CYBERFORCE Q

December 15, 2022

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

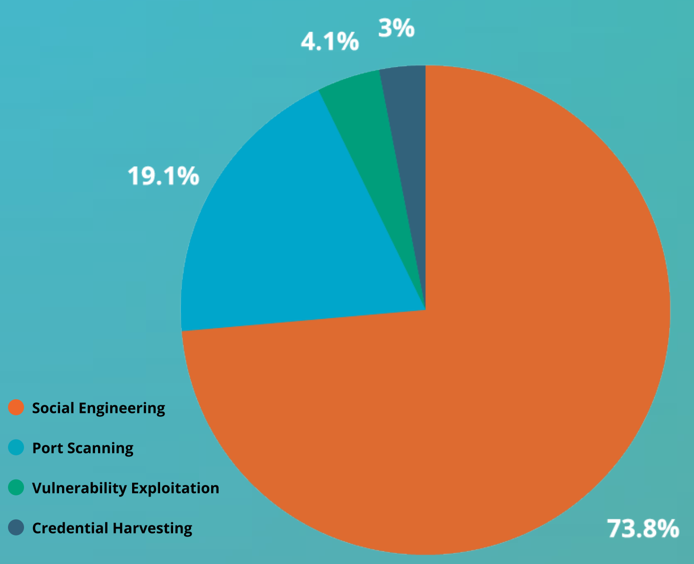
CYBERFORCE | Q NOVEMBER 2022 MONTHLY BULLETIN

As the holiday season gets underway, retail businesses are ramping up their marketing of discounted and limited-time offers for their products and services. To take advantage of this, threat actors are sending out malicious emails that mimic legitimate business discount offers. According to BitDefender researchers, 56% of Black Friday spam emails received during the period from October 26th to November 6th were scams. This number is expected to increase throughout November and December.

01 Executive Summary

Despite the overall trend, the CyberForce|Q team found that reported social engineering attempts decreased by 10% month-over-month. In contrast, port scanning attempts increased by more than 90%. There were minimal changes in credential harvesting and vulnerability exploitation attempts.

The chart below shows our top 4 indicator of compromise categories for November:

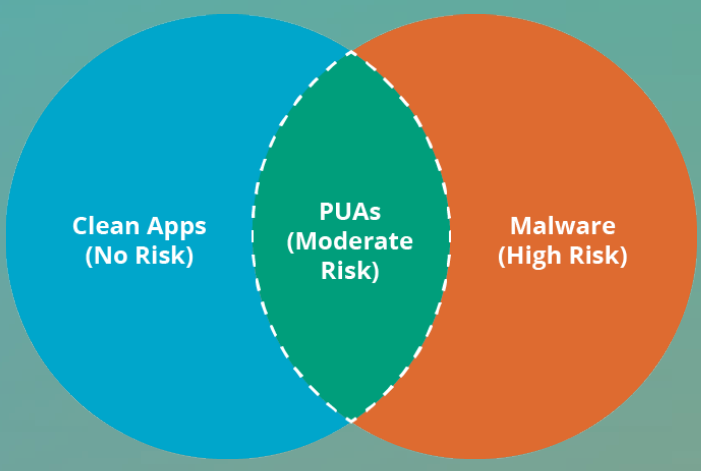


DID YOU KNOW?

Port scanning *is a technique used to identify open ports on a computer system, which can reveal security vulnerabilities. Network services such as internet traffic, email, and VoIP require specific port configurations to work properly. Threat actors may use this information to plan future attacks. While port scanning is not illegal in the U.S., internet service providers may prohibit their customers from onducting unauthorized scans as outlined in their acceptable use policies.*

02 Case Study

PUAs: 'Grey' Software Still Poses Risks to Businesses



Potentially Unwanted Applications (PUAs), also known as greyware, are unwanted software applications, often packaged as smaller, additional components within free software. Many of our client organizations' network monitoring tools notify our CyberForce|Q 24x7 security operations team when their employees attempt to install one of these applications on their corporate devices. Our team then communicates these findings to our client. Throughout November, our team observed a decrease, month-over-month, in PUAs in client environments. This is due, in part, to employee education and awareness of the potential risks of installing unapproved software.

These applications tend to be third-party developed free versions of commercial software. The most common forms of PUAs track, collect, disclose and sell the user's personal information to advertisers during application usage, unbeknownst to the user. This is widely considered an unethical practice because it violates the security interests of users without their informed consent. While this does not cause any immediate damage to the user's computer, cyber criminals can obtain passwords or payment card data or other information not meant for public disclosure, increasing the risk of a more disruptive future security incident, such as identity theft, credit card fraud, or widespread compromise of an organization's internal network.

Steps to Mitigate Risk

- Review the company's Acceptable Use Policy (AUP), which may (and should) include constraints on software downloads. This helps secure computing resources and data from cyber-attacks and data breaches.
- Keep systems and applications current with security–related patches, especially those related to network and internet activity such as browsers, media players, email clients, and news readers.
- If authorized, always download software from the original manufacturer and not from freeware or download portals.
- If you must visit untrusted websites for application downloads, never allow ActiveX controls, browser plug-ins, or other types of applications to be installed on your system.

03 External Trend Spotlight

Emotet Malware Returns After 4-Month Break

During November, CyberForce|Q observed multiple attempts to distribute and infect client systems with Emotet malware. Emotet, globally distributed via widespread spam email campaigns with malicious Microsoft Office file attachments, first observed in 2014 and originally used for foreign cyberespionage, is widely regarded as the most dangerous and sophisticated malware operation of all time. The malware and the criminal gang behind it recently returned after a 4-month break in operation due to coordinated efforts from international law enforcement to disrupt its infrastructure.

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 and penalties, costs for forensic and investigation activities, loss of revenue from business downtime, among other expenses.