A Trend Micro Research Paper

Finding Holes

Operation Emmental

David Sancho, Feike Hacquebord, and Rainer Link

Forward-Looking Threat Research Team

Contents

Introduction

Like Swiss Emmental cheese, online banking protections may be full of holes. Banks have been trying to prevent cybercrooks from accessing their customers' online accounts for ages. They have, in fact, invented all sorts of methods to allow their customers to safely bank online.

This research paper describes an ongoing attack we have dubbed "Emmental" that targets a number of countries worldwide. The attack is designed to bypass a certain two-factor authentication scheme used by banks. In particular, it bypasses session tokens, which are frequently sent to users' mobile devices via Short Message Service (SMS). Users are expected to enter a session token to activate banking sessions so they can authenticate their identities. Since this token is sent through a separate channel, this method is generally considered secure.

Some of the banks we looked into do not exclusively use this system. They usually complement it with other ways to ensure the security of their customers' banking sessions such as using photo-TANs or issuing physical card readers.[1] However, the fact remains that banks let most of their customers use session tokens with the aid of SMS and leave more secure methods for premium clients only or as an alternative option, possibly due to increased operating costs and ease of use.

The attackers in this case who are most likely to be based in a Russian-speaking country set up a system that could defeat session token protection. This particular attack actively targets users in Austria, Switzerland, Sweden, and Japan.

In response, we proactively contacted the banks that the cybercriminals behind Operation Emmental attempts to phish so they could take appropriate measures to protect their clients.

Attack Details

The attack starts when users receive an email in their local language. Attackers usually pose as senders from a popular company. The sample email below supposedly came from a well-known online retailer in Germany and Switzerland but it is fake. Because the retailer is very popular, recipients are most likely its customers. We also saw fake emails supposedly sent by a popular brand among Swiss users.

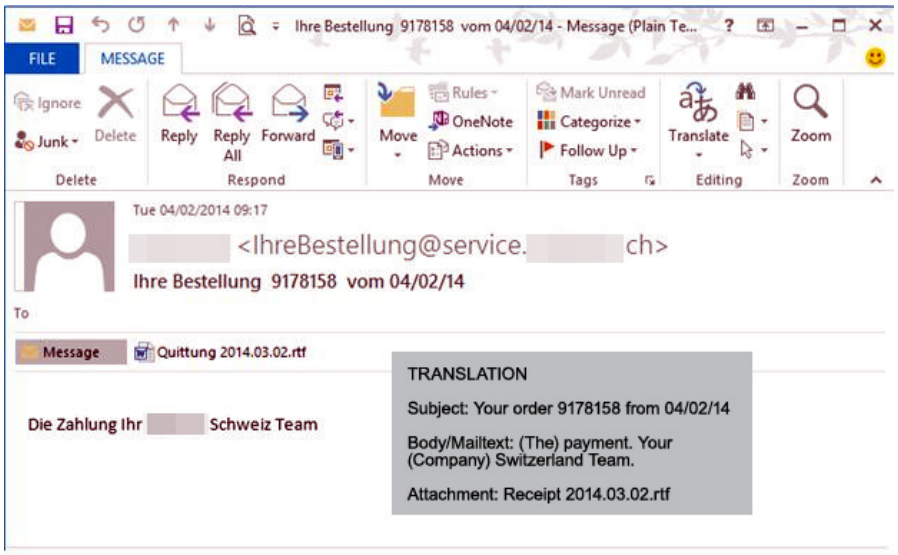

Figure 1: Sample fake email
(Image source: http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan:Win32/Retefe.A#tab=2)

When opened, the attached .RTF file contains another file.

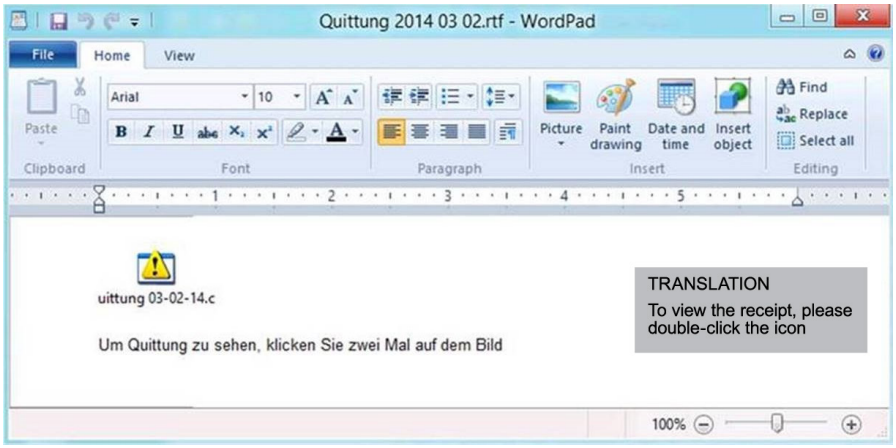

Figure 2: File attached to the fake email sample when opened
(Image source: http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan:Win32/Retefe.A#tab=2)

Note that the file extension embedded in the document is masked because it is very long. However, if the users are curious enough to open the file, they will see a warning that they are opening a .CPL file or a Control Panel item, which could be dangerous.[2]

Figure 3: Security warning that pops up when the embedded file is clicked (Image source: http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan:Win32/Retefe.A#tab=2)

Running the .CPL file downloads and executes another file called *"netupdater.exe,"* which is supposedly a Windows® update tool. In reality, however, installing the fake update tool results in malware infection.

