THREATS TO BANK CUSTOMERS. NON-TARGETED ATTACKS

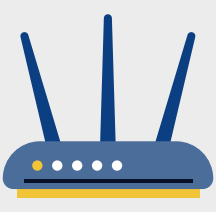
Part II

ROOT LEVEL RESOURCES

Web phishing[1] and social engineering remain the predominant threats to bank customers.

Continued rapid evolvement of **DNS hijacking** enables scammers to conduct even more effective phishing attacks.

Let's briefly review what this method basically involves:



Gaining access to the router via either of two ways:

Variant 1

Password brute-forcing – providers that lease routers to users tend to neglect security considerations, setting default passwords and leaving admin interfaces accessible over the internet.

Variant 2

Exploiting known vulnerabilities – keeping residential routers updates is no easy task. The support cycle for such devices is typically short, and security updates are often unavailable. Even where they are available, only a low percentage of end users bothers to update the equipment.

Modifying DNS server settings, propagated to all devices connected to the Wi-Fi network of the compromised router.

IP address spoofing – when certain domain names are requested, malicious DNS servers return fraudulent IP addresses. E. g., when the user enters the URL of a trusted website such as a bank in the address bar, what the server returns instead of the bank's IP address is a false one.

Once the data from phishing victims is collected, it may be used in one of the following ways:

Sending the data by email (remains the most popular)

Saving the data to a local text file, from which the scammers can transfer it to a remote server using a number of methods

Uploading logs to a remote FTP server (a rare scenario)

Scammers who specialize in phishing data from bank customers use web-inject control panels for managing phishing pages. This technique, which lately has seen a surge, allows them to perform real-time attacks, receive one-time passwords from victims, and accomplish other operations required to confirm financial transactions. U-Admin is one of the most popular among such control panels.

Social engineering

without using malware or phishing websites also remains one of the most common schemes, which may look like this:

1. The attacker makes a phone call, pretending to be calling on behalf of the bank, and informs the client that an attempt to break into their personal account or withdraw funds from it has been registered.
2. The attacker persuades the unsuspecting victim that the bank's security service allegedly needs their cooperation in solving a technical problem as part of the effort to stop the fraud.
3. The victim is asked to urgently install a remote access app on their smartphone, allegedly for security reasons.
4. Once the remote access app is installed, the attacker opens the mobile banking app and withdraws funds from the victim's account.

In the course of a social engineering scheme, the victim either gives away all their banking credentials or, following the attacker's instructions, installs remote access application on their computer, enabling the attacker to perform online banking operations on the victim's behalf. In the more recent version of the scheme, the victim is asked to install a remote access app on their mobile device.

ATM trojans

ROOT LEVEL RESOURCES

Emerging threats

Unnamed trojan from Africa

This malware enables the attacker to control the ATM through the PIN pad: directly interact with the dispenser whenever a correct PIN code is entered, or withdraw all the available cash from the ATM whenever a bank card with a certain number is used. To bypass white lists, the attackers use the file cmd.dll, a system tool similar to cmd.exe and implemented by the developers of ReactOS.

HelloWorld

The malware is available for purchase on an underground forum in the following versions:

- An executable file analogous to Cutlet Maker, with or without a keygen;
- An IMG image that can be written to a flash drive;
- A CD image;
- A floppy disk image;
- An ISO image for downloading via PXE (currently being developed).

This trojan works on all Wincor/Diebold Nixdorf models dated later than 2001 that have MXFS/CSCW dll files. The price is $2,000 for the executable or an image, $3,000 for all versions, and $10,000 for the source code.

History of existing ATM Trojans

Cutlet Maker

One of the most widespread ATM trojans, found in various free versions since 2017. Cutlet is successfully used by fraudsters throughout Europe as well as Russia and other post-Soviet countries.

ATMii

ATMii, which first appeared in 2017, is known for targeting specific operating systems. This trojan could run on Windows 7 and Windows Vista, while the most popular operating system used in ATMs at that time was Windows XP.

Alice

This trojan has been known since November 2016. In comparison to the free Cutlet Maker, Alice is less convenient to use. More recently, it has not been seen in widespread use.

