An Intelligent Driving Enterprise:
CACTER Gateway Escorts O365

CACTER Email Security Gateway System
CACTER邮件安全云网关
Compatible with O365
Interception efficiency up to 99.8%

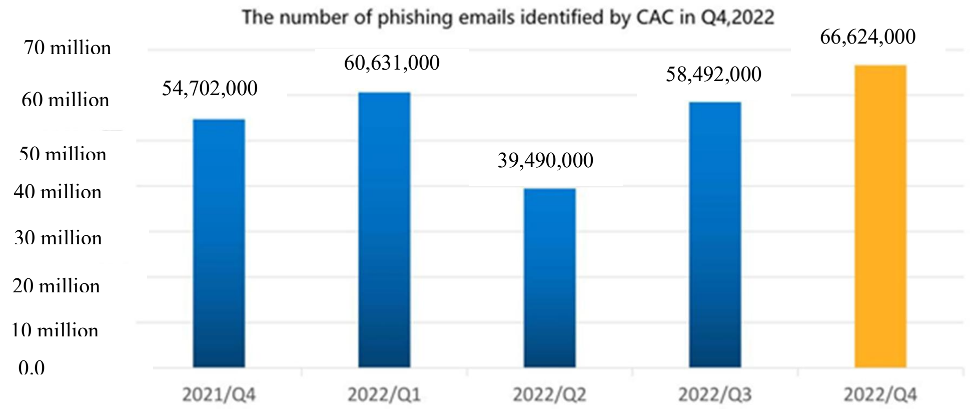
Customer Background

An intelligent driving enterprise is an international creative high-tech enterprise and takes the lead in the field of intelligent driving in the world. It concentrates on offering customers personalized solutions on intelligent driving, to open a new amazing era of intelligence together.

Product used: CACTER Email Security Gateway System

Pain Points and Difficulties

According to data of the Coremail Anti-spam Center, the number of phishing emails identified by CAC was 181 million in 2021 and increased to 225 million and by 24.1% in 2022, which suggests that in 2022, 617,088 phishing emails were daily received and sent on average.



Source: Coremail Anti-spam Center

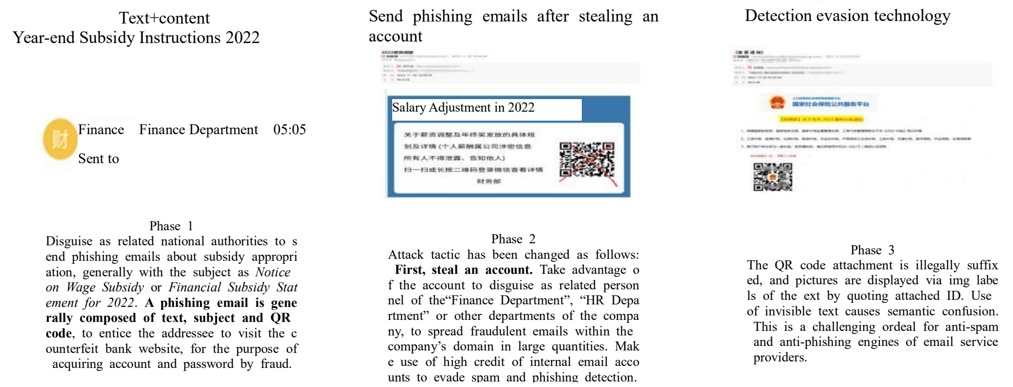
Ownership: CACTER Email Security (cacter.com)

Phishing emails: Addressees are enticed by tactful baits to reply to designated recipients in respect of their confidential information such as accounts and passwords, or they are guided to link to specific webpages, where they enter the confidential information that the attackers want to acquire.

Phishing tricks are so diverse that precautions cannot ward off them. For instance, subjects on talent subsidies, annual bank examinations, express delivery for foreign trade and confirmation of financial settlement entice users to click phishing emails of emails, to steal sensitive data, individuals' bank accounts and passwords, etc.

In respect of this, Coremail anti-spam experts reveal that while security practitioners are facing more terrible ordeals, enterprises bear growing risks and pressure from cybersecurity.

Phishing Emails on [Labor/Talent Subsidies from the Country] - Evolution of Phishing Techniques



Text+content
Year-end Subsidy Instructions 2022

Finance Finance Department 05:05
Sent to

Phase 1
Disguise as related national authorities to send phishing emails about subsidy appropriation, generally with the subject as *Notice on Wage Subsidy* or *Financial Subsidy Statement for 2022*. **A phishing email is generally composed of text, subject and QR code**, to entice the addressee to visit the counterfeit bank website, for the purpose of acquiring account and password by fraud.

Send phishing emails after stealing an account

Salary Adjustment in 2022

关于薪资调整及年终奖发放的具体规划及详情（个人薪酬属公司涉密信息所有人不得泄露、告知他人）
扫一扫或长按二维码登录微信查看详情
财务部

Phase 2
Attack tactic has been changed as follows: **First, steal an account.** Take advantage of the account to disguise as related personnel of the"Finance Department", "HR Department" or other departments of the company, to spread fraudulent emails within the company's domain in large quantities. Make use of high credit of internal email accounts to evade spam and phishing detection.

Detection evasion technology

Phase 3
The QR code attachment is illegally suffixed, and pictures are displayed via img labels of the ext by quoting attached ID. Use of invisible text causes semantic confusion. This is a challenging ordeal for anti-spam and anti-phishing engines of email service providers.

