Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Researchers at IBM Security Trusteer’s mobile security research team discovered the attacks, although they have not revealed details of which banks were affected nor how much was stolen – although it’s known that each attack was capable of reaping millions of dollars or euros. The attacks were carried out by using mobile device emulators – standard software tools used by developers to create mobile apps – to spoof actual customer details.

According to IBM: “The scale of this operation is one that has never been seen before, in some cases, over 20 emulators were used in the spoofing of well over 16,000 compromised devices. The attackers use these emulators to repeatedly access thousands of customer accounts and end up stealing millions of dollars in a matter of just a few days in each case. After one spree, the attackers shut down the operation, wipe traces, and prepare for the next attack.”

In order to mount the attacks, the thieves needed access to data for the customers, most likely gleaned and aggregated from previous data breaches and phishing campaigns. The data includes: usernames and passwords; device identifiers; and in some cases, the ability to access an account’s SMS messages, to intercept two-factor authentication (2FA) codes.

By setting up a network of machines running emulators, the attackers could rapidly cycle through accounts, using customised applications adapted specifically for the task. If an emulated ‘device’ was blocked by an institution, the attackers could quickly spin up another. The criminal group also emulated the systems it was targeting in order to test the attack software, as well as monitoring fraudulent transactions in real time while they were underway.

These are capabilities not often seen in the cybercrime world, and according to IBM: “It is likely that those behind it are an organised group with access to skilled technical developers of mobile malware and those versed in fraud and money laundering. These types of characteristics are typical for gangs from the desktop malware realms, such as those operating TrickBot or the gang known as Evil Corp.”

According to Craig Young, principal security researcher at Tripwire: “The banks themselves are the ones with the data to see the big picture and recognise fraudulent activity. Migrating customers to better forms of 2FA is a great starting point, but the authentication methods need to evolve faster and become better at recognising suspicious behaviours. For example, the attackers in this case were using VPN providers as a relay to have an appropriate IP geography for their emulators. The use of regional IPs to fly under the radar was a smart move by the attackers but the bank should not have had any difficult recognising that users were suddenly logging in from VPN services who had never used them before. Rather than simply monitoring for suspicious IP address locations, they should have been tracking what networks the clients logged in from.”

North Korea attacks Covid-19 research bodies

The Lazarus group, North Korea’s state-run hacking operation, recently targeted two organisations in an attempt to steal research relating to Covid-19 vaccines, according to an analysis by Kaspersky.

The two attacks used different tactics, techniques and procedures (TTPs), but Kaspersky said it found enough in common – including similarities in the post-exploitation process – to convince it that the same attacker was behind both incidents. And the malware used points directly to the Lazarus group.

Kaspersky doesn’t name the targets in its report, but says that a government ministry of health was attacked using the wAgent malware in October 2020, with two servers being compromised. The malware opened a reverse shell, allowing the attackers access to the machines.

The second attack, in September 2020, used the Bookcode malware against a pharmaceutical firm developing and distributing a Covid-19 vaccine. This malware also has the capability to open a backdoor. Kaspersky couldn’t identify the infection vector in this case.

In the past, Lazarus has used spear-phishing to deliver malware, although ESET has also previously detected supply-chain chain attacks in which the malware was injected into updates for legitimate software used by targets.

“These two incidents reveal the Lazarus Group’s interest in intelligence related to Covid-19,” Kaspersky said in its report. “While the group is mostly known for its financial activities, it is a good reminder that it can go after strategic research as well.”

The TTPs that helped Kaspersky identify the attackers as Lazarus included: extracting infected host information, including password hashes from the registry sam dump; using Windows commands in order to check network connectivity; and using the WakeMeOnLan tool to scan hosts in the same network.

In its blog post, Kaspersky concluded: “We assess with high confidence that the activity analysed in this post is attributable to the Lazarus group. In our previous research, we already attributed the malware clusters used in both incidents described here to the Lazarus group.”

The Kaspersky report is here: http://bit.ly/3hKQ37d.

Meanwhile, the US Department of Justice (DOJ) has seized two domains that have previously been used to impersonate the real websites of two pharmaceutical companies involved in the development of Covid-19 vaccines – Moderna and Regeneron. The lookalike domains – mordernatx[.]com and regeneronmedical[.]com – faithfully copied the real sites. However, they also used the sites to run scams, host malware and perform phishing attacks. For example, visitors to the ‘Contact us’ pages on both sites were asked to fill in copious amounts of personal data or contact the companies via a phone number which turned out to be a VoIP number connecting to the criminals behind the scams.

Finally, the US Federal Trade Commission (FTC) says that more than 275,000 US residents have reported financial losses amounting to more than $211m due to Covid-related scams since the start of 2020. There’s more information here: http://tabsoft.co/2LmMZSG.