appgate

CASE STUDY

A LARGE MULTINATIONAL BANK EMPLOYS PROACTIVE MALWARE DETECTION TO STOP FRAUD ATTACKS AND PROTECT ITS CUSTOMERS FROM ZEUS PANDA, MARCHER TROJANS

SUMMARY

This bank approached Appgate to address concerns about malware attacks against their customers. We discovered an attack campaign actively targeting the institution, employing two notorious banking Trojans – known as Zeus Panda and Marcher.

Today, Appgate's Detect Safe Browsing (DSB) Framework is integrated into all of the bank's web and mobile platforms. The clientless solution from DSB Framework analyzes the bank's online platforms to check if they have been tampered with, while our client-side solution detects the presence of financial malware on user devices, and blocks the transmission of pilfered credentials to cybercriminal command-and-control servers. Finally, DSB Mobile integrates into the financial institution's mobile app to provide a highly secure connection between the mobile banking platform and the customer's device

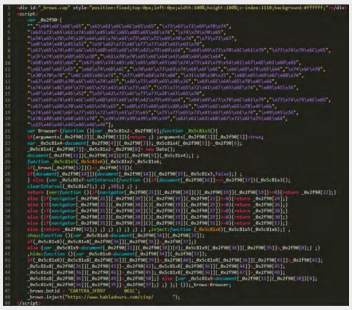
SOPHISTICATED TROJANS TARGETING THE BANK

The Zeus Panda malware injection that we found targeting the bank was particularly potent due to its ability to capture not just user login credentials, but also second-factor authentication (2FA) passcodes. It did this one of two ways, depending on whether the malware was targeting a corporate or personal bank customer.

In the case of corporate customers whose computers were infected by Zeus Panda, the Trojan injected a malicious script into the bank's login page, adding an extra form field for the 2FA one-time password (OTP). The user would obtain their OTP, and if they entered it into the malicious field, it would be captured by the attackers – along with their login credentials.

On the other hand, personal banking customers attempting to log into their bank accounts from infected computers were directed by the malware to a bogus page where they were asked to download a mobile application (the Marcher Trojan) onto their phone. If the user did so, it would enable the cybercriminals to intercept the SMS-delivered OTP authentication sent to the Marcher Trojan posing as the bank's legitimate mobile app.

Zeus Panda silently lies in wait on an infected machine until the customer attempts to log into the target bank's webpage and, when they do, it injects its malicious script, compromising what the user sees on what would otherwise be a legitimate webpage.



The malicious JavaScript, in purple, taht was injected into the bank's login page when an infected user attempted to login

THE NEED

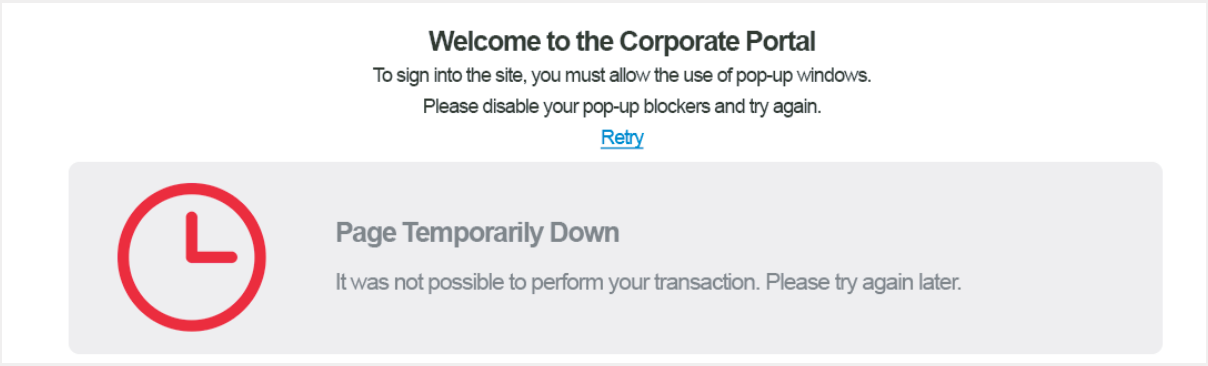
In a coordinated attack campaign, fraudsters targeted a financial institution's customers with two different kinds of malware. The bank needed to quickly detect and mitigate the threats, and prevent them from victimizing customers and stealing account funds.

SOLUTION IMPLEMENTED

The DSB Framework secures the connection between a bank's platform and the customer's device so that transactions can be made safely, even on malware-infected devices. The solution can also detect and neutralize any malware present on laptops, mobile phones and tablets. Further, the DSB Framework detects whether any malicious code has made its way onto the bank's login pages, helping secure the financial institution's entire customer base, no matter what kind of device they choose to do their banking on. The combination of these detection and safe-connection capabilities made both the Zeus Panda and Marcher Trojans powerless to carry out financial theft.

