INSIDE DEVELOPMENT | FINANCIAL TECHNOLOGY

New security concerns raised for RedRose digital payment systems

*By **Lisa Cornish** // 28 November 2017*

Topics: Innovation & ICT , Türkiye (Turkey) , United Kingdom , Australia

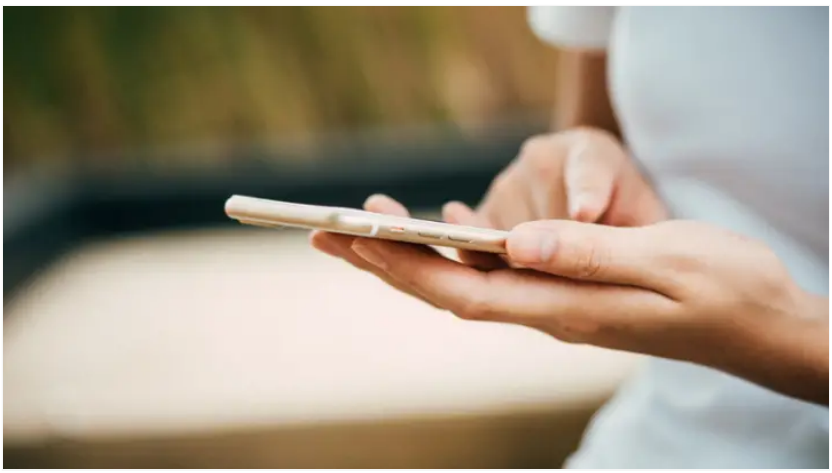

Photo by: Porapak Apichodilok

CANBERRA — Two players in the cash payments sector are squaring off after one company penetrated the other's cyber security, accessing beneficiary records of a leading NGO, and revealing what they claim is a serious security flaw.

Emerson Tan, chief executive officer for Mautinoa Technologies — a self-acknowledged emerging competitor in the digital payments space — informed Devex last week that his organization had found a lack of security in an active RedRose deployment managed by Catholic Relief Services in West Africa. Through the security breach, they could access personal, economic, geographic, and photographic information about beneficiaries, which could be downloaded for offline analysis.

In response, RedRose denied that any systematic breach took place and said it was the victim of industrial espionage by its competitor. The organization said that their systems are secure.

“The unauthorized access was not sanctioned by our client or RedRose and was unlawful, unethical, reckless and done with malicious intent,” a RedRose statement, supplied through Timothy Blank from Dechert LLP, said.

But experts warn the hole underscores concerns that the humanitarian and development sector are rushing into digital cash payment systems space, without taking seriously security.

“This is about as bad as it gets for data loss and system compromise, and anyone using RedRose products should be taking immediate action to remediate the exposure,” Seth Hardy, a Toronto based security research expert with four years of experience researching digital attacks against NGOs, told Devex. “This is a major compromise of data.”

How was personal payment and information accessed?

The report by Mautinao Technologies detailed the nature of the information accessed by their staff member that occurred while conducting “competitive research” on RedRose’s Android App ahead of applying for a tender by the Norwegian Refugee Council for the provision of payment solutions.

The report says that while researching, they came across an old Android application package, or APK, for an NGO app that appears never to have gone live. “Our engineers were very surprised to discover that the code was not obfuscated at all, and had all its API endpoints exposed in clear text.” The information needed to identify points to access systems and data from were essentially visible to the public.

The discovery prompted further research producing “very large numbers of extremely vulnerable beneficiaries’ personally identifying data,” said the report. The information was “exposed in plain text with no meaningful security controls.”

In decompiling the application package, Mautinoa Technologies report that it was not obfuscated. “From the package names, it looked like it was not developed by RedRose CPS themselves, but a Turkish outsourcing firm called http://maviucak.com,” the report reads.

Using Charles Proxy, a cross-platform HTTP debugging proxy server application, they identified the backend address the site was trying to access. Attempts to communicate

with the backend resulted in timeout messages. “While using Charles Proxy, we also noticed that the app did not perform certificate pinning, which is a very significant red flag,” the report says. And this encouraged them to look at subdomains of redrosecps.com, finding internal training documentation, internal wiki and API reference. The wiki, which is no longer accessible for public viewing, provided information on the default account name and password for the Android app.