The administrator of this intelligent driving enterprise feels the same. He said,

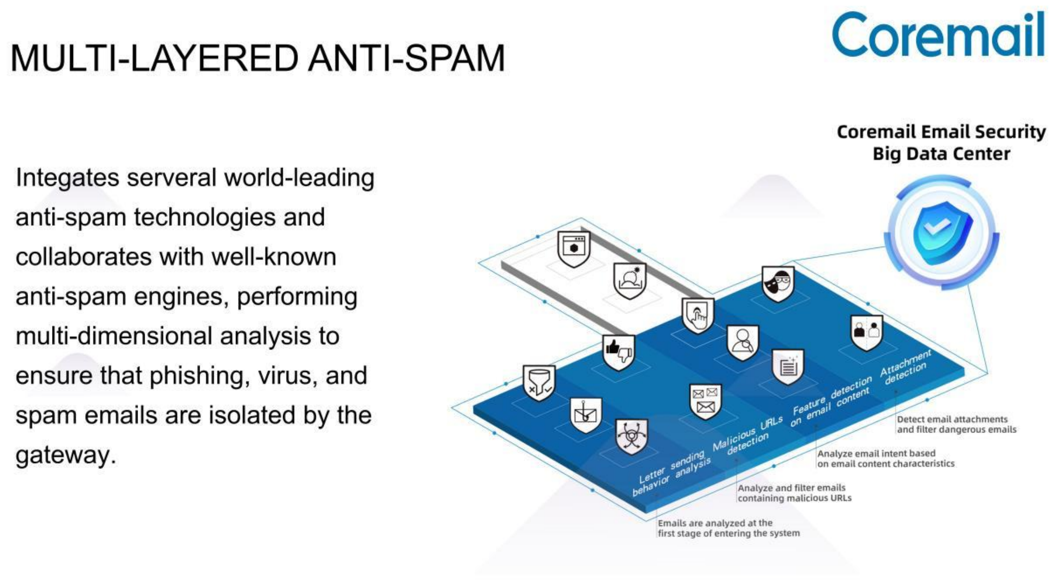
“**In the local domain, a cybersecurity incident ever happened. Users were enticed via a phishing link to fill in their sensitive data such as email account and password. The phishing link was spread very fast and in large quantities.**"

Although this incident was controllable and didn't cause severe consequences, from the perspective of safety and regulation, it was a serious security incident. All of us considered that reliable security products must be used for preventing recurrence of such incidences.

It is understood that t**his intelligent driving enterprises uses O365 as its email system, and merely relies on the email protection function of this system** without deploying gateway products. However, this protective measure is far from enough for an international company. **On one hand, O365 has no functions for checking URL or protecting against malicious files. As a result, its anti-spam capacity has been greatly weakened.** On the other hand, subjects and tracks of phishing emails are constantly changed and upgraded. Inevitably, gateway performances must be improved. Otherwise, enterprises cannot effectively defend against such malicious emails.

Solutions

CACTER email security cloud gateway perfectly satisfies this requirement. It can effectively intercept 99.8% of malicious emails dependent upon its own anti-spam engine and in combination with the anti-spam capacity of the anti-spam center of NERVE 1.0 (a neural network platform).



MULTI-LAYERED ANTI-SPAM

Integates serveral world-leading anti-spam technologies and collaborates with well-known anti-spam engines, performing multi-dimensional analysis to ensure that phishing, virus, and spam emails are isolated by the gateway.

Coremail
Coremail Email Security Big Data Center
Letter sending behavior analysis
Malicious URLs detection
Feature detection on email content
Attachment detection
Detect email attachments and filter dangerous emails
Analyze email intent based on email content characteristics
Analyze and filter emails containing malicious URLs
Emails are analyzed at the first stage of entering the system

The most intuitive feeling of this enterprise is that after deployment of the cloud gateway, it has witnessed a drastic decrease in the number of malicious emails in the local domain. The administrator reported,

"After application of the cloud gateway, the situation has truly improved a lot. No security incident like the last one has recurred, and almost all phishing emails have been directly intercepted by the gateway."

Apparently, after it was attacked by the phishing email, **this intelligent driving enterprise has attached great importance to gateway capacity for intercepting and isolating malicious emails**. Due to Coremail's 24-year foundation building in the email industry, powerful R&D strengthens and good word-of-mouth in the market, CACTER email security cloud gateway has been flavored by the enterprise as its preferred choice. In addition, this cloud gateway has gained trust for its constant stable protection after its launch.

The Administrator said,

"I think content filtration is a good characteristic function. With this function, well-organized phishing emails can be filtered in contents and forms for us accordingly without omission."

The administrator recognized the function, and speaking of user experiences, the administrator also has the say. He said,

"With simple functions, the gateway is easy to master and operate by users, but some small functional modules might be hard to understand by some ordinary operation and maintenance personnel. However, the functions are relatively comprehensive and practical as a whole."

One flaw cannot obscure the splendor of the jade. **CACTER email security cloud gateway was given 9.5 points by this intelligent driving enterprise** (1-10 points). This has greatly boosted Coremail's morale for development in the field of email security and let us realized the major responsibilities we have to shoulder. We will not abuse our customers' trust. Instead, it is our mission and responsibility to create better email security products.