RLW TECHNOLOGY WHITE PAPER

DNGUARD

THE MODERN CYBER SECURITY THREAT: PHISHING & MALWARE SCAMS

DATE

09 FEBRUARY2021

PREPARED BY

RYAN WADE

HEAD OF INFORMATION TECHNOLOGY

TABLE OF CONTENTS

AN OVERVIEW

The data in this study on phishing & malware scams and responses show that countless organizations are swarmed by suspicious emails targeting employees but are not prepared to process and respond to those threats.
In fact, most organizations feel they have little, if any, expertise in anti-phishing practices, and that their incident response processes are grossly ineffective.
What this tells us is that a vast majority of organizations today are simply unequipped and inexperienced to to deal with phishing & malware scams.

Even after heavy investing in tech, more than 66% of business found email-related threats to be the most threatening to their organizations.
It's clear that major steps need to be taken within a majority of business to address phishing & malware scams effectively.
Chiefly, automation of phishing email analyses, and helping incident responders know the difference between mere noise and legitimate threats to security.

NEARLY 2/3

of surveyed IT executives have dealt with a security incident originating with a deceptive email.

43%

of respondents say their phishing response ranges from "totally ineffective" to "mediocre".

NEARLY 1/2

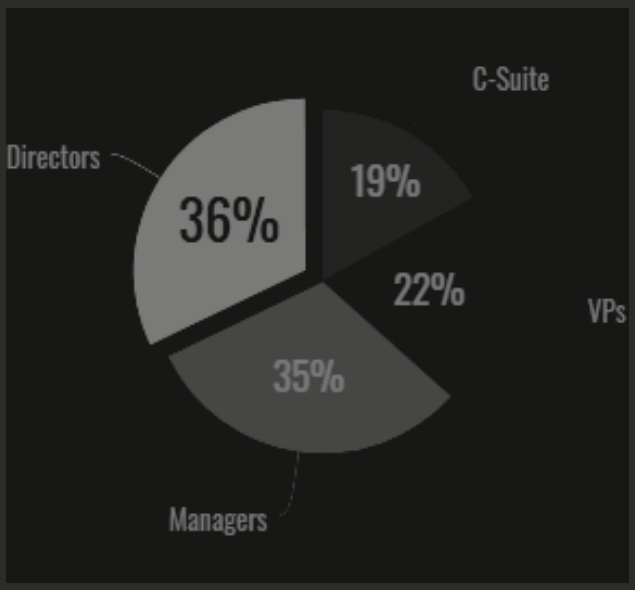
of respondents say their biggest challenge is too many threats and too few responders.

90%

still worry most about email-related threats and scams.

OUR METHODOLOGY

In May 2017, Gatepoint Research surveyed select IT professionals across 1,400 businesses of every size and various industry sector about their phishing & malware response strategies.



MAJORITY OF REPORTED PHISHING SCAMS HAD TARGETED SENIOR DECISION-MAKERS:

BUSINESSES SURVEYED BY YEARLY REVENUE:

% of businesses that earned over $1.5 Billion:
57%

% of businesses that earned $500 Million to $1.5 Billion:
14%

% of businesses that earned under $500 Million:
29%

NUMEROUS INDUSTRIES WERE INVOLVED IN THIS SURVEY AS WELL, INCLUDING:

- Business services
- High tech
- Manufacturing
- Healthcare
- Financial
- Retail
- Trade
- Wholesale trade
- Transportation
- Consumer services
- Telecom
- General

NEARLY 1/3 OF RESPONDENTS SEE MORE THAN 520 SUSPICIOUS EMAILS AND ATTACKS WEEKLY

On top of that, most filtering technologies miss something hugely significant: a potentially costly security breach.

The average employee sees more than 130 emails per day. So it's only natural that phishing & malware is such an effective attack on security.

So how do a handful responders sort through thousands and thousands of attacks manually, to determine whether they are serious threats or just spam? Within the span of an ordinary day it would be impossible.

The answer is two-pronged. Businesses need to discover solutions that:

HOW MANY SUSPICIOUS EMAILS ARE REPORTED IN YOUR ORGANIZATION EACH WEEK?

36% reported under 50 suspicious emails

17% reported 51 to 100 suspicious emails

17% reported 101 to 500 suspicious emails

21% reported over 1000 suspicious emails

LEVERAGE BROADER TEAMS TO IDENTIFY PHISHING

AUTOMATE AND ORCHESTRATE PROTOCOL RESPONSES

PROOF OF CONCEPT ON 50 USER SECURITY BUSINESS ENVIRONMENT.

Over a period of 4 weeks we ran a proof of concept for a security firm in Gauteng, with an office staff count of 50 users.
Before we installed DN-guard the client complained about streaming live CCTV data from their client sites was slow while they had huge ISP bandwidth capacity. Office staff complained about speed in transferring of data or company info within the business and to clients. Client was also worried their IT team was not able to keep up with current threats and ensure the network was secure.

The answer: DN-Guard was installed onto the main router and firewall.

BLOCKING ANY FORM OF ADULT CONTENT, PHISHING OR MALWARE ATTACKS TO THE SITE.

ADDITIONAL SECURITY LAYER 7 SECURITY ENSURING STRICT SECURITY FOR THE SITE.

CLIENT EXPERIENCED A FASTER NETWORK, AND WAS ABLE TO PREFORM ALL COMPANY REQUIREMENTS WITHOUT FAILURE.

DURING THE POC WE PROCESSED THE FOLLOWING STATS.

OVER 27 MILLION

DNS Queries

570 000

Blocked by Filters

167

Blocked malware & phishing

629

Blocked adult websites

32%

Bandwidth Speed Increase

DN-GUARD

DN-GUARD IS DESIGNED FOR ALL ENVIRONMENTS, FROM THE HOME TO SCHOOLS, SME AND CORPORATE ENVIRONMENTS. COVERING A WHOLE NETWORK TO A SINGLE MOBILE DEVICE.

Wish to get in touch and find out more.

WEB: www.rlwtech.co.za
Email: info@rlwtech.co.za

A product of RLW Technology Pty Ltd
www.rlwtech.co.za
info@rlwtech.co.za
0115683305
2021/303894/07

@rlwtechnology

@rlwtechnology

@rlw-technology

+27(0)82 774 5615

Proudly affiliated with EA Services t/a Electair