Endpoint Protection - Symantec Enterprise

Archived: 2026-04-05 13:50:12 UTC

In December 2015, employees from several Russian banks were targeted with spoofed emails, a common technique in attack campaigns. The emails were made to look like they were from the Central Bank of Russia and offered employment to their recipients. Instead of being an actual employment offer, the emails were an attempt to deliver Trojan.Ratopak onto the target's computer.

Trojan.Ratopak was likely used because it can allow the attacker to gain control of the compromised computer and steal information. The threat can open a back door on the computer and allow the attacker to perform a variety of actions, including logging keystrokes, retrieving clipboard data, and viewing and controlling the screen. It can also be used to download other malicious files and tools. The narrow focus of the attacks and the use of Ratopak could be a hint to what the attackers were after.

Legitimate-looking emails

The attackers went to some effort to make the emails appear legitimate, even going as far as to register a domain very similar to the genuine Central Bank of Russia website. The URL for the Central Bank of Russia website is "cbr.ru", while the URL for the attacker-controlled website is "cbr.com.ru". The link to the attacker's site was included in the email sent to their victims and pointed to an archive file. Once extracted, the archive file opened a fake document and downloaded Trojan.Ratopak. We have seen Ratopak signed with stolen certificates, which can be used to avoid detection because it makes the malware appear to come from a legitimate source. We've previously seen stolen certificates used by attack groups including Black Vine and Hidden Lynx.

The emails sent out for this campaign appear to have been written by a native Russian speaker, using clean and simple language. This is also backed up by the fact that the attackers would need to speak Russian to make use of

the information stolen through Ratopak. There are no obvious errors, except for one. The name in the “From:” line of the email header differs from the signature at the end of the email. This and the “.com” in the URL are the clearest indicators that this is a fake email.

