# Chthonic Banking Trojan

This is a security alert for all TruShield clients, the financial services industry, and the community as a whole. We have learned of a new variant of the Zeus Trojan called Chthonic Banking. This Trojan uses PayPal as a technique to spread.

## About Chthonic Banking Trojan

Chthonic was discovered by Proofpoint analysts. This Trojan uses email to spread and the emails used are from legitimate services like PayPal. The malicious actors send an email to the intended victim. As an example, one email was observed closely by Proofpoint analysts. The subject of the email contained the phrase “You’ve got a money request” and appeared to have come from PayPal. According to Proofpoint, the senders of the emails are not spoofed and are legitimate or stolen PayPal accounts. The malicious actors use their account to request money

The problem is that because this email is sent from a legitimate service, and is a legitimate account, it is not being blocked, due to its non-malicious intent. Within the body of the email that was sent a malicious URL is inserted into the notes section of the PayPal money request page. The malicious actors use social engineering tactics to get their victims to click on the malicious link that they included within the specially crafted message. Of course, if any person were to receive such an email, they would hopefully raise concerns due to a lack of memory about the money owed or from wanting to find out more about this request they received. So, the likelihood of users clicking on the malicious link is very high because it deals with money, and most individuals do have different financial accounts connected to their PayPal account.

Once the malicious link is clicked the users are taken to a different website that downloads an obfuscated JavaScript file. If the user decides to open the file, then an executable containing the Chthonic Trojan and a second payload AZORult is downloaded. This particular campaign bypasses security measures put in place because of the legitimate use of non-malicious services like PayPal.

## Indicators of Compromise

| **URL in the email message:** |
|---|
| hxxp://goo[.]gl/G7z1aS?paypal-nonauthtransaction.jpg] |
| **URL after the goo.gl redirect (hosting the js):** |
| [hxxp://katyaflash[.]com/pp.php] |
| **SHA256 paypalTransactionDetails.jpeg.js:** |

| |
|---|
| 865d2e9cbf5d88ae8b483f0f5e2397449298651381f66c55b7afd4b750eb4da4 |
| **URL JavaScript payload flash.exe:** |
| [hxxp://wasingo[.]info/2/flash.exe] |
| **SHA256:** |
| 0d2def167ecf39a69a7e949c88bb2096cfd76f7d4bf72f1b0fe27a9da686c141 |
| **Domain Chthonic C&C:** |
| kingstonevikte[.]com |
| **URL Chthonic 2nd Stage hosting:** |
| [hxxp://www.viscot[.]com/system/helper/bzr.exe] |
| **SHA256 Chthonic 2nd Stage (AZORult):** |
| 10d159b0ddb92e9f4b395e90f9cfaa554622c4e77f66f7da176783777db5526a |
| **URLAZORult C&C:** |
| [91.215.154[.]202/AZORult/gate.php] |

## Mitigation

- Avoid clicking on links in an email. Type the website address directly into the search bar to navigate to a particular business page.
- Consider using open source analysis tools to analyze URLs within an email.

## Conclusion

Zeus continues to evolve and remains a prominent Trojan in the banking malware family. Its campaign uses social engineering tactics through legitimate services to scare its victims into downloading this malicious new variant of the Trojan Chthonic. This raises concerns about the fact that this maybe the new path that other malicious campaigns may take to avoid being detected by other antiviruses.

## References

https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan

http://news.softpedia.com/news/chthonic-banking-trojan-distributed-via-legitimate-paypal-emails-506659.shtml

http://www.theinquirer.net/inquirer/news/2466291/hackers-spreading-chthonic-zeus-malware-via-legitimate-paypal-emails

**TruShield Security Solutions**

TruShield is a leading provider of Managed Security Services across the globe. We are dedicated to helping companies achieve success by making sure they are properly prepared against the current and emerging threats in today's digital world. Our service offerings include: Continuous, 24/7/365 Monitoring, Penetration Testing and Vulnerability Assessments, Audit and Compliance, and many other Managed Services such as Managed Firewalls and Hosted Log Management. We also offer Security Awareness Training and Management Consulting services.

Contact us today to find out how we can help you protect your organization and safeguard your information.

### Contact Information:

Email: support@trushieldinc.com
Web: www.trushieldinc.com
Phone: (877)-583-2841

### Follow us on:

Twitter: @TruShield
LinkedIn: https://www.linkedin.com/company/trushield-security-solutions
Facebook: https://www.facebook.com/trushieldinc