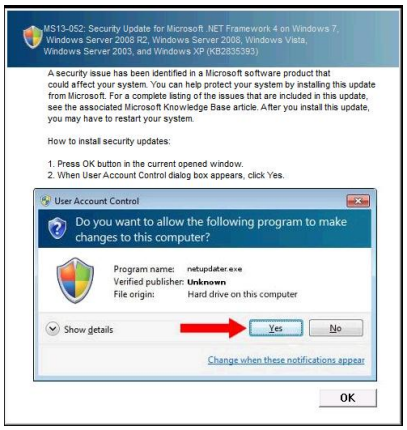

Figure 4: Supposed update tool installation prompt (Image source: http://blogs.technet.com/b/mmpc/archive/2014/02/27/a-close-look-at-a-targeted-attack-delivery.aspx)

Malware

Malware infection, meanwhile, has three system effects, namely:

1. The malware changes the system's Domain Name System (DNS) server settings to point to one that is under the attackers' control.[3] From this point forward, the attackers gain control over how the infected system resolves Internet domains.

2. The malware installs a new root Secure Sockets Layer (SSL) certificate in the infected system. This allows the attackers to display content from secure phishing sites without triggering a warning from the browser.

3. The malware deletes itself without leaving any trace, which makes it difficult for users to detect infection after installation. This means that if the infection attempt was not immediately detected, any anti-malware check that follows will not detect anything since the file will no longer be there. The infection is not such; it is only a configuration change on the system.

