Red Cross blames hack on Zoho vulnerability, suspects APT attack

therecord.media/red-cross-blames-hack-on-zoho-vulnerability-suspects-apt-attack/

February 16, 2022

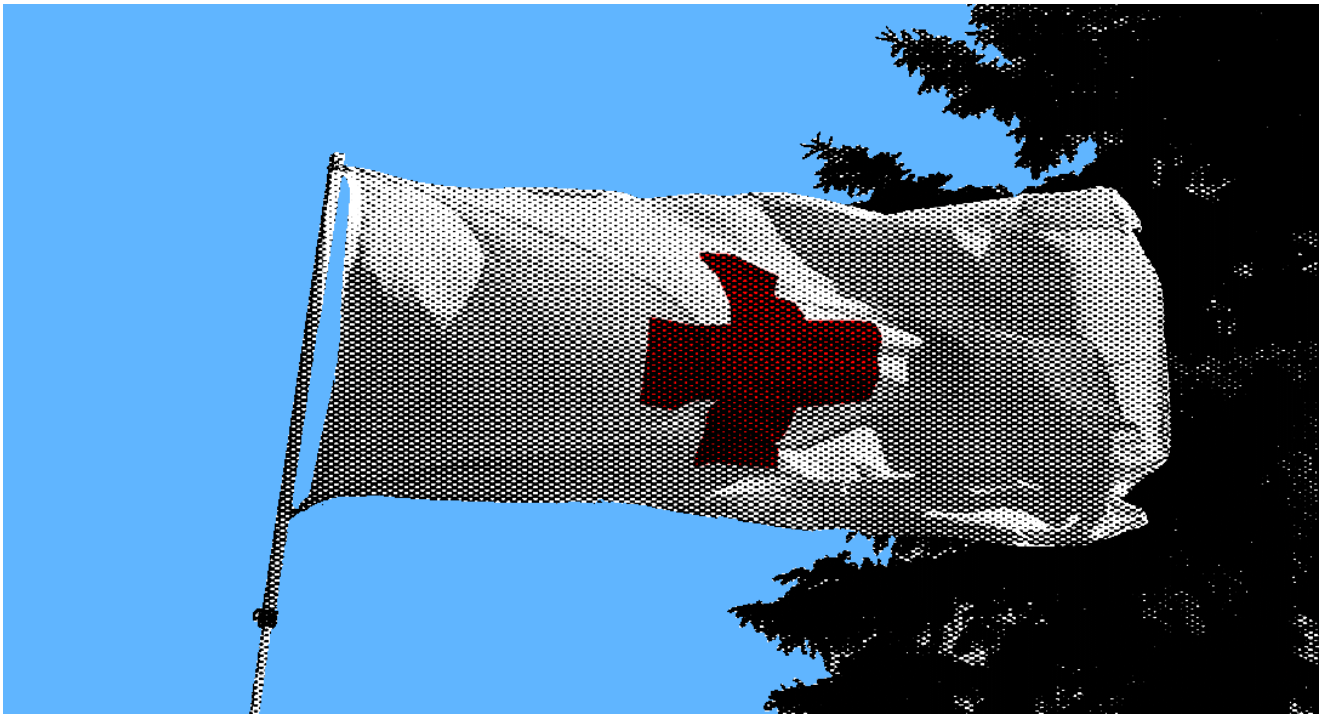

Image: Kevin Paes, The Record

After making headlines last month, additional details are emerging about the hack of the Red Cross organization and the possibility that the attack was carried out by a state-sponsored hacking group.

In an update to its original breach disclosure, the Red Cross said today that while the breach was found and disclosed on January 18, the actual intrusion took place last year, on November 9.

The Red Cross said the hackers used an exploit for the CVE-2021-40539 vulnerability to gain an initial foothold inside their network.

Impacting the Zoho ManageEngine ADSelfService Plus, a password management and single sign-on (SSO) solution from Indian company Zoho, the Red Cross said this vulnerability allowed attackers to bypass authentication, place web shells on its servers, and then move laterally across its network and compromise administrator credentials.

The intruders used this access to compromise a Red Cross program called **Restoring Family Links**, which is a web-based system used by Red Cross volunteers to reunite family members separated by conflict, disaster, or migration.

When it discovered the breach last month, the Red Cross begged the hackers not to leak any data they stole from this program, as it would have put “highly vulnerable people” at even greater risk.

The details of more than 515,000 persons are believed to have been collected in the hack, including data such as names, locations, and contact information.

Red Cross suspects state-sponsored group

But while initially it was not known who was behind the attack, the Red Cross said today that the hacking tools used in the breach are typically used by “advanced persistent threat groups,” a term typically used to describe state-sponsored hacking groups. We quote:

- The attackers used a very specific set of advanced hacking tools designed for offensive security. These tools are primarily used by advanced persistent threat* groups, are not available publicly and therefore out of reach to other actors.
- The attackers used sophisticated obfuscation techniques to hide and protect their malicious programs. This requires a high level of skills only available to a limited number of actors.
- We determined the attack to be targeted because the attackers created a piece of code designed purely for execution on the targeted ICRC servers. The tools used by the attacker explicitly referred to a unique identifier on the targeted servers (its MAC address).
- The anti-malware tools we had installed on the targeted servers were active and did detect and block some of the files used by the attackers. But most of the malicious files deployed were specifically crafted to bypass our anti-malware solutions, and it was only when we installed advanced endpoint detection and response (EDR) agents as part of our planned enhancement programme that this intrusion was detected.

The Red Cross said the attacker’s advanced offensive tools are what prevented it from detecting the breach sooner, with the attackers spending 70 days inside its network before discovery.

Despite pinning the attack on a suspected state-sponsored hacking group, the Red Cross did not formally attribute the attack to any organization just yet.

Nevertheless, a Palo Alto Networks report from November 2021 linked exploitation of the same Zoho vulnerability to a Chinese state-sponsored group known as APT27.

A week after the Red Cross disclosed its breach in January 2022, the German government also published a security alert warning local companies and state agencies about similar APT27 attacks leveraging the same Zogo vulnerability, which may provide additional clues about who may have been behind the Red Cross compromise.

The Red Cross hack turned a lot of heads last month and even made the US State Department to publish a rare statement on the matter, calling the incident “a dangerous development.”

“To ensure states and vulnerable people can continue to trust and rely on the Red Cross and Red Crescent Movement for the help they need, states should join the ICRC in raising the alarm about this breach,” the agency said last month.

Tags

- APT
- APT27
- China
- nation-state
- Red Cross
- vulnerability
- Zoho

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.