Lodestone

NOVEMBER 2022

STATE OF CYBER

monthly newsletter

HOOK, LINE, AND SINKER: PHISHING GROWS EVEN MORE DESTRUCTIVE AS THREAT ACTORS PIVOT TO EMAIL - CONNECTED APPLICATIONS

Lodestone has responded to hundreds of business email compromises (BECs) over the past several years, in which threat actors gained access to a company employee's email account using tactics such as leaked credentials, phishing, and brute force. Once an email account has been compromised, threat actors often begin searching for ways to defraud a company's customers, partners, or employees. This frequently involves searching for invoices or other payments within the account's mailbox that the threat actor can use to attempt unauthorized banking changes. This may include replacing the bank account a third party wires payments for the company to with a bank account controlled by the threat actor.

Lodestone has recently noted an evolution in BECs where threat actors with access to a compromised email account identify connected accounts that could be accessed via single sign-on (SSO) or the shared credentials of the email account. In some cases, threat actors may be able to identify payroll systems or other company payment resources and send a second phishing email to gather banking information or redirect monetary transfers related to payroll or other company-sponsored payments.

As the destructive potential of BECs increase through the targeting of connecting accounts, implementing strong security and best practices within your organization's environment is more critical than ever. Lodestone recommends taking the following steps:

- Enable multi-factor authentication (MFA) across your environment.
- Conduct routine security awareness training and phishing simulations.
- Perform routine auditing of suspicious account activity.
- Implement a policy that requires that all payment changes be confirmed over the telephone between the customer or third party and an established contact at your organization.

CYBERCRIMINALS SEE ALLURE IN BEC ATTACKS OVER RANSOMWARE

While ransomware has been trending for some time, reports published by industry incident response firms note an 84% increase in BEC-related cyberattacks in the first half of 2022.

WHY LOG4TEXT IS NOT ANOTHER LOG4SHELL

A new Apache vulnerability has discovered that organizations should ensure their applications are patched against. It is important to note, however, that this vulnerability does not overtake Log4Shell in terms of severity.

BLACK BASTA RANSOMWARE GANG INFILTRATES NETWORKS VIA QAKBOT, BRUTE RATEL, AND COBALT STRIKE

Trend Micro reports a resurgence in Qakbot, a malware that is commonly trojanized and distributed via phishing email.

CALLBACK PHISHING ATTACKS EVOLVE THEIR SOCIAL ENGINEERING TACTICS

Industry experts have observed a rise in phone-based phishing ("vishing") attempts. Lodestone recommends that organizations ensure that employees receive frequent training to address social engineering both via email and phone calls and maintain a strong security culture.