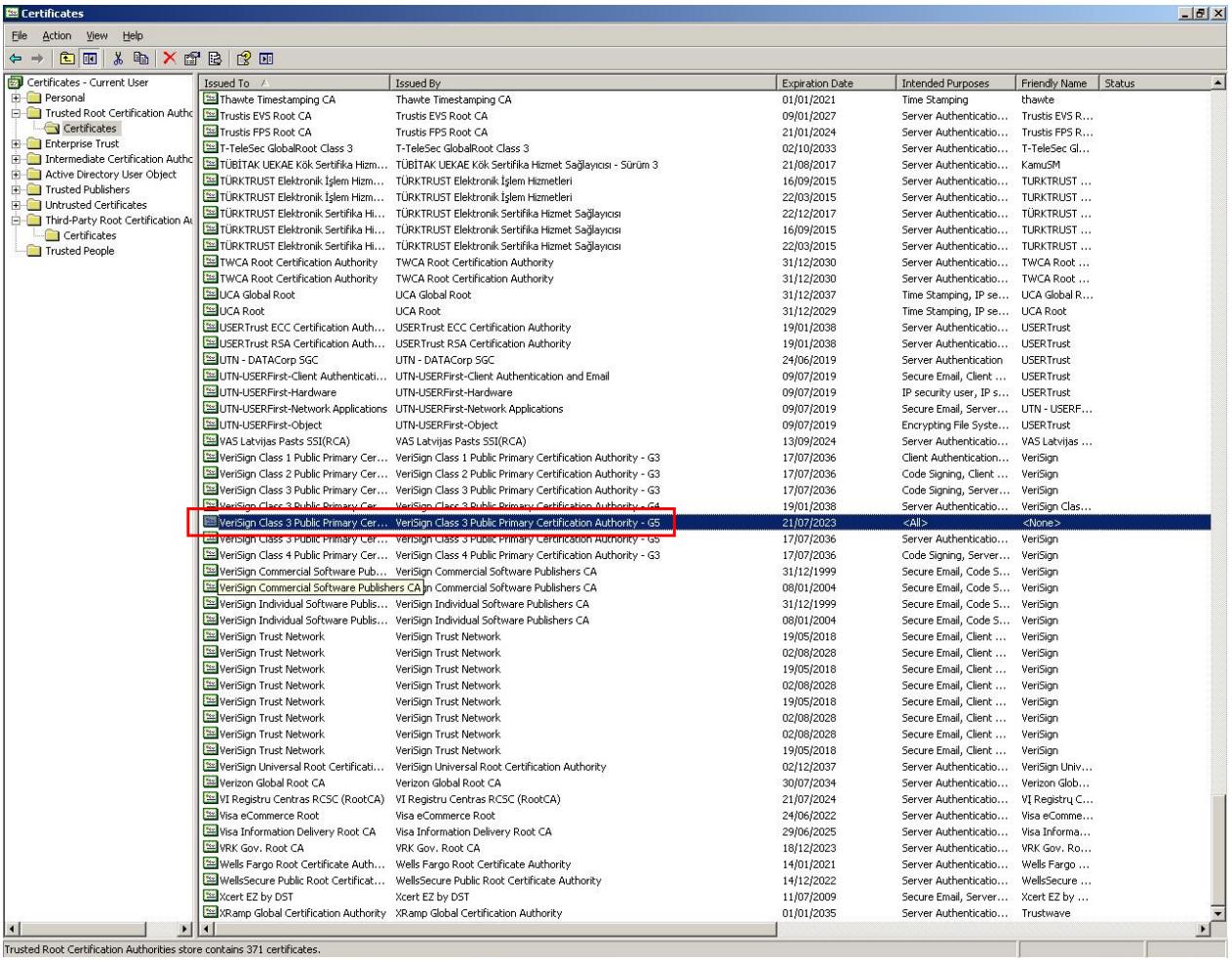

Figure 5: Certificate store after the rogue SSL certificate is installed

Rogue DNS Servers

We detected a variety of rogue DNS servers involved in the attack. We were able to investigate one of them for a few days before it stopped working. Further investigation revealed that every time users of infected machines would try to access six bank domains in Austria, seven in Sweden, 16 in Switzerland, and five in Japan, they would be directed to a malicious server instead. In essence, accessing any of the 34 banking sites using an infected computer leads users to communicate with a phishing server instead of their bank's server.

The following paragraphs describe what happens when users access one of the phished banks' site via an infected system. Note that the communication occurs via secure HTTP but since the system has a fake certificate installed, the users do not see any browser warning.

First, the users land on a phishing page that asks them to log in, revealing their usernames, bank account numbers, and some other numbers that they supposedly received from their banks. This is normal and expected. The users are then asked for their personal identification numbers (PINs), which serve as their passwords. This is also a regular form of authentication. Note that the users are already giving away their first authentication factor to access their accounts at this point.

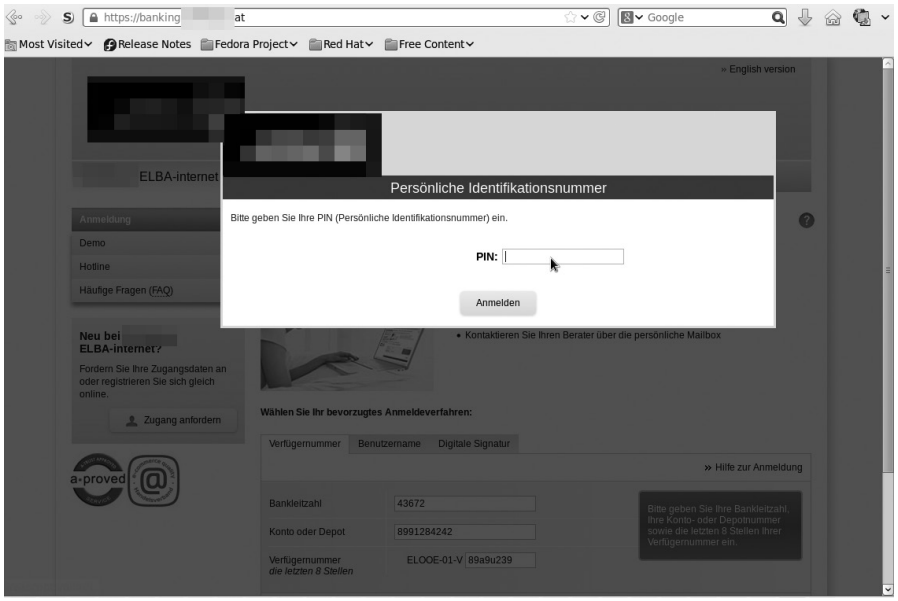

Figure 6: Fake prompt to get users to give away their first authentication factor when they try to access the bank's site via an infected computer

The users are then asked to provide a one-time password generated by their bank's mobile app. The regular procedure is to wait for an SMS from the bank but instead of that, the phishing page instructs the users to install a special mobile app in order to receive a number presumably via SMS that they should then type into a website form. The site looks secure but it is fake so the mobile app provided is not trustworthy.