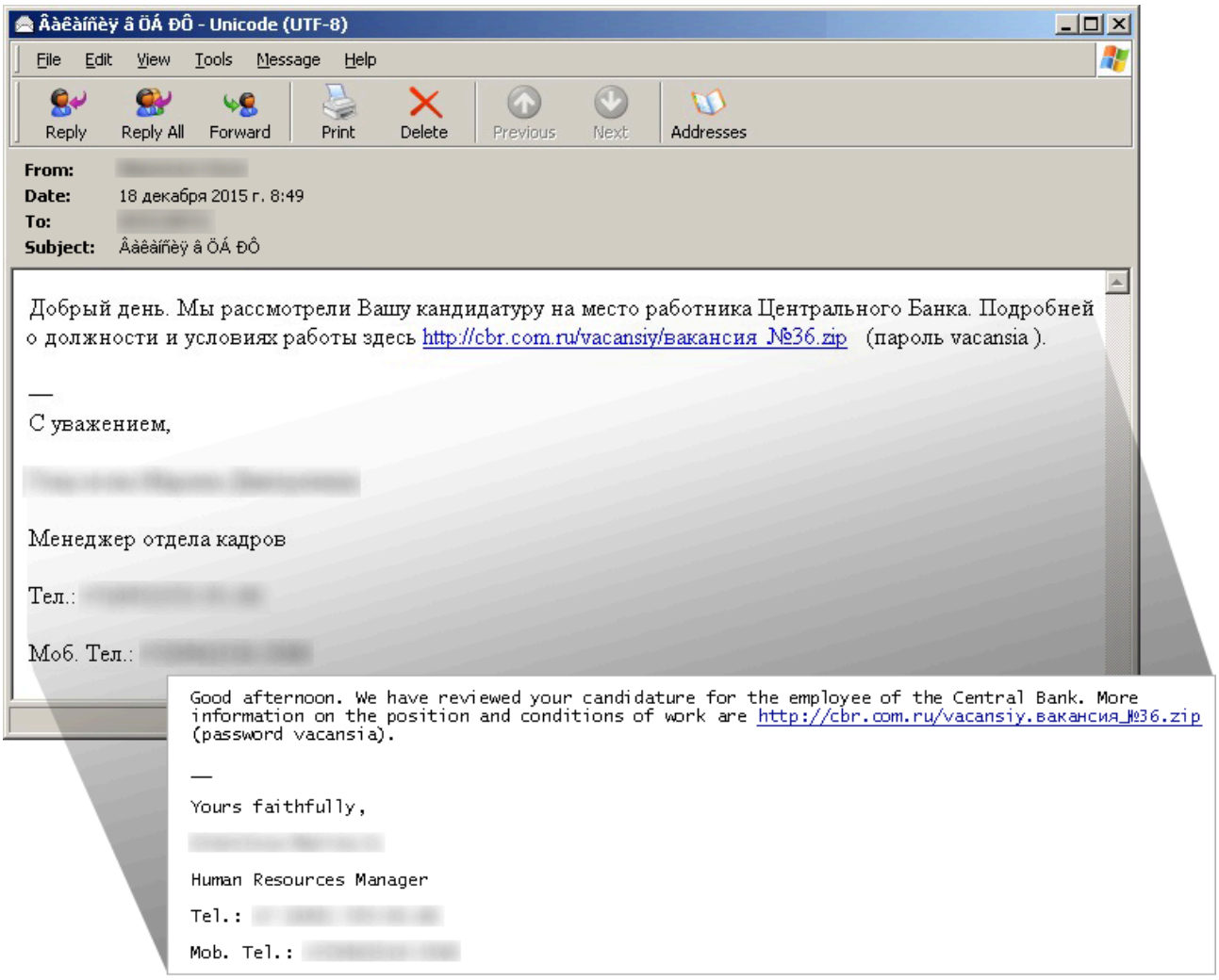

Figure. Spoofed employment offer email (in Russian) with a link to Trojan.Ratopak and translation

A similar email attack that also utilized Trojan.Ratopak occurred in October. We discovered that the attackers used another domain similar to a legitimate one to host the threat, but were not able to obtain a copy of the email. The attackers used the name of a private bank and the URL again included “.com.ru” instead of “.ru”. Given the attack in December, it is very likely that the attackers spoofed their email so it appeared to come from the private bank, and then used a link or attachment from the fake banking website to download the threat onto the victim’s computer.

Narrow, targeted attacks

Symantec has identified six Russian banks that were targeted in these attacks. All of the affected computers are located in Russia. Of those computers, a substantial number used accounting and document management software that allowed secure documents to be exchanged with the government for tax purposes. A common link between several of the victims was a piece of software created by SBIS, a Russian company that develops, among other things, accounting and payroll applications. In URLs used by SBIS, their accounting software is referred to as “buh” (buh.sbis.ru/buh/ for example. “Buh” is the Russian term for accountant).The attackers behind these attacks

used “buh” in their URLs, knowing their victims would be running SBIS accounting software. By using this string in their URLs, the attackers can disguise their attack by making their activities look like normal traffic. This approach has led other researchers to label Trojan.Ratopak as “Buhtrap”

Compromised computers may connect to the following domains; note the use of “buh” in several of them:

- google997.com
- microsoft775.com
- newsbuh1c.net
- buh.klerk.us
- buhnews.com
- football.championat.biz
- forum.ru-tracker.net
- icq.chatovod.info
- rss.sport-express.biz

The threat also checks the language of the compromised computer. If it isn’t Russian or Ukrainian, then the malware stops its attack. Ratopak may also terminate and delete itself if it recognizes that it is being run on a virtual machine or a researcher’s computer.

The attackers’ goal

While there is no conclusive evidence of the attacker’s goal, the attacks appear to be financially motivated. The specificity of the targets−employees at certain banks using accounting software to send the government tax information−certainly points towards this goal. By using Ratopak, which can open a backdoor and log keystrokes, the attackers could position themselves to steal money, either by controlling the compromised computer or using the employees’ stolen login credentials. Any goal beyond that, including what the attackers may have wanted with government tax information, is currently unknown.

