

Another Version of Zeus is on the Loose

Alert Summary

The Federal Bureau of Investigation (FBI) recently issued an alert on a new version of the Zeus Trojan called Gameover, which is distributed via spear phishing attacks aimed at commercial accounts and ultimately lead to account takeovers. Emails purporting to be from NACHA (The Electronic Payments Association) inform the victim organizations of a failed ACH transaction. The victim's computer is infected with the Trojan when they click on the link contained in the email.

Alert Details

Gameover is used to steal online banking login credentials and can defeat several forms of dual-factor authentication. Cyber thieves initiate large dollar wire transfers from the compromised accounts. The cyber thieves employ a number of tactics in this scam, including the use of money mules and distributed denial of service attacks (DDos).

After the cyber thieves initiate wire transfers out of the account, they conduct a DDos attack on the financial institution in attempt to take down the institution's website. The FBI believes the DDos attack is used as a smoke-screen to deflect attention from the wire transfers.

The wires are transmitted to high-end jewelry stores, which is where the money mules come into play. The perpetrators contact the high-end jeweler with a request to purchase precious stones and high-end watches. The jewelry store is informed payment via wire transfer will be made and someone will come in to pick-up the merchandise.

Do not open emails purporting to be from NACHA. NACHA does not send emails directly to businesses or consumers.