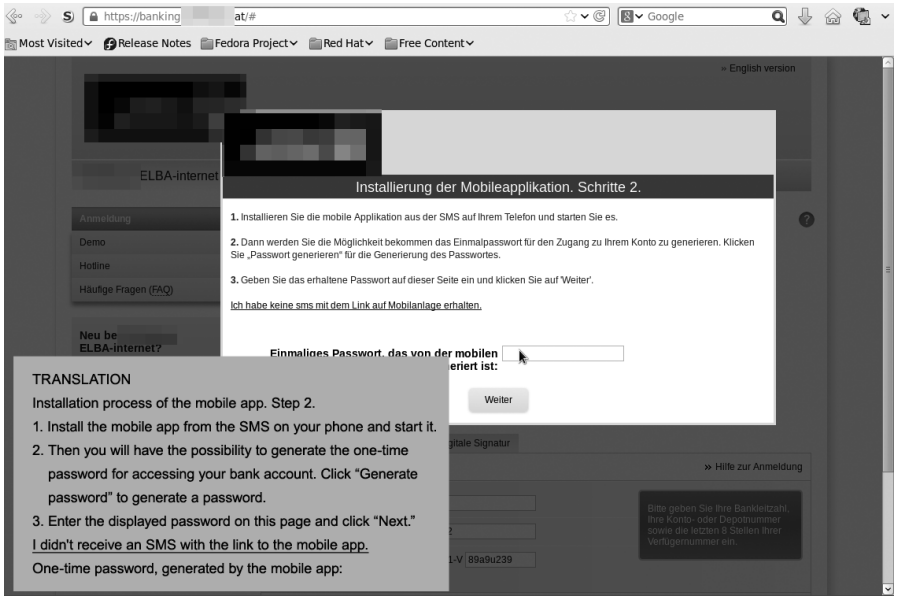

Figure 7: Instructions users who access the bank's site via infected computers get to install the dubious mobile app

The SMS that the bank should supposedly send never arrives. The users are forced to click the "I didn't receive the SMS" link. When clicked, they get a prompt to install the mobile app. They are led to a shortened URL that leads to *http://security-apps.biz/[bank name].apk*—a page that hosts the rogue Android™ app.

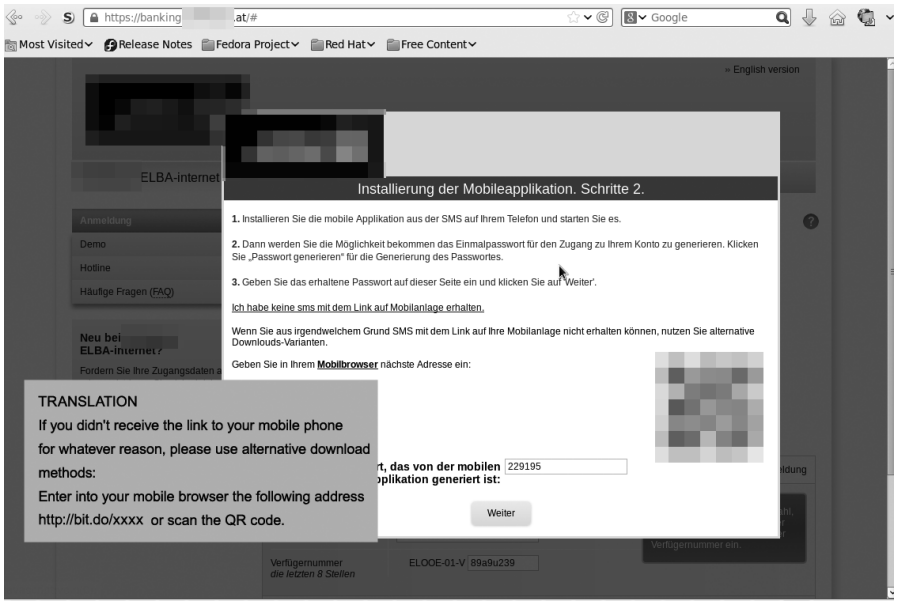

Figure 8: Further instructions users who access the bank's site via infected computers get to install the rogue mobile app
Note the awkward-sounding text, which could mean that the author is a non-native-German speaker.

At this stage, the users have to enter the password that was “generated” by the fake app. The app has a preset list of possible passwords and just randomly chooses one. The Web page, meanwhile, simply checks if one of those possible passwords was entered. Guessing numbers does not work, the users will not be able to proceed with the fake banking authentication. If a correct number is entered though, the site claims that the new security feature has been successfully enabled. The whole procedure only serves to lure users to install the app and leave it on their phones because without it—the phishing page claims—the users will no longer be able to bank online in the future.

