CYBONET

www.cybonet.com

PineApp Mail Secure Anti-Phishing White Paper

About CYBONET

CYBONET, formerly PineApp, was originally established as an Email Security Solutions Company. Since 2002 CYBONET's internet security and network control products enable SMB/Es and Telcos to comprehensively protect their critical network infrastructure. Whether through the flagship PineApp Mail Secure solution or the next generation of Cyber Protection solutions, CYBONET is dedicated to security. With a renewed emphasis on our valued Partner community as well as the development of a platform for Managed Service Providers to more efficiently deliver our solutions, CYBONET is committed to bringing our technologies to all corners of the globe.

For further details, contact info@cybonet.com

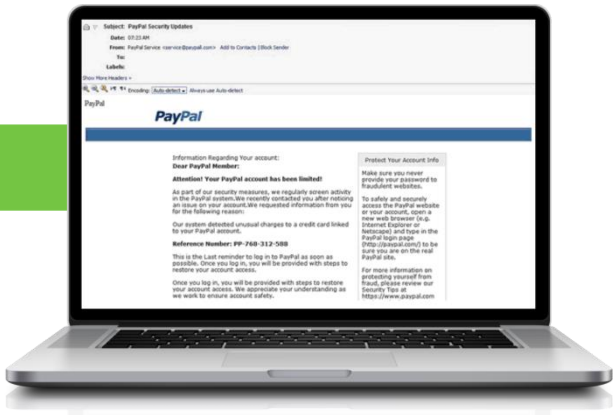
Introduction

Phishing is a form of identity theft which deceives both businesses and customers into giving out personal information, such as credit card and bank account details. People are easily tricked since many corporations, including banks, offer their customers access to their accounts over the web. Therefore, when hackers send spam emails containing links which lead to what appear to be legitimate websites, customers and businesses are easily fooled into inputting their personal information.

Signs of a Phishing Scam

At first glance, it may not be obvious to the recipients that the message in their inbox is not from a legitimate business. This is because Phishing scammers send emails that appear to come from trustworthy sources, by using their official logos as well as the ‘from’ field of the email containing the .com address of the company mentioned in the email. The email will most likely also contain a clickable link which will appear to take you to the company's website. However, clicking on the link will redirect you to a spoofed website which will then demand you to input personal data such as credit card details in order to solve a problem and stop your account being shut down. It is important to be wary of emails containing links, particularly from banks, since banks widely practice the policy of not sending emails with links to personal accounts.

Here is an example:



Subject: PayPal Security Updates
Date: 07:23 AM
From: PayPal Service <service@paypal.com>
To:
Labels:

Encoding: Auto-detect

PayPal

Information Regarding Your account:
Dear PayPal Member:

Attention! Your PayPal account has been limited!

As part of our security measures, we regularly screen activity in the PayPal system.We recently contacted you after noticing an issue on your account.We requested information from you for the following reason:

Our system detected unusual charges to a credit card linked to your PayPal account.

Reference Number: PP-768-312-588

This is the Last reminder to log in to PayPal as soon as possible. Once you log in, you will be provided with steps to restore your account access.

Once you log in, you will be provided with steps to restore your account access. We appreciate your understanding as we work to ensure account safety.

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal login page (http://paypal.com/) to be sure you are on the real PayPal site.

For more information on protecting yourself from fraud, please review our Security Tips at https://www.paypal.com

Phishing Growth

● ● ●

Phishing is a serious threat to both consumers and businesses. 90% of Phishing attacks involve attempts to steal credit card information.

Spear Phishing is particularly dangerous as it usually involves sending emails from companies that customers are already conducting business with. Since the email appears to be from someone known, consumers are more likely to give up their personal and credit card information much more freely.

Recent Phishing Scams

● ● ●

Netflix – As recent as July 2016 scammers sent an email claiming to be from Netflix. They asked users to re-input their information in order to prevent their account from being closed, resulting in the identify theft of the customers' personal information.

Apple – Similarly with Apple, a phishing scam involved scammers being sent an email or text saying that their account was wrongly charged. Hackers then sent a link encouraging customers to input their credit card and bank information in order for them to be refunded appropriately. The scammers then fraudulently stole this information for their own use.

Anti-Phishing

● ● ●

PineApp Mail Secure's Anti-Phishing module combines several layers and technologies to detect and block Phishing attempts. The main technologies used are:

Anti-Phishing Database

PineApp Mail Secure maintains a database which is updated on a daily basis. This database features millions of known Phishing URLs and domain names. If one of the listed URLs appears in a mail, it is blocked.

SURBL

A RBL (Realtime Blackhole List) which is designed to block or tag Phishing attempts based on URIs (usually their domain names) scattered in the message's body. In this case, the RBL is not intended to block the source of the spam message. Instead, SURBL is used to block spam based on its message content. Even if a spammer uses new domains, they may point to the old, blocked IPs and will therefore be blocked, right from the first spam message received.