But in discovering the backend to the application for live CRS project based in West Africa, Mautinoa Technologies tested the default username and password — discovering that CRS had not changed it, and that it provided administrator access. “The deployment is live as of 15 November 2017,” the report reads.

GPS data and registration details associated with the deployment — including photographs — were exposed, with the report expressing concern that it appeared possible to administer the entire program from this interface.

Other backends discovered were not accessible using the default username and password, and a script was written to repeatedly attempt to access the backends with invalid passwords. “Of all the backends, only https://redrose2.redrosecps.com had protection against password brute forcing,” the report claims, an important security measure for protecting hacking attempts.

“There is no lockout mechanism, so you can potentially load up a 50 million password file and sequentially try all of them,” Tan explained to Devex. “The systems we investigated did not show any real time protection.”

Mautinoa Technologies then turned their attention to the mobile application.

Modifying the old APK to point to the live CRS deployment backend, they were able to login to the production backend. “Using Charles Proxy, it was possible to capture a login and complete synchronization session,” the report says. “The app downloads all data from the backend upon first startup, and then it mostly works offline.” For the CRS deployment, Tan said tens of thousands of beneficiary records were automatically downloaded in the process.

While the CRS deployment uses DESFire V1 contactless smart cards, which currently have not been broken, the report says accounts on the keys required to provision cards

by CRS were stored in plain text, “allowing for easy cloning of cards, with a little reverse engineering.”

“In addition, all the PIN codes for the smart cards were stored in plain text on the backend,” the report says.

Mautinoa Technologies discovered that updated APK files were downloaded from non-password protected dropbox links, confirmed by Devex, meaning there was no need to reverse engineer a new version of their application.

With a cache of data already accessible, Tan said he and his staff member panicked and ceased activities to report the potential risk to NGOs using the RedRose system.

“We didn’t try accessing further systems or information,” Tan said, adding that his organization deleted all data downloaded during the investigation following requests from CRS. “But we were panicked enough that pin numbers and values needed to create cards were in the clear and there was no way of preventing fraud.”

The response of RedRose

RedRose has downplayed the severity of the attack, chalking it up to little more than corporate sabotage and insisting that its systems were not compromised. RedRose told Devex that the company has “conducted a forensic audit of its platform and is aware that a certain company, apparently acting under false pretences and for its own corporate gain, intentionally and unlawfully accessed a client’s system by inputting a valid username and password, both of which had been compromised.”

They said the credentials have since been deactivated and the unauthorized access is not a system related issue, but a username and password management issue.

“We can confirm that this is an isolated incident which we believe does not pose a risk of harm to our clients or beneficiaries,” RedRose said. “As the Android application is an open source platform, it is widely known to be susceptible to reverse engineering. Accordingly, we do not include personally identifiable information in the application. At all times, our system defenses and safeguards were fully active and operational, and the rogue company therefore failed in its further attempts to unlawfully access other clients’ information.”

Their statement advised that their security systems were robust and in line with industry standards.

“Our system uses Mifare DESFire EV1 cards, which are secure and cannot be cloned due to the additional security measure of unique multi-level security keys for each card. RedRose is also fully compliant with ISO 27001 – IT security risk and management and ISO 9001 Quality Management System. RedRose will be undertaking a full penetration test of its system to review and test its security infrastructure.”

What is the takeaway for NGOs?

After reviewing the report, Hardy, the security expert, explained to Devex that despite the fact that the Android application was old, its ability to still connect to live and active systems was a security issue RedRose needed to address. “Any app changes to fix the security issues would need to be accompanied by fixes to their server software,” Hardy said. “If the old app still works, it's still broken.”

“If a company is advertising secure products, it must have security built in from the very beginning, implemented and tested at every step of the way,” he said. “These problems were found during a simple audit using standard tools and techniques, which implies that security was not a consideration in their development process.”

He continued, “the RedRose compromise seems to be pretty egregious and a systemic problem — it's not a single mistake, it's a lack of security awareness and understanding across all their systems.”

Hardy urged NGOs using RedRose products to take immediate action to remediate the exposure.