WinPot (Cutlet V2)

The first ad promoting this malware appeared at an underground forum in 2018. The trojan comes complete with the source code, the prices ranging from 500 to 1,000 USD. Like its predecessor, this trojan is used to attack ATMs in European countries.

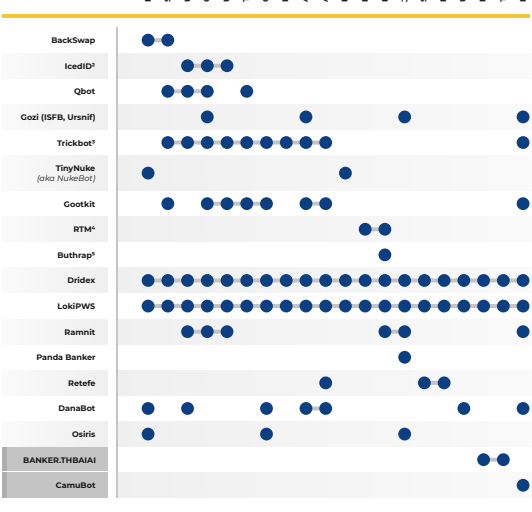
Ploutus

This malicious program has been available for purchase since 2016. Scammers in Mexico have been using it for a long time, joined by their U.S. counterparts in 2018. Despite its age, Ploutus remains actively used, and in 2019 ads offering it for purchase began reappearing on hacker forums.

PC trojans

ROOT LEVEL RESOURCES

The use of PC trojans in bank hacking continues to decline, and no newly developed techniques of theft have been recently identified. Brazil remains the only country where their development is still in progress. Most PC trojans are created by local hackers and used on local targets.



New PC trojans

BANKER.THBAIAI

This trojan was discovered in 2019.
A brief overview of its functionality:

1. The first module infects the computer, then loads and executes PowerShell scripts that write .LNK files into the Startup folder and force the computer to reboot. After the reboot, the user is shown a fake login screen, which is used to capture the login and password.
2. Then the second module is launched, which tries to open Microsoft Outlook and collect all email addresses stored in it. If Outlook is not found, the malware skips this step.
3. Additionally, the remote access program RADMIN is installed on the compromised system.
4. The last one to be installed is a fileless banking trojan, which targets the customers of Brazilian banks Banco Bradesco, Banco do Brasil, and Sicredi.

CamuBot

First used in 2018, CamuBot is known for its unusual distribution method. Instead of using mass distribution, attackers would call the victim on behalf of the bank and ask to visit the bank website, which in reality was a fake used for phishing, in order to download an alleged security module. Once downloaded to the user's system, CamuBot would open a tunnel to the victim's computer and a fake bank website, which would ask the user to enter their online banking login and password.

Android trojans

ROOT LEVEL RESOURCES

Stealing money via banking android trojans may involve any one of the three basic techniques:

Money transfers via text messaging

(drawback: only a few banks offer text messaging money transfer services, and the limits on the transfer amount are low)

Fake mobile banking app

(drawback: the distribution of fake mobile banking apps requires significant investments as well as marketing and promotion efforts)

Collecting bank card data, logins and passwords, etc. through fake dialog screens

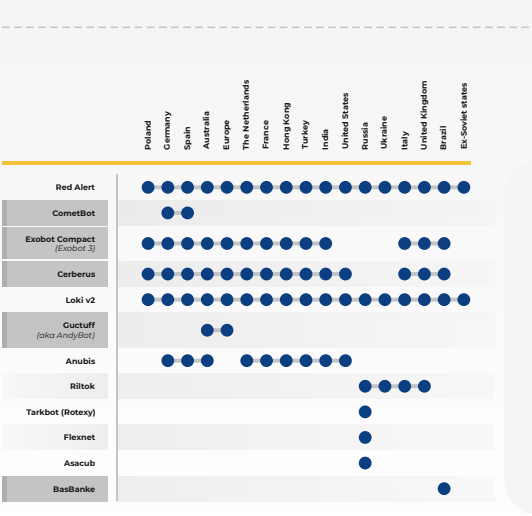
(the most effective way)

When newer Android versions came out with a stricter security policy and user apps lost the ability to show arbitrary windows, the fake dialog screen method stopped working. Most developers of Android trojans failed to adapt to the updates, and many formerly effective trojans became useless. Some projects have closed, and their developers left the scene. The development of these trojans noticeably slowed down, and the level of damage from their activity dropped.

