External Fraud Alert

A bi-weekly publication from the Accordo Team

Nov 3, 2017

Phishing Attacks in the Banking Industry

InfoSec Institute

The banking industry is a prime target for phishing attacks. According to Kaspersky Labs, in 2016 there were over one million Trojan attacks on banks (a type of malware disguised as standard software). Hackers are also focusing more on leveraging gaps in bank security, rather than attacking individual accounts; recent incidences include the 2014 Carabank attack on the Russian banking system, and the Trojan program, Dyreza, which infected over 100,000 units. Phishing emails targeting C-level executives, referred to as whaling, is another tactic used by cyber hackers; in one such incident, a hacker successfully stole $75 million from a Belgian bank (Crelan). Firms should train personnel on common phishing techniques, and periodically update training material to reflect newer methodologies. Link

Cybersecurity: Ransomware Alert

SEC (May 17, 2017)

The recent ransomware attack known as WannaCry (also WCry or Wanna Decryptor) accessed servers through phishing emails, scam websites and vulnerabilities in the Windows Server Message Block (SMB) and Microsoft Remote Desktop Protocol (RDP). The SEC urges broker-dealers and investment advisor firms to review Homeland Security's U.S. Cert Alert TA17-132A, and to ensure all updates and patches for system software are properly installed. Link

Hedge Funds Flip ICOs, Leaving Other Investors Holding the Bag

Bloomberg (Oct. 3, 2017)

Hedge funds with discounted access to initial coin offerings (ICOs) are taking advantage of the favorable terms and re-selling the digital coins at higher margins; the trend is reminiscent of typical IPO "pump-and-dump" schemes. In the Kik ICO presale, Blockchain Capital, Pantera Capital and Polychain Capital purchased digital coins at a 30% discount, and at least 80% of cryptocurrency ICOs will be doing presales. SEC Chairman, Jay Clayton, warns retail investors to be aware of fraudulent activity in the newly regulated space. Link

Security Trends in the Financial Services Sector

IBM (2017)

IBM Managed Security Services Threat Research group conducted research on cybercrime and security trends in the financial services industry. Cyber attacks on financial services firms rose by over 25% in 2016 with a notable increase in SWIFT and Business Email Compromise (BEC) attempts. IBM'S research found that injection attacks were the major attack type for financial services security clients, targeting more than 50% of firms queried. Injection attacks allow an unauthorized hacker to input data in a system, thereby gaining control of data or damaging data integrity; the attack type includes both command and shell command injections, which hackers can use to gain full access to customer PII. Link

Recent Financial Fraud Incidents

Source: Industry Research and Survey

ACCORDO