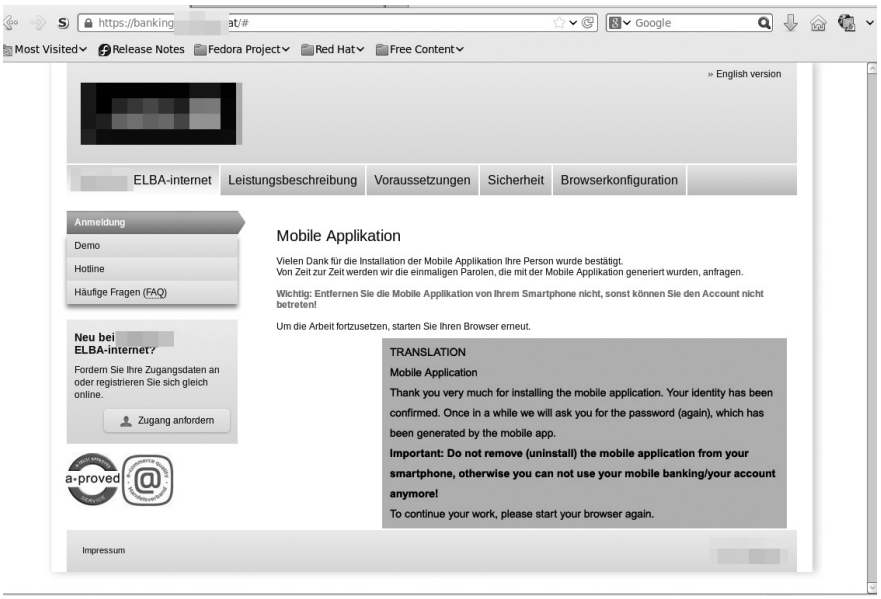

Figure 9: Final instructions users who access the bank’s site via infected computers will see related to the rogue mobile app installation
Again, note the awkward-sounding German text.

Installing the Android app allows the attackers to gain full control of users’ online banking sessions because, in reality, it intercepts session tokens sent via SMS to users’ phones, which are then forwarded to the cybercriminals. The spoofed website allows the attackers to obtain the users’ login credentials while the mobile app intercepts real session tokens sent by the banks. As a result, the attackers obtain everything they need to fake users’ online banking transactions.

Android apps with logos of different banks send the real tokens to a compromised server that serves as the attackers' command-and-control (C&C) server. All of the Android application package or .APK binaries we obtained spoofed legitimate banks' logos and corporate colors. These banks also have one thing in common—they all required a single-session token for each transaction. This piece of information is the attackers' target because once stolen, they can fully impersonate users on banks' real sites.

Rogue Mobile App

This section provides a more complete overview of the fake apps that the attackers created for users to install on their smartphones. The rogue Android apps generate a password that users need to start online banking sessions. This password is supposed to be entered into the fake banking site while the scam occurs behind the scenes.

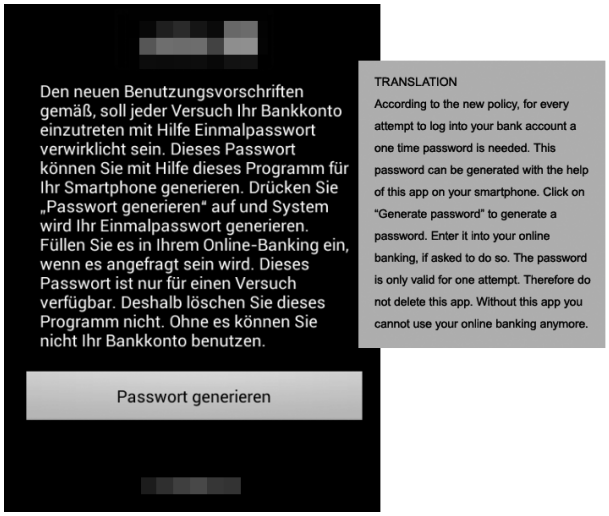

Figure 10: Rogue mobile app's password generator
Again, note the awkward-sounding German text.

Figure 11: Sample fake password that the rogue app generates

In reality, the app waits for an SMS from the bank, which provides a legitimate session token. When received, the app silently hijacks the communication and forwards the stolen information to the attackers' C&C server. This would allow them to conduct banking transactions in the guise of bank customers. In case of absence of Internet connectivity, the app can also forward stolen session tokens via SMS. It also has the capability to transfer personally identifiable information (PII) such as phone number, phone model, Global System for Mobile Communications (GSM) operator, country/region, and other data from victims' phones to the C&C server. The malicious app also registers its own SMS listener service and has its own SQLite database to store messages and settings. It also has the ability to receive remote commands. The SMS listener service executes every time an infected Android mobile phone is booted. Even worse, uninstalling it displays a stern warning that could convince victims to leave it on their phones. It does not help that the banks whose customers are targeted by this attack do not officially support Android apps.

Attribution

In normal malware infection cases, hints of attribution are extremely scarce. In this particular attack, however, we were able to obtain clues that although may not be definitive could shed some light on who are behind it. The following details allowed us to obtain information on the attackers:

- A log message in the app, "Obnilim rid," is Russian slang that translates to "set to zero." The app also has a leftover function to check the country the victim's subscriber identity module (SIM) card is registered in. It specifically checks for Austria and Switzerland to make sure the attackers find targets that they can fully victimize. It also checks for Russia although this function could only be a remnant from their testing to avoid infecting their computers. Note, however, that this function is never called because further scrutiny revealed that it was replaced by another function.

