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

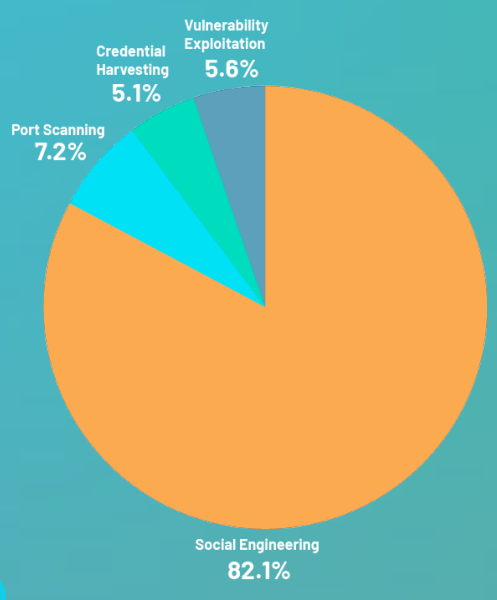
CYBERFORCE | Q

OCTOBER 2022 MONTHLY BULLETIN

Throughout the month of October, the CyberForce | Q team observed phishing (namely social engineering) emails as the primary attack vector for threat actors attempting to gain initial access to internal client systems.

01 Executive Summary

The chart below shows our top four indicator of compromise (IOC) categories for October. Note that Credential Harvesting and Social Engineering are phishing sub-types, thus compromising 87.2% of our top indicators.



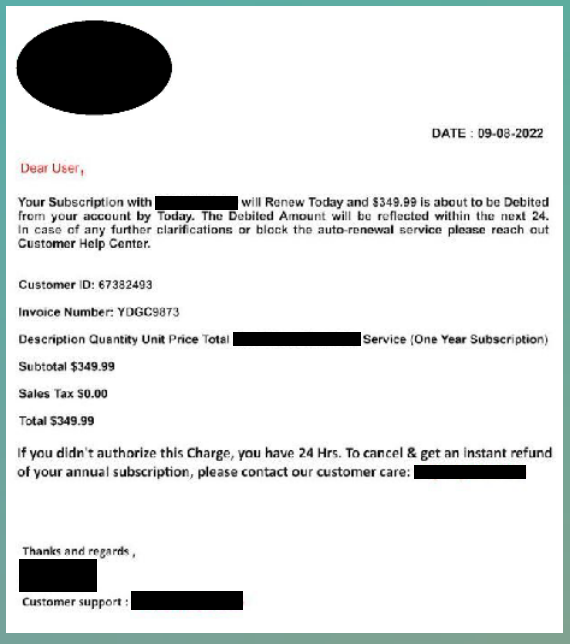
This, of course, is no coincidence. According to Verizon's 2021 Data Breach Investigations Report, 85% of breaches involved the human element, which includes phishing emails. As cyber criminals have become smarter and more efficient in their tradecraft, the number of phishing and social engineering attempts has only increased, year-over-year. This, in turn, can prove costly for an organization, often comprimising one-third or more of a security team's daily workflow allocation.

At CyberForce | Q, not only are our security operations analysts highly trained in identifying phishing emails reported to us by our clients, but our ability to automate the phishing lifecycle workflow process drastically cuts down on the average time in triage.

02 Case Study

Callback phishing campaign targeting users with fake invoice scams

CyberForce|Q observed an ongoing social engineering campaign (a widespread and opportunistic campaign referred to by security researchers as BazarCall) within multiple client environments. The email messages leverage fake, outstanding subscription invoices in an attempt lure corporate users into financial fraud or internal network compromise. The invoice, typically for a ubiquitous service such as Geek Squad or PayPal, includes a callback number for the recipient. If called, they are greeted by a fake customer service agent, who attempts to lure the user into handing over their bank account information or downloading additional software to help remediate the purported issue.



[redacted]

DATE : 09-08-2022

Dear User,

Your Subscription with [redacted] will Renew Today and $349.99 is about to be Debited from your account by Today. The Debited Amount will be reflected within the next 24. In case of any further clarifications or block the auto-renewal service please reach out Customer Help Center.

Customer ID: 67382493

Invoice Number: YDGC9873

Description Quantity Unit Price Total [redacted] Service (One Year Subscription)

Subtotal $349.99

Sales Tax $0.00

Total $349.99

If you didn't authorize this Charge, you have 24 Hrs. To cancel & get an instant refund of your annual subscription, please contact our customer care: [redacted]

Thanks and regards ,

[redacted]

Customer support : [redacted]

On the surface, this phishing trend may appear to be a simple scam attempt with no significant impact on an organization. However, it has the capability to infect a domain user's system with ransomware - a type of malware that cost U.S. organizations $159.4 billion in 2021. A successful ransomware infection can halt business-critical services and operations in often less than 4 hours, thereafter, leaving executive decision-makers in a high pressure legal, ethical, and finacial bind. Moreover, critical infrastructure has become a prime target among cyber criminals leveraging ransomware, as interruptions to bussiness-critical services can have widespread impact to customers, public trust, reputation, revenue, among other areas of impact.

Steps to Mitigate Risk

- Educate your employees on how to recognize the psychological triggers used in social engineering attacks
- Educate your employees and conduct iterative formal security awareness training sessions with mock phishing simulations that mimic trending threats
- Keep all systems current with the latest security patches and updates
- Enforce an organization-wide security policy that includes but isn't limited to password expiration and complexity

03 External Trend Spotlight

Microsoft Confirms Server Misconfiguration Led to 65,000+ Companies' Data Leak

Microsoft confirmed that it inadvertently exposed information related to thousands of customers following a misconfiguration of an internal server, leaving 2.4 terabytes of data, consisting of invoices, product orders, signed customer documents, partner ecosystem details, among other sensitive documents accessible to cyber criminals. Microsoft did not observe any malicious activity during this lapse in security, but such data leaks could be exploited for extortion, social engineering attacks, or a quick profit.

The company said it's in the process of directly notifying impacted customers.