Conclusion

Targeted emails using finely crafted social-engineering tricks have become commonplace, with an increasing number targeted at employees of financial institutions. While these emails sent to Russian bank employees appear to contain job offers, they only help give attackers access to the targeted computers. Users can avoid these attacks and others like them by being aware and taking the appropriate action if offered a job or service that they didn’t apply for**.**

Mitigation

Symantec advises caution when receiving unsolicited emails extending job offers or referencing non-existent job applications. Even if an email seems legitimate, the attackers may have gone to serious effort to disguise the fact that it is actually fake. We also advise following these best practices:

- Do not open attachments or click on links in unsolicited email messages
- Ensure that your computer is fully patched and up to date
- Keep security software up to date with the latest definitions

Protection
Symantec's Email Security products can be used to defend against email-based attacks.

Norton Security, Symantec Endpoint Protection, and other Symantec security products protect users against these attacks with the following detections:

Antivirus

- Trojan.Ratopak

Intrusion prevention system

- System Infected: Trojan.Ratopak Activity

Technical details

Trojan.Ratopak is delivered in a convoluted way and is a collection of several components installed in three stages.

Stage 1: Email
The path to Trojan.Ratopak begins with an email (Figure 1) that is sent to the victims. This email contains a link to a file on the cbr.com.ru website. If the victim clicks on the link, a malicious file with downloader capabilities is downloaded. This file has the following hash:

- bbac2e213bb8bafae6c6587a5bf477d3

Stage 2: Downloader
The downloaded file from stage 1 is a Nullsoft installer that contains obfuscated Nullsoft script.

The following decoy file is extracted from the Nullsoft installer and then opened with shellexecute:

- %Temp%\vacanciya.doc

The malware then checks the default language ID using the following API:

- GetSystemDefaultLangID

If the language is not Russian or Ukrainian, the malware will exit and delete itself.

It checks for the following processes to determine if it is running on a virtual machine or a researcher's computer:

- wireshark.exe
- regmon.exe
- filemon.exe
- procmon.exe
- vboxservice.exe
- vmtoolsd.exe
- ollydbg.exe

- windbg.exe
- syserapp.exe
- x96_dbg.exe
- x32_dbg.exe
- x64_dbg.exe

If it finds any of these processes, the threat will exit and delete itself.

It checks for the following .dll files to determine if it is running on a sandbox:

- dbghelp.dll
- pstorec.dll
- vmcheck.dll

If it finds any of these .dll files, the threat will exit and delete itself.

After the threat passes these checks, it downloads a file from the following HTTP URL:

- [REDACTED]7.com/kliko/res1.cab

Stage 3: Trojan.Ratopak
This downloaded file from stage 2 has the following hash and is Trojan.Ratopak:

- f4ae5579930f20ccc41d1f8b1e417e87

Ratopak arrives as a Nullsoft installer containing both clean files and malicious components. Ratopak uses clean applications to launch itself. This technique is referred to as side-loading and has also been seen with Backdoor.Korplug.

The threat checks for the language ID with the following API:

- GetSystemDefaultLangID

If the language is not Russian, it will exit and delete itself.

The Trojan drops the following file, which is a .7z password-protected archive:

- %Temp%\install.dat

The password for install.dat is 9041bU7n4R and it contains clean and malicious files. The clean files (Guide.exe and Videoconverter.exe) are executed first and then the malicious files are loaded through the side-loading technique.

The Trojan may then try to connect to one of the following domains to receive instructions:

- google997.com
- microsoft775.com
- newsbuh1c.net

Symantec has also detected the threat connecting to the following locations:

- buh.klerk.us
- buhnews.com
- football.championat.biz
- forum.ru-tracker.net
- icq.chatovod.info
- rss.sport-express.biz