At the early stage of online banking, banks used to send confirmation codes for transactions via text messages. However, with the spread of mobile apps, text messaging has been mostly replaced with push notifications, which are both cheaper for the bank and safer, since all Android banking trojans are able to intercept text messages. The advent of push notifications is another reason for the decrease in activity of these trojans.

However, bypassing security restrictions is still possible using Accessibility Services, a special set of features designed to make it easier for persons with disabilities to use their mobile devices. By acquiring permission to use the Accessibility Service, the malicious app basically gets the opportunity to block the windows of other applications, control the device with voice commands, listen to the content instead of reading it, manage push notifications, secretly unlock the device, and perform arbitrary operations while keeping the screen turned off.

The trojan uses Accessibility Services to interact with the elements of app windows and can focus on the object, click on the object, and modify the text content of the object.



New Android trojans

Gustuff

This is basically a continuation of the AndyBot Trojan and created by the same author.

However, the most important difference between Gustuff and other Android trojans is its ability to autoload via the following steps:

- The trojan sends a push notification with the icon of the banking app
- The user presses on the push notification
- The "banking app" opens
- The user enters their login credentials
- Following a command from the server, Gustuff performs autoloading

The monthly fee for using this malware is 800 USD. The developer is careful enough about their own legal safety to provide a disclaimer saying that the bot doesn't work in Russia, post-Soviet states, and the U.S.

Exobot Compact

The third version of the well-known, tried-and-true Exobot trojan. In May 2018, the source code of the Exobot v.2 was released to the public, and the new version has been completely rewritten and optimized. Exobot Compact can run on modern Android versions up to Android 9. The developer takes the same precaution as the creator of Gustuff, prohibiting the use of the bot in Russia, ex-CIS, and the U.S., though at the same time offering fake pages for U.S. banks. The fee is 1,500 dollars per month.

Cerberus

A trojan somewhat similar to Gustuff in terms of functionality – in particular, it can work with push notifications from banks as well. However, the Cerberus trojan also implements the following self-protection methods:

1. Turning off Google Play Protect and turning itself off after the expiration date set in the admin control panel;

2. Blocking attempts to delete the bot, to disable administrator rights, or to stop Accessibility Services.

3. Detection of being started up in a sandbox by reading the accelerometer.

The monthly fee is 2,000 USD. Same as the developer of Gustuff, the creator of Cerberus prohibits the use of the trojan in Russia and the ex-CIS countries.

CometBot

While this trojan is not as powerful, it, too, can run on the latest versions of Android. The offer includes ready-made web fakes specifically imitating several German and one Spanish bank, but the malware's functionality can be easily extended to support faking banks in other regions. CometBot's monthly fee is $850.

BasBanke

This new Android trojan targets the customers of Brazilian banks. While the functionality of BasBanke is fairly basic, the developers have managed to publish it on Google Play, securing more than 10K downloads. The trojan features keylogging, screen recording, and text message interception functions.

However, no attacker can reach their goals as long as the attack is detected and stopped in time. Detecting and stopping the threat is possible at any stage of the attack, provided that the required protection measures have been taken.

1 – One of the oldest and simplest types of fraud, which has been gradually replacing more complex attacks involving expensive trojans or hacking tools.

2 – Still uses web injects and uses autoloading to automatically steal money from bank accounts.

3 – Over the last year, has been enhanced with new updates that collect passwords from installed applications, steal configuration files from SYSVOL directories on the domain controller, use Mimikatz, perform fileless attacks, and send mass mail from compromised computers. The new version of this trojan allows for targeted attacks on large organizations.

4 – The only currently active trojan in Russia, the homeland of most banking trojans. Most of its victims, however, are customers of the banks with poor security protocols

5 – Earlier, the owners of the Buhtrap2 botnet tried autoloading through 1C, a Russian ERP system, but this method allowed for early detection of infected devices and prevention of theft.