- We were also able to see connection logs from underground sources from the owners of this malware. It turns out that most of them were from Romania. This made us think that one of the associates in this cybercriminal enterprise is based in that country. A Russian speaker based in Romania could be responsible for the whole operation. Or the brains behind the operation could be based in Russia and the Romanian connection only plays a small part in the attack. We cannot say for sure.

Conclusion

Operation Emmental is a complex operation that involves several components in order to defeat a particular online banking protection system used in several countries. The infrastructure required to pull the attack off is not inconsequential—the attackers need a Windows malware binary, a malicious Android app sporting various banks' logos, a rogue DNS resolver server, a phishing Web server with several fake bank site pages, and a compromised C&C server.

Emmental is an attack that has very likely evolved over time. The fact that the most salient part of the attack—the PC malware—is not persistent likely helped the attackers keep a low profile. We believe this allowed them to use different infection strategies, not just through emails, although we have not been able to detect any other means.

The malware that the attackers used revealed a weakness in single-session token protection strategies. Banks and other organizations that continue to use these are exposing themselves and their customers to rogue mobile apps. More advanced defenses, which include the use of multiple transaction authentication numbers (TANs), photo-TANs, and card readers, should be considered. Even though these are more complicated to maintain, every organization must gauge if it is worth the investment in order to shore up their defenses. Protecting clients in phishing scenarios is often outside the control of the organization being phished. Bank clients are advised to take all necessary precautions to secure their transactions, especially since the attacks mentioned in this paper occur entirely on their side.

In sum, the attackers are most likely Russian speakers, either use a single proxy server hosted in Romania or live there, and regularly avail of shady Russian cybercriminal underground market services.

Appendix

IP Addresses That Hosted the Attackers' Rogue DNS Servers

- *5.39.219.212* (mid- to end of April 2014)
- *193.169.244.73* (October–November 2013)
- *193.169.244.191* (January 2014)
- *93.171.202.99* (February 20, 2014, 14:44:31 GMT and February 25, 2014, 02:47:32 GMT)
- *37.221.162.56* (December 2013, probably)
- *78.108.179.81* (early April 2014, probably)

Online Android Malware Binary Repositories Found

- *http://tc-zo.ch/security/[bankname].apk* (SHA1: *1e5ea1d2a747c69402746fe67e0ef0fbabc597e2,* MD5: *7830bebd3e4cde85b972b279e7ff41ba)*
- *http://tc-zo.ch/security/[bank name].apk* (SHA1: *bf06da598e5ecfd6beec887696ab6572a890c99b,* MD5: *99a41514e6d91b1737561e1b692cc88c)*
- *http://tc-zo.ch/security/[bank name].apk* (SHA1: *8af1977a7a8cd34ea6aee16e6fd1b470f5f28c01,* MD5: *6a418fad387ee3421ad54919782fa884)*
- *http://security-apps.net/[bankname].apk* (SHA1: *1c4caa8a40e478f39317fb286b61a60500666ce9,* MD5: *d9e55d68d406ee5ab9f55868f41320a2)*
- *http://security-apps.net/[bank name].apk* (SHA1: *739614dc008c69a096462b1daf1cc045978af47b,* MD5: *488179c297c6222ea46a91aff41207d1)*

- *http://security-apps.net/[bankname].apk*(SHA1:*660bc950548e8855c5869cfa4d79b96b16b97f20,* MD5: *1f2b68cd0243735ed0190cb26838d9c8)*
- *http://security-apps.net/[bankname].apk*(SHA1:*b5d22afde28040ccfddbc3ffd9dde0f493808275,* MD5: *411f072ec42cbe389222b066c83cb874)*
- *http://security-apps.net/[bankname].apk*(SHA1:*ba12730eb5c0cb144231810e102a608653d142a6,* MD5: *e4c138848edeee7b21597817c2e904db)*
- *http://security-apps.net/[bankname].apk*(SHA1:*28c1bab281844b3ccf6671414ebe4e6824f185b6,* MD5: *502857570c7a318cb89421a512c99067)*
- *http://security-apps.biz/[bankname].apk*(SHA1:*1c4caa8a40e478f39317fb286b61a60500666ce9)*
- *http://security-apps.biz/[bankname].apk*(SHA1:*739614dc008c69a096462b1daf1cc045978af47b)*
- *http://security-apps.biz/[bankname].apk*(SHA1:*660bc950548e8855c5869cfa4d79b96b16b97f20)*
- *http://security-apps.biz/[bankname].apk*(SHA1:*b5d22afde28040ccfddbc3ffd9dde0f493808275)*
- *http://security-apps.biz/[bankname].apk*(SHA1:*ba12730eb5c0cb144231810e102a608653d142a6)*
- *http://security-apps.biz/[bankname].apk*(SHA1:*28c1bab281844b3ccf6671414ebe4e6824f185b6)*

