Ryan Jackson
12/1/23
CS462

Cyber Attack on The International Committee of The Red Cross

The International Committee of The Red Cross experienced a major cybersecurity attack. The attack compromised a mass amount of personal data of over 515,000 people along with the login information of around 2,000 ICRC staff and volunteers. This attack occurred in January of 2022. The data is said to have originated from around 60 Red Cross affiliates. The incident left the International Committee of the Red Cross (ICRC) with a massive problem and had a large impact on its operations.

One major question is “Who was behind the attack?” Since the incident, The Red Cross has given an update on the matter and still could not be certain about who was behind the attack. According to an update given in June 2022, the Red Cross has not made any contact with the hackers. The perpetrators utilized various tools and tactics in order to fly under the radar. They acted as typical users on the network as well as administrators to access confidential data. The Red Cross found that the attackers had maintained access to the servers for months.

As stated prior, the attack was said to have taken place in January of 2022, however, the initial breach was in November of 2021. The attackers used tools and tactics that were specifically made for this specific attack. The attack displayed a level of sophistication that is not typically found in your everyday generic attack. The attackers crafted their malicious files in order to bypass anti-malware. They used code specifically to target ICRC servers. As stated earlier, there were a couple of months of the presence of hackers before the actual attack. Before or during this time, they could have tailored

the attack to the ICRC network rather than a generic attack. Specific MAC addresses were targeted, so it is confirmed that there must have been plenty of recon in those months. Essentially, the hackers were able to enter the network by exploiting an unpatched critical vulnerability. This allows for malicious activities to take place internally. Again, this was made easier by disguising themselves as admins, which would render encryption useless. Offensive security tools allow for this to occur.

There is a lot of nuance in cybercrime. The intentions of a hacker are not always negative. There are different types of hackers. This all depends on motive. There are white hat hackers and black hat hackers. A white hat hacker is an ethical hacker. They find the loopholes that may be present in a system and report back to the organization in question to rectify the system's errors. Penetration testers also fall under this qualification. These are individuals who test and find vulnerabilities, however, in the hands of malicious hackers, we have seen the repercussions.

The director-general of the ICRC, Robert Mardini, has shown his concern and mentioned the potential risks associated with a breach such as this one. The main risk being the possibility of doxxing or the sharing/leakage of personal and confidential information. Mardini stated "An attack on the data of people who are missing makes the anguish and suffering for families even more difficult to endure. We are all appalled and perplexed that this humanitarian information would be targeted and compromised" (ICRC, 2022). The ICRC plays an important role in reuniting families that have been separated due to conflict, and other external factors. Programs that deal with such instances were then forced to the shutdown. The Red Cross also made sure to inform those who were affected about the data breach. This consisted of public

announcements, phone calls, physical travel, and more. The ICRC made sure to give information on the matter and how to protect themselves. Assuming that those affected were not connected, they said to contact the local Red Cross. It is mentioned to regularly monitor your financials for any suspicious activities. If anything is found, make sure to report it right away. Along with that, make sure to change passwords and make them strong passwords. Two-factor authentication is probably ideal as it will add another layer of security. They also developed a question and answers page for those who have been affected. They made it a point to get individuals to familiarize themselves with the Q&A article provided. They have made sure to let the public know that this is not something to be taken lightly.

At this point in time, of course, their systems are now back online and changes have been made. There is a new two-factor authentication process. They also made sure to conduct penetration tests for good measure. As a matter of fact, the systems went back online only after successfully running penetration tests. There also must be prevention methods for the future, most of which are dealing with maintenance. There should be regularly scheduled patchings. Update the systems to reduce potential vulnerabilities. Along with that, establish regularly scheduled penetration tests and risk assessments. Not only is this simply good practice, but it allows for a better understanding of new patches and potential vulnerabilities. On the organization's side of things, there are plenty of guidelines in place for ethical hacking. The ethical hacker must make sure to seek authorization from the organization in question. They must completely define the scope of the process. What systems/networks/etc are being tested and dealt with? The ICRC has already stated that they are taking some of these

steps. Policies are crucial and ensure protection. Organizations should establish limitations and clearly state what assets, products, etc are to be “hacked.” All parties must be on the same page. Reporting and documentation are arguably the most important part of the process. All findings should be reported. Policymakers have addressed the hacking with the Computer Fraud and Abuse Act (CFAA), enacted in 1986, which prohibits intentionally accessing a computer without authorization. Federal law states that first-time offenders who violate the CFAA may be punished with fines up to $5,000 per crime, imprisonment ranging from 1 to 10 years, or potentially a combination of the two.

The Red Cross has made it clear that they are looking to establish stability and trust once again. Practices such as ethical hacking can lead to the building of trust and reputation of a company, network, etc. Customers, clients, volunteers, and stakeholders look to have or establish trust and look for a positive and stable company reputation. Interaction between an ethical hacker and an organization needs to maintain a level of trust. Ethical hackers could undergo questionable means and tactics. Their actions could result in a question of their professional ethics. It could be argued that ethical hackers partake in questionable activities, however, if they are ethical, the rationale would likely be justified in some way, shape, or form. But the keyword of that statement is “If.” Blurred lines are always something to keep in mind. Customers, clients, and stakeholders may prioritize data/network protection over everything and this could serve as a selling point.

In conclusion, The International Committee of The Red Cross experienced a very drastic wake-up call. The Offensive security tools, administrator privileges, and

anti-malware bypassing caused this unfortunate incident. Attacks such as this are a result of a very well-orchestrated plan and plenty of time. Steps were taken to remedy the issue. As mentioned earlier, the Red Cross informed the individuals who were affected. The company hoped to use this attack on personal data as a catalyst for change. It will serve as a data point and a reminder to continue to strengthen security.

Ryan Jackson
12/1/23
CS462

References

International Committee of the Red Cross. (2023, January 17). *Cyber attack on ICRC: What we know*. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

Kost, E. (2023, March 02). *How did Red Cross get hacked?: Upguard*. RSS. https://www.upguard.com/blog/how-did-red-cross-get-hacked

McLaughlin, J. (2022, January 20). *Cyberattack on Red Cross compromised sensitive data on over 515,000 vulnerable people*. NPR. https://www.npr.org/2022/01/20/1074405423/red-cross-cyberattack

Constantinescu, V. (2022, February 17). *State hackers breach Red Cross networks with Zoho Bug, ICRC says*. Hot for Security. https://www.bitdefender.com/blog/hotforsecurity/state-hackers-breach-red-cross-networks-with-zoho-bug-icrc-says/