Stephen McDonald, co-director of the Centre for Humanitarian Leadership, told Devex that there is a real concern that payment systems and security measures in place among NGOs are severely lacking — and NGOs need to work better and together to provide secure systems for all data and all beneficiaries.

“The thing that really concerns me — it is something I have witnessed myself — is that quite often practices in U.N. agencies and NGOs will be for those involved in program design to go out and seek a vendor without involving expertise around data systems and security,” McDonald told Devex. “Even then, it is not uncommon for systems or

infrastructure people to say that if it is not on their systems, they are unconcerned about it, as it does not impact their systems infrastructure."

And he said it raises security concerns about others systems NGOs are using to collect a range of data, including health information. "As an industry or workforce, we are not asking the questions around data security — and we should have learned these lessons years ago from corporate data breaches," McDonald said. "There is a real risk of failure through ignorance."

Minimization of costs to maximize reach, McDonald said, is often an excuse to look outside the organization for technical support and expertise. But he said NGOs need to question what price should be put on the protection of information associated with people already vulnerable and at risk.

"If we are talking about conflict or contested settings, what price is worth some of these families' data being accessed or manipulated and being targeted, regarded by one party or another in a conflict environment as an enemy?" McDonald asked. "I think there is a real risk that people whose data has been exposed could be at risk of real physical harm. My understanding is that it provides all of the information collected about individual beneficiaries."

There may also be criminal risk, McDonald said, with exposed systems potentially defrauded. "If it is easy enough to access the system and change data with a cash program system, what is to stop somebody with criminal intent of getting into these systems and diverting finances elsewhere?"

McDonald said he was surprised no incidents have been reported yet. "I've been talking to people about this issue about data security and protection for some time," he said. "This comes back to how as the sector we view innovation. Very seldom do we investigate the human factors that need to be looked at in that innovation through questioning security."

McDonald urged the sector to fill the gap in thinking and practice associated with technology and cyber security. He called for investigation into use of common platforms across agencies that they can own collectively or common approaches to data and security standards, saying this happens in a range of other sectors including flight navigation and airport systems.

“We are inadvertently putting the people we support at risk if we don’t,” McDonald said.

Hardy warned that without dedicated security people, or even administrators, NGOs were putting themselves and their beneficiaries at further risk. After all, Mautinoa Technologies entered the CRS backend using a default password — suggesting the most basic human-centered oversight.

“Any time user data is collected, including for legitimate uses like this, an organization is taking on risk,” Hardy said.

CRS stands firm

Tan has denied accusations of malicious intent. The common practice following a data or systems security issue would be to go to the company and report the issue. But Tan said he personally chose to go to the NGOs to “avoid a cover up.” In his explanation, he cited the “public record” of RedRose CEO Jeremy Cole, whose previous organization was embroiled in a corruption scandal.

“Yes we are competitors to RedRose, but at the end of the day that shouldn’t dilute the case that this is terrible,” Tan said. “Our experience in the national security world suggests that people are very vulnerable through these systems — if we can run through it in 45 minutes with the most junior of my staff being able to access systems, then it does not pose much of a challenge to Russians, Syrians, Iranians, and Saudis. Just take your pick.”

The report was supplied to NGOs including CRS, the International Committee of the Red Cross, and Mercy Corps, as well as the Electronic Cash Transfer Learning Action Network to reach a wide network as possible.

Paul Eagle, vice president of marketing and communications with CRS, told Devex that Mautinoa Technologies had provided information on the data access, which they read on Nov. 20. But Eagle assured the “unauthorized access” had occurred in a single program instance in West Africa.

“Since being notified of the security concerns, we have been working with RedRose to ensure that the system is secure and that beneficiary data is safe,” Eagle said.

Within CRS, Eagle explained, RedRose is primarily used for asset transfer — such as a direct distribution or e-voucher. “CRS is working with the RedRose platform in several projects across multiple countries as a project management tool.” And during procurement processes, Eagle explained that CRS sought demonstrable compliance for system security requirements. “We have also worked with local country programs to advise on the security of systems, and we have begun to bake security into the design of our centrally-managed systems.”

