HACKING EXPOSED

WHAT YOUR CYBERSECURITY VENDOR DOES NOT WANT YOU KNOW

ANSWERS TO 5 KEY CYBERSECURITY QUESTIONS

TABLE OF CONTENTS

INTRODUCTION

Almost every major company experiences at least one cloud data breach each year, whether they realize it or not. Genuine protection against cloud data breaches begins by discovering the answers to the following five key questions.

1. Why do hackers produce free phishing kits?

2. How do professional hackers breach companies *in minutes* when cybersecurity vendors show incredible statistics regarding the number of attacks they block?

3. What's the relationship between malware, exploits, and phishing links?

4. Why are breaches escalating despite historic cybersecurity spending?

5. Can a company really stop a determined hacker from breaching its computers?

1. FREE PHISHING KITS - WHY THEY EXIST

87% of free phishing kits do not use IP Cloaking.

Cloaking is the most effective method for hiding malicious content from security scanners. The hacker's link sends benign content to security scanners and sends malicious content to everyone else. The simplest method is to identify security scanners by their IP addresses. Hiding malicious content based on IP addresses is often called IP Cloaking. IP Cloaking is extremely simple and effective.

Imperva's analysis of 1,019 free phishing kits revealed that 87% were not using IP Cloaking. So why do hackers spend weeks or even months developing free phishing kits only to leave out the very simple inclusion of IP Cloaking? Professional hackers distribute these free phishing kits to advance their own selfish interests. These kits are designed *to be caught*.

Why did a minority of the free phishing kits include IP Cloaking? This small minority of free phishing kits contained backdoors to allow the kit developers to obtain a copy of all stolen data. Hackers include IP Cloaking in these kits because they benefit from the successful evasion of cloud scanners.

2. HOW COMPANIES ARE BREACHED IN MINUTES

"The time from the attacker's first action in an event chain to the initial compromise of an asset is typically measured in minutes."

The 2019 Verizon Data Breach Investigations Report reveals that professional hackers compromise most companies *in minutes*. The report further shows that virtually every company can be breached in less than a day. In other words, companies are routinely hacked in less than a day while cybersecurity vendors tout incredible statistics regarding the number of attacks they block. How can both be true?

Consider the combined findings of Imperva and Verizon. Verizon documents that professional hackers can breach any company they want, while Imperva shows that free phishing kits don't use evasion techniques. In other words, professional hackers feed the cybersecurity vendors' statistics by producing and distributing kits that are designed to be caught. Then professional hackers use standard evasion tactics to enter your computers anytime they want. The next page details precisely how they do this.

3. MALWARE, EXPLOITS, AND PHISHING

94% of malware is distributed by email.

Hackers create malware that exploits a vulnerability in the targeted device. The 2019 Verizon Data Breach Investigations Report found that this malware is distributed via email 94% of the time. Email links (not attachments) were the hackers' preferred delivery mechanism (according to ProofPoint's Q3 2019 Threat Report).

The vast majority of both malware and phishing campaigns are initiated by email links. This is how professional hackers breach any company they want in less than a day. Hackers successfully use email links for the vast majority of hacking even though most companies subscribe to a time-of-click security service. In other words, over 85% of successful hacking attacks use email links that bypass traditional time-of-click security.

Clearly, traditional time-of-click services are not protecting you. In fact, they are the weak link that hackers rely upon to breach your company. The following page explains how hackers bypass them at will.

4. MORE BREACHES WITH MORE SPENDING

Global cybersecurity 2020 spending is expected to exceed $173 billion.

According to Australian Cyber Security Growth Network, global spending on cybersecurity is expected to exceed $173 billion. Yet, companies are getting breached more often than ever. Why?

A survey of over two-thousand live phishing sites revealed that 95% use IP Cloaking to redirect security scanners to benign content. Now here's a stunning truth. Company devices used to be fully protected from IP Cloaking when on-premise scanners were used. On-premise scanners enter the internet through the same gateway that other company devices do, and therefore have the same Internet address as the company devices. Therefore, IP-based cloaking doesn't work.

Cloud scanners have different IP addresses than company devices. Cybersecurity vendors convinced companies to move to the cloud without solving the IP Cloaking issue. As companies moved to the cloud they left the environment where they were safe in order to adopt cloud services that make them defenseless. As more and more companies embraced the cloud, the number of breaches skyrocketed despite the increase in cybersecurity spending.

5. KEEPING DETERMINED HACKERS OUT

"Using redirects to trick link scanning products is nothing new..."

As Rhino Security Labs acknowledged, hackers have been using redirects to bypass known sandbox and threat protection providers for many years (since the advent of cloud adoption). When companies moved to the cloud, they gave hackers carte blanche freedom to breach company computers at will.

If your company wants to keep the convenience of cloud services, your company can use three basic strategies to keep a determined, remote hacker out. First, prevent the hacker's malware from being downloaded (by changing your time-of-click service to one that blocks cloaking). Second, prevent any downloaded malware from being able to reach out to the hacker's command and control center (a separate whitepaper will be released detailing how to accomplish this). Third, try to patch every vulnerability in every device and in every app.

The third strategy is impossible to fully implement. However, the first two strategies can block even the most determined hacker. TocMail Inc. focuses on the strategies that work so that you can finally keep even the most determined hackers out.

IMPLEMENTATION

95% of professional phishing sites use IP Cloaking to bypass email security. Why is this *the* method hackers use for nearly every data breach? The largest cybersecurity vendors' time-of-click services have the following senseless design:

1. The service accesses the original link contained in the email.
2. The service follows the link's redirects until it reaches the final destination.
3. If the path and final destination seem to be fine then the service sends you to the original link.
4. The original link can now send you anywhere it wants, including a different, harmful destination.

Incredibly, the largest cybersecurity vendors' last step is to hand control back to the hacker's link.

Of course your company can easily be hacked with this nonsensical approach. That's why most companies are getting breached each and every year. TocMail solves the time-of-click design flaw via its patented PhishViewer technology. PhishViewer sends you straight to the final destination, not the original link. Therefore, the original link *cannot* take you somewhere else.

Your company can block the vast majority of hacking in minutes, simply by using TocMail's time-of-click service. Our solution is instant to deploy, simple to use, and uniquely effective.

ABOUT US

TocMail stands for "time of click mail." TocMail offers patented time-of-click protection against the hacking technique used in the vast majority of company breaches.

Our commitment is to provide the strongest protection possible against remote hackers. Our innovative solutions keep your company safe in ways that no one else can.

Connect with us today to learn more!

TocMail Inc.
3901 NW 79th Ave.
Suite 245 #873
Miami, FL 33166 U.S.A.
+1 305-728-2043

TocMail.net