Intelligence Note

Prepared by the
Internet Crime Complaint Center (IC3)
January 19, 2011

E-MAILS CONTAINING MALWARE SENT TO BUSINESSES CONCERNING THEIR ONLINE JOB POSTINGS

Recent FBI analysis reveals that cyber criminals engaging in ACH/wire transfer fraud have targeted businesses by responding via e-mail to employment opportunities posted online.

Recently, more than $150,000 was stolen from a US business via unauthorized wire transfer as a result of an e-mail the business received that contained malware. The malware was embedded in an e-mail response to a job posting the business placed on an employment website and allowed the attacker to obtain the online banking credentials of the person who was authorized to conduct financial transactions within the company. The malicious actor changed the account settings to allow the sending of wire transfers, one to the Ukraine and two to domestic accounts. The malware was identified as a Bredolab variant, svrwsc.exe. This malware was connected to the ZeuS/Zbot Trojan, which is commonly used by cyber criminals to defraud US businesses.

The FBI recommends that potential employers remain vigilant in opening the e-mails of perspective employees. Running a virus scan prior to opening any e-mail attachments may provide an added layer of security against this type of attack. The FBI also recommends that businesses use separate computer systems to conduct financial transactions.

For more information on this type of fraud and prevention tips, please refer to previous Public Service Announcements by clicking the links below:

- http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf
- http://www.ic3.gov/media/2010/WorkAtHome.pdf
- http://www.ic3.gov/media/2009/091103.aspx

Anyone who believes they have been a target this type of attack should immediately contact their financial institutions and local FBI office, and promptly report it to the IC3's website at www.IC3.gov. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The IC3 also uses complaint information to identify emerging trends and patterns.