Odinaff Trojan attacks banks and more, monitoring networks and stealing credentials

By Danny Palmer

Published: 2016-10-11 · Archived: 2026-04-05 21:37:25 UTC

Cybercriminals are targeting banks in the UK and around the world with new Trojan.

Image: iStock

A previously undocumented banking Trojan is targeting financial institutions across the globe and is being used by cybercriminals to spy on networks of compromised organisations and stealthily defraud them of funds.

The Odinaff trojan has been active since January this year, carrying out attacks against organisations operating in the banking, securities, trading, and payroll sectors, as well as those which provide support services to these industries.

According to cybersecurity researchers at Symantec, the Trojan contains custom-built malware tools purposely built for exploring compromised networks, stealing credentials, and monitoring and recording employee activity in attacks which researchers say can be highly lucrative for hackers -- and bear the hallmarks of the Carbanak financial Trojan.

Those behind Odinaff are using a variety of techniques to break into the networks of targeted organisations: the most common method of gaining access is tricking employees into opening documents containing malicious

macros.

While macros are turned off by default in Microsoft Word, the recipient can opt to enable them -- which they're encouraged to do by a malicious attachment -- at which point the Odinaff Trojan will be installed on their system. One way a user can avoid being infected in this way is simply to keep the default setting of not allowing macros to be disabled.

Odinaff lures victims into enabling macros and allowing the Trojan to be installed.

Image: Symantec

Another common technique involves the use of password protected .RAR archive files, which trick the victim into installing Odinaff. While cybersecurity researchers haven't been able to determine how these malicious documents and links are distributed by cybercrminals, it's believed spear-phishing is the main method of deployment.

Odinaff is a sophisticated Trojan which is capable of taking screenshots of infected systems between every five and 30 seconds which it sends back to a remote command-and-control server. The Trojan also downloads and executes RC4 cipher keys and can issue shell commands.

Once the Odinaff Trojan has performed the initial compromise of the infected machine, a second piece of malware known as Batel is installed. This second malware infection is capable of running payloads solely in the memory, effectively enabling it to stealthily run in the background.

Given the specialist nature of these attacks, Odinaff requires large amount of manual intervention, with those involved carefully managing attacks and only downloading and installing new tools when required, suggesting that the group behind it is sophisticated and well resourced.

Indeed, cybersecurity researchers suspect that Odinaff is in fact related to the Carbanak hacking group which has stolen over one billion dollars from banks since first appearing in 2013. Researchers note that one of the IP addresses used by Odinaff has been mentioned in connection to the Oracle Micros breach, an attack which saw the compromise of hundreds of point-of-sale devices.

In addition to this, three Odinaff command and control IP addresses have been connected to previous Carbanak campaigns, which saw banks in 30 countries being targeted by criminal actors suspected to originate from Russia, Ukraine, Europe, and China.

While many cyberattacks against banks are limited by region -- for example, Zeus Trojan variant Panda specifically targeted Brazil in the run-up to the country hosting the Olympic Games -- the fact that like Carbanak, Odinaff is targeting financial institutions across the entire globe could ultimately mean the two types of attack are related.

Banks across the world have been attacked with this Trojan, but it's banks in the US find themselves most targeted by Odinaff, followed by Hong Kong, Australia, and the UK.

The countries most targeted by Odinaff

Image: Symantec

The Odinaff group is just the latest in a line of cybercriminal groups who've realized that while it's -- in theory -- much harder to infiltrate the networks of a bank, the potential payoff can be very, very lucrative. The GozNym banking Trojan and the data-stealing Qadars Trojan malware are other examples of how hackers are trying to break into banks.

Read more on cybercrime

- Fighting a hidden enemy: Why banks need to step up the war on cybercrime
- How to empty your bank's vault with a few clicks and lines of code
- Hackers hit central banks in Indonesia and South Korea
- Malware strikes Starwood, Marriott and Hyatt hotels, exposing customer card data [CNET]
