

Anatomy of an Account Takeover



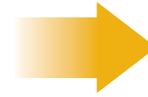
Malware such as Black Hole Exploit, Zeus, Citadel, is built.



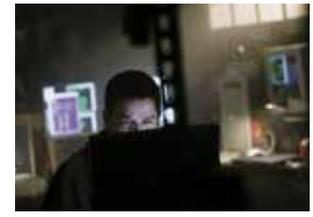
Malware sent via attachments or phishing attempts through spam.



User opens attachment or follows link.



Executes malicious code on PC and/or Network.



Hacker monitors compromised PC and waits for user to access accounts.



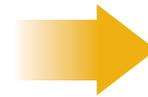
Staff member signs into Online Banking.



Hacker hijacks Online Banking session when user enters credentials/token.



Hacker creates fraudulent ACH or Wire Transfer.



Fraudulent transaction sent to bank for processing.



Bank receives what appears to be a legitimate request.

Malware is software used or created by attackers to disrupt computer operation, gather sensitive information or gain access to private computer systems. Most malware is installed when users unknowingly infect their devices on the Internet when they are directed to malicious sites via targeted phishing emails that contain malicious links or attachments.

Common email phishing schemes purporting to be from:

- The Federal Deposit Insurance Corporation (FDIC) regarding your business's ACH activity
- NACHA indicating that your business's ACH membership has expired
- ADP, a payroll service company
- The bank, related to a rejected wire transfer
- Law enforcement agencies issuing traffic violations in New York City
- Adobe Software regarding an upgrade for Adobe Acrobat Reader and Adobe X Suite Advanced
- A credit card company regarding an overdue payment
- The Better Business Bureau
- Booking.com, a hotel booking website, regarding a reservation
- Shipping companies, such as FedEx, UPS or DHL, regarding a parcel that was not properly delivered
- PayPal regarding changes to your email address, an account review notification or your account availability

If you receive an email that you are not sure about, contact the sender through reputable means such as a published or known phone number or email address. If you believe you have been a victim of a phishing attack, please contact us immediately.