KnowBe4
Human error. Conquered.

WHITEPAPER
SME's and Cyberheists

KnowBe4
Human error. Conquered.

whitepaper

SME’s and Cyberheists

CYBER CRIMINALS NOW TARGET SMALL / MEDIUM ENTERPRISES LACKING SOPHISTICATION AND APPROPRIATE SECURITY, SMES MAKE GREAT TARGETS FOR CYBER GANGS

CYBER CRIME HAS MOVED BEYOND SIMPLE IDENTITY THEFT

Cyber criminals are now successfully targeting small and medium enterprises using specialized banking Trojans, especially malware called Zeus. These smaller organizations represent good targets as they often lack the sophistication and knowledge of the Fortune 1000 to prevent attacks.

WHAT IS THE ZEUS MALWARE

Zeus is a Trojan horse that steals banking information by keystroke logging. This malware tracks and logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. Zeus is spread mainly through drive-by downloads and phishing schemes that prey on employees by having them click on something . Since July 2007 Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and Business Week.

CASE IN POINT

Patco Construction in Sanford, Maine filed suit in York County Superior Court Sept. 18, seeking the return of $345,000 not recovered from $588,851 in funds cyber criminals were able to transfer to bank accounts across the country from Patco’s Ocean Bank. The illegal transfers began on May 7, when thieves hijacked the company's online banking credentials, moving $56,594 to several individuals that had no prior business relationship with Patco. The transfers continued, and Patco officials only learned the fraud was occurring because some of the funds were transferred to invalid bank accounts. The company filed suit, alleging the bank was negligent in allowing cyber criminals to break through the security system.

BEYOND PATCO

The Patco case and others have thrown a rift in the relationship between banks and their customers. Whereas personal relationships have always been important in the banker- customer connection; the threat of fraud is transcending normal business procedures. This is especially the case in small community banks with tight profit margins. Customers want to be protected, yet often cannot pay the price of securing that protection. Banks feel the customer is responsible for their computers and networks and the losses are their problem, but then run the risk of losing customers.

DIGITAL CRIME NOW TWICE REAL-WORLD ROBBERIES

Digital crime now outpaces real-world bank robberies in terms of losses. In 2009, there were 8,818 bank robberies netting criminals an average of $4,029 -- a total of about $35.5 million, according to the FBI's Uniform Crime Reporting (UCR) program. However, 60 percent of bank robbers were caught, often very quickly. Compare that to Automatic Clearing House (ACH) fraud statistics. ACH is a nationwide electronic funds transfer network which enables participating financial institutions to distribute electronic credit and debit entries to bank accounts and to settle such entries.

The recent arrests connected with Zeus accounted for some 390 reported cases where $70 million was stolen from accounts. The criminals had attempted to steal some $220 million. The investigation mainly netted the lowest ranks of the criminal network -- the so-called money mules that remove stolen funds from their accounts and transfer the money to international accounts abroad. In general, the money mules are people who are duped into believing they are working for a legitimate company processing payments.

THE LAW

The Uniform Commercial Code holds that institutions must take "commercially reasonable" steps to protect customers against fraud. For most banks, the bar for what is considered reasonable for online banking authentication was set by a 2005 document issued by the Federal Financial Institutions Examination Council, which concluded that simply requiring customers to enter just a user name and password was inadequate. However, many banks still use that simple authentication procedure for their Internet Banking websites.

ANALYSIS

The Internet is the 21st century crime scene. Cyber theft has become one of the biggest challenges facing our society today. We can no longer remain ignorant and hope it will go away. Banks and customers alike must educate themselves and give employees Internet Security Awareness Training, including procedures and necessary security measures. Accounts must be monitored by companies on a regular basis and questionable transactions queried immediately. Simultaneously, banks must use the highest level of security to protect their customers. The financial relationship is at stake – trust is of utmost importance. Today that trust must be earned on both sides.

RESOURCES

InfoWorld:
http://www.infoworld.com/t/malware/zeus-threatens-strike-down-community-banks-803

NetworkWorld:
http://www.networkworld.com/news/2009/092409-construction-firm-sues-after-588000.html

Washington Post:
voices.washingtonpost.com/securityfix/2009/09/construction_firm_sues_bank_af.html

DigitalMediaLawyer:
http://www.digitalmedialawyerblog.com/2009/10/patco_construction_v_ocean_ban_1.html

Risk Management:
http://riskmanagemnet.banking--businessreview.com/news/acts_policies_and_tools_to_safeguard_financial_institutions_from_fraud_101029

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created by two of the best known names in cybersecurity, Kevin Mitnick (the World's Most Famous Hacker) and Inc. 500 alum serial security entrepreneur Stu Sjouwerman, to help organizations manage the problem of social engineering tactics through new school security awareness training.

More than 1,700 organizations use KnowBe4's platform to keep employees on their toes with security top of mind. KnowBe4 is used across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

- KnowBe4 wrote the book on cyber security (8 books and counting between Mitnick and Sjouwerman).

- KnowBe4 is the only set-it-and-forget-it security awareness training platform "by admins for admins" with minimum time spent by IT to get and keep it up and running.

- The platform includes a large library of known-to-work phishing templates.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com