Heuristic Fraud detection sets of rules

PineApp Mail Secure uses Heuristic rules in order to detect possible new Phishing attempts. PineApp Mail Secure has over 2,500 sets of rules to detect characteristics of Phishing. The heuristic engine uses a score-based system to identify Phishing.

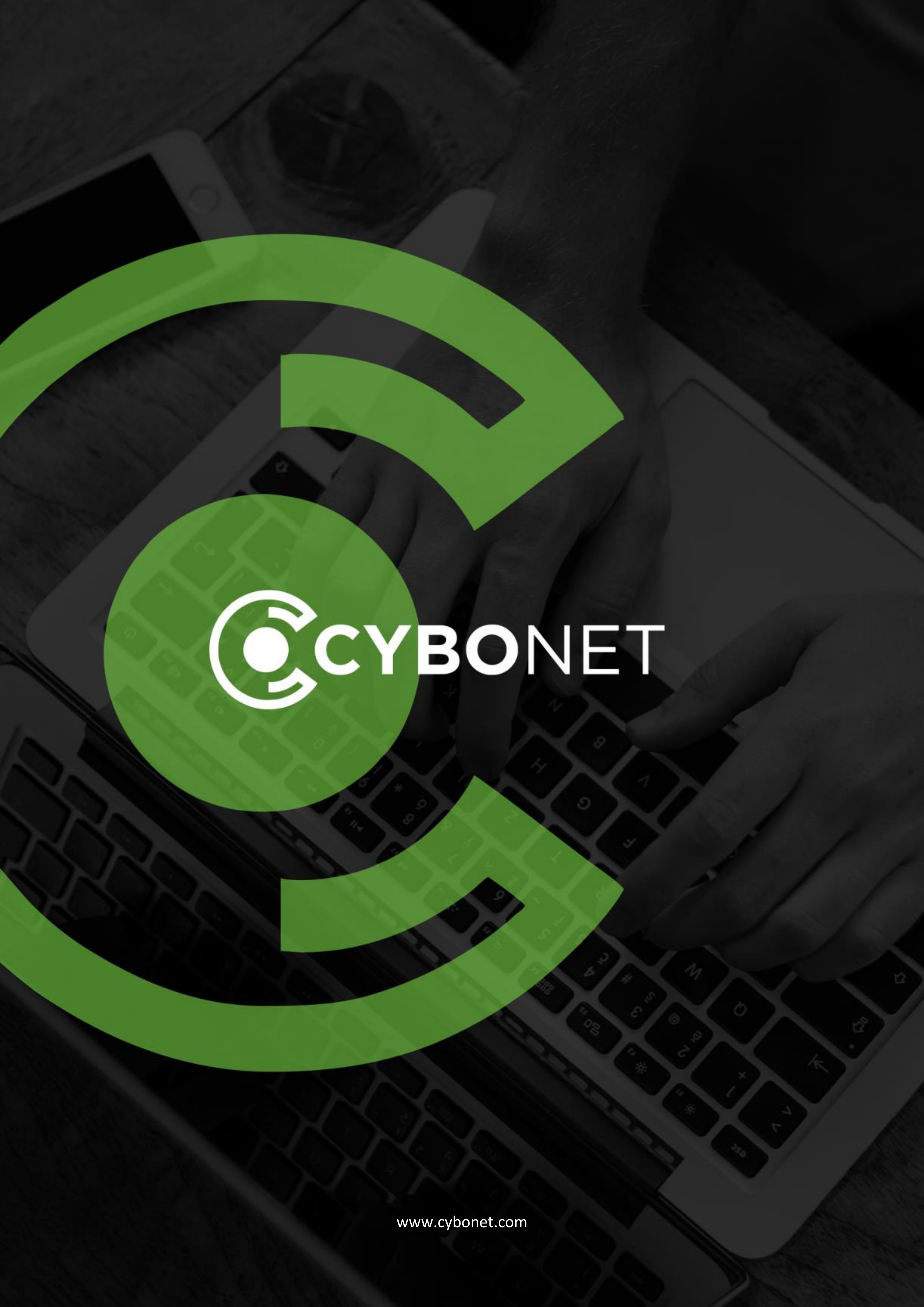
Zombie detection

Most Phishers use zombie computers to distribute their emails. Zombie computers are computers that were involuntarily hacked (whether by Trojan horses or by direct hacking) and are being used for mail distribution.

PineApp Mail Secure has a unique Zombie Detection System – ZDS. It identifies zombies and automatically blocks them at the session level (similar to RBL). CYBONET has a central ZDS, RBL-like server, which dynamically blocks identified IPs. Since a zombie computer owner can change his IP, ZDS automatically adds or removes IP addresses from blacklists.

IP Reputation

A powerful additional layer used to block Zombies at the SMTP session level. IP Reputation saves bandwidth and lowers the load on your PineApp Mail Secure system.



CYBONET

www.cybonet.com