THE BENEFITS

A very flexible, powerful and stable access
The multi-pronged malware defense strategy detects and neutralizes sophisticated attacks of all kinds, including banking Trojans and Man-in-the-Middle attacks, keeping customer accounts safe from unauthorized entry into their online bank accounts



THE PAGE DISPLAYED AFTER THE ZEUS PANDA TROJAN SUCCESSFULLY

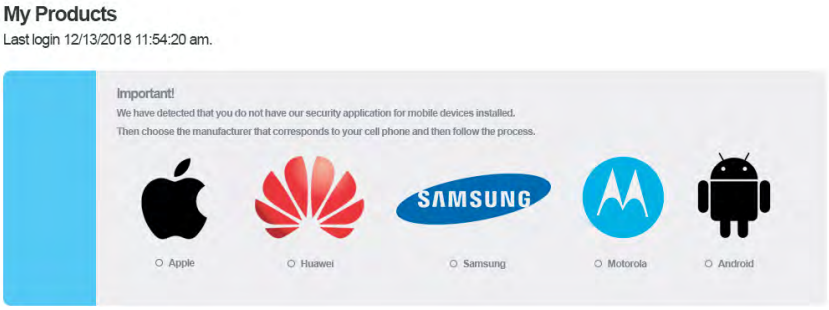
FROM ZEUS PANDA TO MARCHER

How the malware behaves after injection depends on what kind of bank customer the compromised user is. The 2FA process for corporate customers is more secure than that offered to personal customers, and the Trojan cannot gain access to it. To get around this, the malware simply asked for it, and the corporate user – likely thinking nothing was amiss – entered the out-of-channel OTP they received in the malicious form field. When they did so, they were directed to a screen that stated: "Page Temporarily Down" This was a smokescreen designed to confuse the user.

For personal customers who had been tricked into divulging their login credentials, a separate screen was displayed that directed them to download what appeared to be the "latest mobile security app" from the bank. Users who believed that their Bank must have deployed a new security measure to keep them safe (albeit without previously telling them about it), would likely follow through with the process.

Users were then directed to download the malicious application posing as new security app – not from an official app store, but from a link provided by the cybercriminal – and once they did so, the personal customer's mobile device would be infected with the Marcher mobile banking Trojan.

With the Marcher Trojan in play, the cybercriminal was now ready to capture the 2FA provided by the bank, but unbeknownst to the customer, the security measure had been circumvented. The hacker now had all he needed to steal the customer's account funds at will.



Zeus Panda Trojan directing a personal banking customer to download "the latest security app" that is, in reality, the Marcher mobile banking trojan.

HOW APPGATE DETECTED AND HELPED THE BANK MITIGATE THE THREATS

Our Detect Safe Browsing (DSB) Clientless solution detected the presence of the malware injection on the transactional page when a customer whose device had been infected with the malware visited the site. DSB then provided actionable evidence in the form of a screengrab using the solution's Malware Snapshot feature, which included the username of the victimized customer. This enabled the institution to take immediate action to mitigate the attack, including automated blocking of any infected sessions and contacting the first victims to further investigate threat vectors and malware strains used in the attack.

Our mobile safe-browsing solution, DSB Mobile, protects all communications between a financial institution and its customers through a banking application, meaning that malicious apps like Marcher can't capture user information or 2FA. Indeed, the malware's interception of SMS messages serve as a good reminder that regulatory bodies throughout the world are no longer recommending SMS messages for two-factor authentication because of situations like this. Further, in cases of malicious apps that deploy other credential-stealing techniques (such as an overlay attack, keyloggers, or pharming), DSB Mobile safeguards against those as well. In the case described above, the malicious apps used in the attack were quickly added to a blacklist, so subsequent customers wouldn't download them in the first place.

Finally, bank customers who downloaded and installed DSB Client on their PCs were automatically protected thanks to the incorporation of the attack's details from our knowledge base.

The DSB Client was able to effectively neutralize the effect of Zeus Panda and all other banking Trojans by cutting off the malware's ability to communicate with the attackers' command-and-control structure, and Appgate Security Operations Center agents ultimately removed the C&C servers from the internet.

Appgate has been closely tracking the evolution of the Zeus Panda Trojan, giving us the ability to detect when cybercriminals attempt to develop or repackage the malware or its command-and-control servers – and when we do, we react accordingly. Doing so effectively defuses any future attacks – so much so that it was no longer profitable for the hacker group to attempt to relaunch the attack going forward.

ABOUT APPGATE

Appgate. brings together a set of differentiated cloud- and hybrid-ready security and analytics products and services. These include Appgate SDP, the industry's leading software-defined perimeter solution, the Total Fraud Protection suite of risk-based authentication and digital threat protection capabilities and a range of innovative threat management and analytics offerings including the Brainspace digital investigations platform and the company's Immunity range of offense-oriented software and adversary simulation services. Today, these products secure more than 1,000 organizations across 40 countries.

appgate