Despite the ability of outside parties to have accessed their systems, CRS does not believe there has been prior unauthorized access. “Based on our analysis, there is no risk to beneficiary distributions and vendor payments,” Eagle said. “As a result, we are not considering alternative distribution or payment options at this time.”

What are the risks to other NGO clients?

A range of other current and past NGOs clients using the RedRose system include the ICRC, Mercy Corps, NRC, Oxfam, and Relief International.

DanChurchAid, an existing client, said they were surprised by concerns of RedRose security and contacted RedRose to clarify the matter.

“We have received a response from RedRose answering the alleged security flaws,” Christer Lænkholm, senior humanitarian adviser for cash and markets with DanChurchAid, told Devex.

“We are currently analyzing the RedRose responses and the findings. Our initial conclusion is that Mautinoa Technologies have gained unlawful access to the system, and because they do not have a constructive dialogue with RedRose, there are a number of misunderstandings which could have been cleared. There are however some issues around weak passwords and easy to guess URLs, and we have instructed the system administrators who manage the RedRose platforms in Ethiopia and Lebanon to review user rights and ensure that every user change their password regularly and uses a strong password.”

Lænkholm said his organization is not concerned that there are security risks associated with the RedRose cash payment system, saying there was no sensitive beneficiary data stored on payment cards or android platform, and the card themselves “should be un-hackable and uncloneable according to sector standards.”

“When assessing the alleged security problems with the RedRose system, it is important to understand what RedRose is,” he said. “RedRose is a closed loop fintech voucher system, meaning it has no links to any financial institutions and no financial data about any bank or mobile money accounts exists in the system. ‘Money’ in the system stays within the system. We pay vendors with checks, bank transfers, using our normal financial system.”

An Oxfam spokesperson said they had been made aware of the situation by RedRose. “We take all matters of the data security seriously. We have been told by RedRose that Oxfam’s data has not been affected in this incident. Nevertheless, we have asked the company for a full report and, as a precautionary measure, have temporarily suspended uploading new data. We will take any further steps as appropriate.”

So far, Oxfam have only used the system in two places — the Democratic Republic of Congo and the Gaza Strip — to help distribute assistance to people they support, but they said no Oxfam supporter data is on the system.

“Scheduled training in Bangladesh on using the system this week will continue, but we will not use any real data until the situation has been resolved to our satisfaction,” the Oxfam spokesperson said. “We are unaware of the system being used more widely, but as a precaution, Oxfam GB is informing other affiliates and will recommend steps to mitigate any further risk as necessary.”

Juliette Ebele, a public relations officer with the ICRC, said they have been informed of these alleged security breaches by Mautinoa Technologies and immediately contacted them to obtain more information about the allegations. “The ICRC’s data protection and ICT security experts were immediately informed to follow up with RedRose on this matter,” she said.

“At this stage, the ICRC is finalizing a pilot project using RedRose ONE in three different countries until 15 December, in order to assess the business, technical and privacy options offered by the system, and compare it to other similar solutions currently available on the market.”

“So far, no data or beneficiary using the RedRose ONE solution through the ICRC has been compromised, nor has an ongoing assistance program been suspended, since the RedRose ONE solution was not fully integrated, but used in parallel with other systems already in place. However, should any serious security threat or system fault arise, the

ICRC will immediately suspend the use of RedRose ONE in the final stage of the pilot project," Ebele said.

Ebele said that as the beneficiary and payment data accessed resulted "from Mautinoa's fraudulent use of a standard default password," it underlined the importance of setting highly secure passwords to protect any digital data and activity on individuals.

"Safeguarding the personal data of individuals is an essential aspect of protecting people's lives, their physical and mental integrity, and their dignity — which makes it a matter of fundamental importance for the ICRC, touching all areas of its activity, whether operational or administrative."

ABOUT THE AUTHOR

Lisa Cornish lisa_cornish

Lisa Cornish is a former Devex Senior Reporter based in Canberra, where she focuses on the Australian aid community. Lisa has worked with News Corp Australia as a data journalist and has been published throughout Australia in the Daily Telegraph in Melbourne, Herald Sun in Melbourne, Courier-Mail in Brisbane, and online through news.com.au. Lisa additionally consults with Australian government providing data analytics, reporting and visualization services.