CYBERFORCE|Q

January 18, 2023

TLP: Clear - Unlimited disclosure, this information can be shared publicly with everyone.

CYBERFORCE|Q DECEMBER 2022 MONTHLY BULLETIN

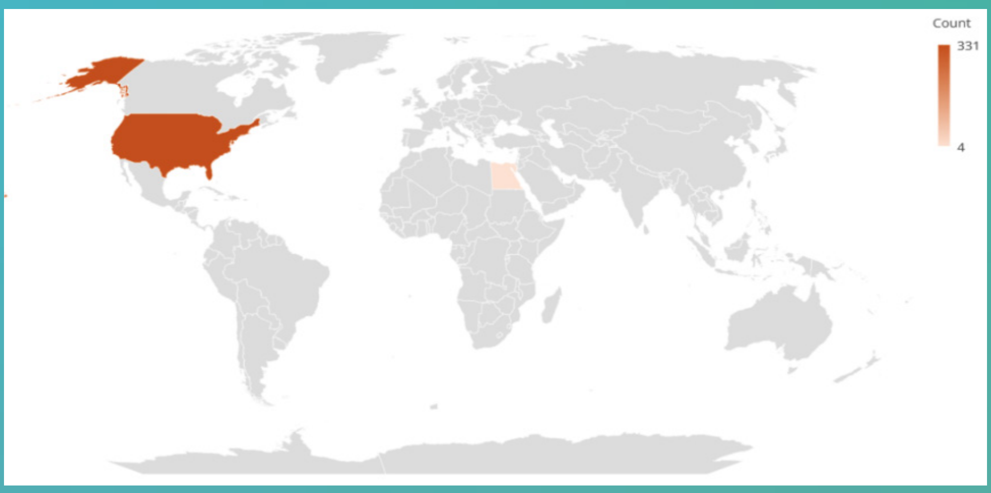
In December, we observed a sustained increase in cyber threats targeting our client organizations. Fortunately, we have also seen improvements in areas such as collaboration, detection and response, and efficient information sharing, which have enabled us to more confidently counter potential threats.

01 Executive Summary

Phishing continues to pose a major risk for organizations and individuals. We have seen a significant increase in the number and sophistication of phishing attempts, with threat actors using increasingly sophisticated techniques to trick users into revealing sensitive information. To protect against phishing, it is essential to implement robust email filtering, multi-factor authentication (MFA), and user education programs, as well as to regularly monitor and review security systems and policies.

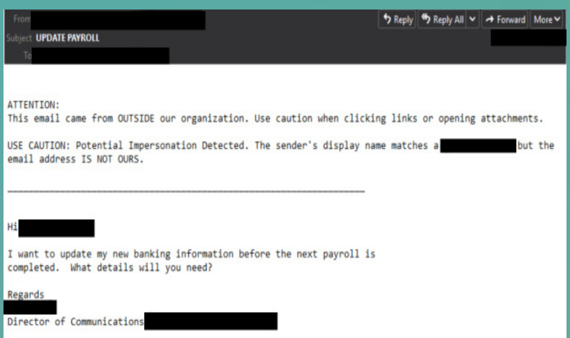
In December, we noticed an increase in phishing activity coming from the United States, with most of the email domains used in these campaigns being registered with either Google (96%) or Apple (4%). This can be particularly effective because trusted email hosting providers like these are often not blocked by security scanners. We also saw a notable phishing activity coming from Egypt. It's worth noting that about 17% of the world's internet traffic passes through Egypt, which makes it a key "choke point" and potentially a vulnerable point for internet security.

The heat map below illustrates each location's traffic volume with colors.



02 Case Study

Impersonation Email Scams on the Rise: How to Protect Your Business



From [redacted]

Subject UPDATE PAYROLL

To [redacted]

[redacted]

ATTENTION:
This email came from OUTSIDE our organization. Use caution when clicking links or opening attachments.

USE CAUTION: Potential Impersonation Detected. The sender's display name matches a [redacted] but the email address IS NOT OURS.

Hi [redacted]

I want to update my new banking information before the next payroll is completed. What details will you need?

Regards
[redacted]
Director of Communications [redacted]

One of the most consistent email-borne threats that our team has observed across multiple client environments is internal impersonation or funds transfer fraud (FTF). In these cases, threat actors use fake email accounts to pose as high-level employees within the company and request changes to their direct deposit payroll accounts. The goal is to obtain sensitive banking information by convincing the end-user to comply with the request.

Common email subject lines often include words like "changes" or "request" in order to grab the recipient's attention-a standard social engineering technique-and encourage them to open the email. For example, a subject line might read "I HAVE A REQUEST" or "Urgent request for information" or "DD Payroll Change". By using language that suggests the email contains important or urgent information, the sender hopes to convince the recipient to open the email and take the desired action.

When our team receives reports of these fraudulent emails, we provide prompt responses and follow up with investigation notes. With the affected organization's authorized consent, we often share this information with other clients in the same industry during our daily meetings. This allows us to keep everyone informed and take action to prevent further attempts from succeeding.

Coalition, a cybersecurity insurance company, reported in their 2022 Cyber Claims Report that the average initial loss (defined as the loss funds before recovery) due to FTF in the first half of 2021 was $388,000, a 78% increase year-over-year. Data breaches, of course, can and do have far-reaching consequences beyond just financial losses, including damage to stakeholder relationships and public trust.

Today, email threats are often designed to evade security scanners and rely on the recipient's lack of vigilance to succeed. Cyber criminals are aware of common security measures and will often tailor their techniques to bypass these defenses. This means that even if an organization has robust security tools in place, it is still important for employees to be vigilant and carefully evaluate each email they receive.

Steps to Mitigate Risk

- Educate employees about the threat of impersonation scams and encourage them to be cautious when receiving requests for sensitive information, especially when the request comes from someone they do not know or trust.
- Implement strict security protocols for verifying the identity of employees before granting access to sensitive information, such as requiring two-factor authentication or using digital signatures.
- Regularly review and update security policies and procedures to ensure that they are effective at protecting against impersonation scams and other forms of cyber-crime.
- Invest in security technologies, such as email filtering and anti-spam solutions, that can help identify and block fraudulent messages before they reach employees' inboxes.

03 External Trend Spotlight

Lilac Wolverine: Nigerian Threat Group Leverages Gift Card BEC Attacks During The Holidays

Lilac Wolverine is a Nigerian threat group that conducts Business Email Compromise (BEC) attacks. They gain access to individuals' email accounts and use them to send large numbers of emails to the contacts on those accounts, asking for assistance with purchasing gift cards. Nigeria has a reputation as a hotbed for BEC activity. During the second half of 2017, researchers at Abnormal observed a sharp increase in the use of gift cards as a payment method in BEC attacks. This has now become the most common way that attackers request payment. This may seem strange, as the average amount requested in gift card attacks is much lower than in other types of BEC threats. However, the main reason for the popularity of gift cards is that they allow threat actors to target a much larger number of individuals.

A successful compromise of an organization's network is capable of not only rendering critical business data inaccessible, but Emotet operators will attempt to extort their victim organizations, often leaving public disclosure of obtained sensitive data as their alternative. According to CheckPoint researchers, Emotet at its peak infected 1.5 million computers globally and caused an estimated $2.5 billion in damages. These damages are not limited to successful extortion attempts but the accompanying business fines, penalties, costs for forensic and investigation activities, and loss of revenue from business downtime, among other expenses.

Contact Us for More Info: ☎ 248-837-1400 ✉ solutions@cyberforceq.com