Cybercrime is focusing on accountants

By Pavel Shoshin

Published: 2019-02-20 · Archived: 2026-04-05 12:49:18 UTC

Our experts have found that cybercriminals are actively focusing on SMBs, and giving particular attention to accountants. Their choice is quite logical — they're seeking direct access to finances. The most recent manifestation of this trend is a spike in Trojan activity: specifically, from Buhtrap and RTM. They have different functions and ways of spreading, but the same purpose — to steal money from the accounts of businesses.

Both threats are particularly relevant to companies that work in IT, legal services, and small-scale production. Perhaps this can be explained by such companies' much smaller security budgets in comparison with companies working in the financial sector.

RTM

Usually, RTM infects victims by using phishing mail. The letters mimic common business correspondence (including phrases such as "return request," "copies of last month's documents," or "request for payment"). Clicking a link or opening an attachment leads to immediate infection, giving operators full access to the infected system.

In 2017, our systems registered 2,376 users attacked by RTM. In 2018, we saw 130,000 targets. And with less than two months having elapsed so far in 2019, we've already seen more than 30,000 users who encountered this Trojan. If the trend continues, it will top last year's record. For now, we can call RTM one of the most active financial Trojans.

The majority of RTM's targets operate in Russia. However, our experts expect it to cross borders and eventually attack users in other countries.

Buhtrap

The first encounter with Buhtrap was registered back in 2014. At that time it was the name of a cybercriminal group that was stealing money from Russian financial establishments — to the tune of at least $150,000 per hit. After the source codes of their tools became public in 2016, the name Buhtrap was used for the financial Trojan.

Buhtrap resurfaced in the beginning of 2017 in the TwoBee campaign, where it served primarily as means of malware delivery. In March of last year, it hit the news (literally), spreading through several compromised major news outlets in whose main pages malicious actors implanted scripts. This scripts executed an exploit for Internet Explorer in visitor's browsers.

A couple of months later, in July, cybercriminals narrowed down their audience and concentrated on a particular user group: accountants working at small and medium-size businesses. For that reason, they created websites with information particularly for accountants.

We recall this malware because of the new spike, which began in late 2018 and is continuing to this day. In total, our protection systems prevented more than 5,000 Buhtrap attack attempts, 250 of them since the beginning of 2019.

Just like last time, Buhtrap is spreading through exploits embedded in news outlets. As usual, Internet Explorer users are in the group at risk. IE uses an encrypted protocol to download malware from infected sites, and that complicates analysis and allows the malware to avoid notice by some security solutions. And yes, it still uses a vulnerability that was disclosed back in 2018.

As a result of infection, both Buhtrap and RTM provide full access to compromised workstations. This allows cybercriminals to change the files used for data exchange between accounting and banking systems. Those files have default names and no additional protective measures, so attackers can change them at will. Estimating the damages is challenging, but as we learned, the criminals are siphoning off assets in transactions that do not exceed $15,000 each.

What can be done?

To protect your business from such threats, we recommend paying exceptional attention to the protection of computers — such as those of accountants and management — that have access to financial systems. Of course, all other machines need protection as well. Here are some more practical tips:

- Install security patches and updates for all software as soon as possible.
- Forbid, to the extent possible, use of remote administration utilities on accountants' computers.
- Prohibit the installation of any unapproved programs.
- Improve the general security awareness of employees who work with finances, but also focus on antiphishing practices.
- Install a protective solution with active behavioral analysis technologies such as Kaspersky Endpoint Security for Business.
