom users who used the same ISP where surprised when they where grouped together in the same "company" folder as complete strangers, sharing email, photos and user names.

- **Personal data sold to advertisers**

  Consumer Reports privacy experts analyzed Zoom's privacy policy and found that it gave Zoom the right to use Zoom users' personal data and share it with third-party marketers.

  After a blog post by Consumer Reports, Zoom hastily rewrote its privacy policy, removing the most disturbing passages.

- **It's possible to "war drive" to locate open Zoom meetings**

  By rapidly cycling trough possible Zoom meeting IDs trough Tor, a security researcher was able to find open Zoom meetings. The tool was able to find about 100 open Zoom meetings every hour.

- **Zoom chats don't stay private**

  Two Twitter users found a flaw in Zoom's private message function. When you are in a meeting and open a private chat with other users, the conversation will be visible in the end-of-meeting transcript.

Original post can be found at our homepage:
https://www.bitidentify.com/blog/zoom-a-trial-by-fire/