Almost 100 Organizations in Brazil Targeted with Banking Trojan

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/banking-trojan-latam-brazil

Threat Hunter TeamSymantec

Up to 100 organizations in Brazil have been targeted with a banking Trojan since approximately late August 2021, with the most recent activity seen in early October.

This campaign appears to be a continuation of activity that was published about by researchers at ESET in 2020. The attackers appeared to be undeterred by exposure and Symantec, a division of Broadcom Software, has found a large number of new indicators of compromise (IOCs) relating to this latest wave of attacks.

Symantec's Threat Hunter Team first became aware of this recent campaign when suspicious activity was spotted in a customer environment on September 30, 2021. This initial suspicious activity was detected by our Cloud Analytics technology, and further investigation found that attempts were being made to download a suspicious file named mpr.dll onto the customer's environment. Msiexec.exe was attempting to download the file

from a suspicious URL. Further analysis indicated that five files were downloaded, four of which were signed and appeared to be legitimate DLL files, but the file named mpr.dll was not signed and was suspiciously large for a single DLL file at 588 MB. Symantec researchers concluded that this was a “Latin American banking Trojan”, due to the similar characteristics and file names seen in this campaign and in the research into Latin American banking Trojans published by ESET in 2020.

Further investigation by our analysts revealed similar activity had been aimed at multiple different organizations since late August 2021. In fact, as many as 98 organizations may have been targeted with similar activity, with all affected organizations based in Brazil.

The sectors targeted with this activity included information technology, professional services, manufacturing, financial services, and government.

What is a “Latin American banking Trojan”?

Banking Trojans are a type of malware designed to steal victims’ online banking information so malicious actors can access victims’ bank accounts. Once on a machine, the malware typically works by monitoring the websites victims are visiting and comparing these to a hardcoded list. If the victim visits a banking website the Trojan will generally display a spoofed login page in a pop-up over the legitimate page in an attempt to harvest victims’ banking credentials. These pop-ups are generally made to imitate the specific banks’ legitimate login pages and are often quite convincing.

While once one of the biggest threats on the cyber-crime landscape, banking Trojans have been usurped in many parts of the world by ransomware in recent times. However, in Latin America particularly they still dominate a lot of cyber-crime activity.

In its 2020 report, ESET determined that there were 11 banking Trojan gangs operating in Latin America, and that these groups cooperated with each other. It came to this conclusion due to the many shared tactics, tools, and procedures used by the cyber criminals deploying banking Trojans in Latin America.

Attack chain for recent activity

We did not observe what the initial infection vector was in this campaign, but it was likely a malicious URL spread via either spam email campaigns or through malvertising, which is typically the first step in Latin American banking Trojan campaigns. Victims are then directed to one of the following malicious URLs:

- hxxps://centreldaconsulta[.]com/
- hxxps://www.centralcfconsulta[.]net/
- hxxps://centralcfconsulta[.]net/index3.php?api=vFUMIfUzGz2QdjxTFKAMyTlh
- hxxps://centralcfconsulta.net/

- hxxps://www.centralcfconsulta[.]net/index3.php?api=r0ubnHRxDycEy5uFPViNA55Y3t
- hxxps://www.centralcfconsulta[.]net/index3.php?api=4DQSbdp3hLqPRGTbOGtl7jCD9FKNViKXmKd9Lv
- hxxps://centreldaconsulta[.]com/index3.php?api=nJsdr1J3h0fsG18sRAVQt6JjVW
- hxxps://centreldaconsulta[.]com/index3.php?api=ThMyMCAQEOLIC9nO
- hxxps://www.centralcfconsulta[.]net/index3.php?api=wen1eIFCeUh0jAS3mWIDUhSLt3sXMQ

Victims are then redirected to an Amazon Web Services (AWS) URL, which it appears the attackers abused to use as a command-and-control (C&C) server. A ZIP file that contains a Microsoft Software Installer (MSI) file is downloaded from the AWS infrastructure.

ESET reported that most gangs deploying banking Trojans in Latin America had started using MSI files as an initial download in 2019. An MSI file can be used to install, uninstall, and update applications running on Windows systems.

If the victim double-clicks the MSI file inside the downloaded ZIP, it will execute msiexec.exe, which then connects to a secondary C&C server to download another ZIP file containing the payload (mpr.dll), along with other legitimate portable executable (PE) files. The URLs observed being accessed by msiexec.exe included:

- hxxp://13.36.240[.]208/ando998.002
- hxxp://13.36.240[.]208/msftq.doge
- hxxp://15.237.60[.]133/esperanca.lig2
- hxxp://15.237.60[.]133/esperanca.liga
- hxxp://52.47.163[.]237/microsft.crts
- hxxp://52.47.163[.]237/nanananao.uooo
- hxxp://15.237.27[.]77/carindodone.ways

The extracted ZIP file contains a renamed legitimate Oracle application - VBoxTray.exe. This is executed to load the payload (mpr.dll) by way of DLL search-order hijacking. DLL search-order hijacking takes advantage of how Windows handles DLLs to allow an attacker to load malicious code into a legitimate process. The mpr.dll file is also bigger than 100 MB in order to evade submission to security services, which tend not to process files above that size. Both of these files and this exact same process were observed in the banking Trojan activity detailed in ESET's report.

Persistence is then created for the renamed VBoxTray.exe so that mpr.dll is always side-loaded into it by way of either Windows Registry or Windows Management Instrumentation (WMI). This is another common technique used in the attack chain for Latin American banking Trojans.

Stay alert for this activity

The various steps taken by the attackers behind this activity to evade detection - such as using a large file for the payload so that it won't be scanned by security software, and leveraging legitimate processes and applications for malicious purposes - show that those behind this attack campaign are reasonably sophisticated actors. The number of organizations affected in this campaign also indicates that a large number of people are likely responsible for this activity - and it may be that more than one group is behind this activity. It could be a number of groups acting in a cooperative manner, as ESET said may be the approach taken by the various banking Trojan attack groups operating in Latin America.

While ransomware dominates much of the discussion on the cyber-crime landscape at the moment, it is important to remember it is not the only threat out there. Banking Trojans have the potential to be a costly problem for individuals and organizations, so people, especially those based in Latin America where this activity appears to be particularly prevalent, need to remain alert to this threat.

Simple steps, like ensuring you have multi-factor authentication enabled on all financial accounts, can help lessen the impact of threats like these.

Protection

File-based:

Infostealer.Bancos

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise (IOCs)

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.