Whois Data

security-apps.net

```
[Querying whois.verisign-grs.com]
[Redirected to whois.reg.ru]
[Querying whois.reg.ru]
[whois.reg.ru]
Domain name: security-apps.net
Domain idn name: security-apps.net
Registry Domain ID:
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.com/
Registrar URL: https://www.reg.ru/
Registrar URL: https://www.reg.ua/
Updated Date: 2014-04-11
Creation Date: 2014-04-11T14:43:12Z
Registrar Registration Expiration Date: 2015-04-11
Registrar: Domain names registrar REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Registry Registrant ID:
```

```
Registrant Name: Domain Admin
Registrant Organization: PrivacyProtect.org
Registrant Street: All Postal Mails Rejected, visit Privacyprotect.org
Registrant City: Nobby Beach
Registrant State/Province: Queensland
Registrant Postal Code: QLD 4218
Registrant Country: AU
Registrant Phone: +45.36946676
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact@privacyprotect.org
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: PrivacyProtect.org
Admin Street: All Postal Mails Rejected, visit Privacyprotect.org
Admin City: Nobby Beach
Admin State/Province: Queensland
Admin Postal Code: QLD 4218
Admin Country: AU
Admin Phone: +45.36946676
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: contact@privacyprotect.org
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: PrivacyProtect.org
Tech Street: All Postal Mails Rejected, visit Privacyprotect.org
Tech City: Nobby Beach
Tech State/Province: Queensland
Tech Postal Code: QLD 4218
Tech Country: AU
Tech Phone: +45.36946676
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: contact@privacyprotect.org
Name Server: ns1.freehosting.io
Name Server: ns2.freehosting.io
Name Server: ns3.freehosting.io
Name Server: ns4.freehosting.io
DNSSEC: Unsigned
```

security-apps.biz

```
Domain Name: SECURITY-APPS.BIZ
Domain ID: D59991216-BIZ
Sponsoring Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Sponsoring Registrar IANA ID: 303
Registrar URL (registration services): www.publicdomainregistry.com
Domain Status: clientTransferProhibited
Variant: SECURITY-APPS.BIZ
Registrant ID: DI_35688038
Registrant Name: Oleg Makarov
Registrant Organization: Private Person
Registrant Address1: Lenina 345
Registrant City: Moskva
Registrant State/Province: Moskva
```

```
Registrant Postal Code: 52236
Registrant Country: Russian Federation
Registrant Country Code: RU
Registrant Phone Number: +7.0952236584
Registrant Facsimile Number: +7.0952236584
Registrant Email: oleg_makarov555@yahoo.com
Administrative Contact ID: DI_35688039
Administrative Contact Name: Oleg Makarov
Administrative Contact Organization: Private Person
Administrative Contact Address1: Lenina 345
Administrative Contact City: Moskva
Administrative Contact State/Province: Moskva
Administrative Contact Postal Code: 52236
Administrative Contact Country: Russian Federation
Administrative Contact Country Code: RU
Administrative Contact Phone Number: +7.0952236584
Administrative Contact Facsimile Number: +7.0952236584
Administrative Contact Email: oleg_makarov555@yahoo.com
Billing Contact ID: DI_35688042
Billing Contact Name: Oleg Makarov
Billing Contact Organization: Private Person
Billing Contact Address1: Lenina 345
Billing Contact City: Moskva
Billing Contact State/Province: Moskva
Billing Contact Postal Code: 52236
Billing Contact Country: Russian Federation
Billing Contact Country Code: RU
Billing Contact Phone Number: +7.0952236584
Billing Contact Facsimile Number: +7.0952236584
Billing Contact Email: oleg_makarov555@yahoo.com
Technical Contact ID: DI_35688040
Technical Contact Name: Oleg Makarov
Technical Contact Organization: Private Person
Technical Contact Address1: Lenina 345
Technical Contact City: Moskva
Technical Contact State/Province: Moskva
Technical Contact Postal Code: 52236
Technical Contact Country: Russian Federation
Technical Contact Country Code: RU
Technical Contact Phone Number: +7.0952236584
Technical Contact Facsimile Number: +7.0952236584
Technical Contact Email: oleg_makarov555@yahoo.com
Name Server: NS1.100MS.RU
Name Server: NS2.100MS.RU
Name Server: NS3.100MS.RU
Name Server: NS4.100MS.RU
Created by Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Last Updated by Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Domain Registration Date: Wed Apr 23 07:02:06 GMT 2014
Domain Expiration Date: Wed Apr 22 23:59:59 GMT 2015
Domain Last Updated Date: Wed Apr 23 07:02:07 GMT 2014
DNSSEC: false
```

security-apps.net

```
[Querying whois.verisign-grs.com]
[Redirected to whois.reg.ru]
[Querying whois.reg.ru]
[whois.reg.ru]
```

```
Domain name: security-apps.net
Domain idn name: security-apps.net
Registry Domain ID:
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.com/
Registrar URL: https://www.reg.ru/
Registrar URL: https://www.reg.ua/
Updated Date: 2014-04-11
Creation Date: 2014-04-11T14:43:12Z
Registrar Registration Expiration Date: 2015-04-11
Registrar: Domain names registrar REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Registry Registrant ID:
Registrant Name: Oleg Makarov
Registrant Organization: Private Person
Registrant Street: Lenina 345
Registrant City: Moskva
Registrant State/Province: Moskva
Registrant Postal Code: 52236
Registrant Country: RU
Registrant Phone: +70952236584
Registrant Phone Ext:
Registrant Fax: +70952236584
Registrant Fax Ext:
Registrant Email: oleg_makarov555@yahoo.com
Registry Admin ID:
Admin Name: Oleg Makarov
Admin Organization: Private Person
Admin Street: Lenina 345
Admin City: Moskva
Admin State/Province: Moskva
Admin Postal Code: 52236
Admin Country: RU
Admin Phone: +70952236584
Admin Phone Ext:
Admin Fax: +70952236584
Admin Fax Ext:
Admin Email: oleg_makarov555@yahoo.com
Registry Tech ID:
Tech Name: Oleg Makarov
Tech Organization: Private Person
Tech Street: Lenina 345
Tech City: Moskva
Tech State/Province: Moskva
Tech Postal Code: 52236
Tech Country: RU
Tech Phone: +70952236584
Tech Phone Ext:
Tech Fax: +70952236584
Tech Fax Ext:
Tech Email: oleg_makarov555@yahoo.com
Name Server: ns1.freehosting.io
Name Server: ns2.freehosting.io
Name Server: ns3.freehosting.io
Name Server: ns4.freehosting.io
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.
internic.net/
```

```
>>> Last update of WHOIS database: 2014-04-24T12:02:37Z <<<
oleg_makarov555@yahoo.com also registered the following domains:
   •   banking-security.net
   •   certificate-security.com
   •   chromeupd.pw
   •   ffupdate.pw
   •   ieupdate.pw
   •   safe-browser.biz
   •   safe-time.net
   •   security-apps.biz
   •   security-apps.net
   •   sfotware.pw
   •   softwareup.pw
```

Both *safe-time.net* and *safe-browser.biz* are registered under a slightly different name—"Oleg Makarevich." Oleg Makarevich is also the name of a security researcher in academia (refer to *http://www.informatik.uni-trier.de/~ley/pers/hd/m/Makarevich:Oleg_B=).* This is likely a red herring left by the cybercriminals.

Mobile App Data

C&C servers found:

- *oguhtell.ch*
- *bastelfunboard.ch*

Both of the servers above are related to compromised legitimate websites.

Based on the mobile app's code, the initial C&C servers have been configured as binary resource files. The app also has a *blfs.key* file that seems to be the blowfish encryption key to decrypt the configuration file held in the encrypted *config.cfg* file. This appears to be an .XML file when decrypted.

The app can send and receive SMS as well as hide them from users. It uses its own SQLlite database to store messages. It accepts remote commands such as "START," "STOP," and "DELE." It can also send user credentials via SMS and HTTP POST.

In a few places within the code, it has the string, *Log.d("HTTP", "Obnilim rid"),* which is Russian slang for "set to zero."

Scouring the Web, we saw automated analyses of the malicious app, which showed slightly different behaviors. The following sources show that the app asked users for bank account details such as account numbers and PIN codes:

- *http://www.apk-analyzer.net/analysis/646/3752/0/html*
- *http://www.apk-analyzer.net/analysis/2026/10631/0/html*

We did not, however, see the said behaviors in the .APK files that we analyzed. Perhaps the attackers have modified their techniques.

References

1. Anni Maxx. (April 9, 2013). *Cronto.* “Comdirect and Cronto Secure Financial Transactions with PhotoTAN.” Last accessed June 6, 2014, http://www.cronto.com/comdirect-and-cronto-secure-financial-transactions-with-phototan.htm.

2. Fernando Mercês. (2014). “CPL Malware: Malicious Control Panel Items.” Last accessed June 6, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf.

3. Forward-Looking Threat Research Team. (2012). “Operation Ghost Click: The Rove Digital Takedown.” Last accessed June 6, 2014, http://www.trendmicro.co.uk/media/misc/rove-digital-takedown-research-paper-en.pdf.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900