FOCUS e-newsletter: Headliner
October 2015

# Top Cyber Threats to Small Credit Unions
# Part 1

*President Obama designated October as National Cyber Security Awareness Month. This campaign by the U.S. Department of Homeland Security is to educate the public and private sectors about cybersecurity and "increase the resiliency of the nation in the event of a cyber incident." We asked information specialists in NCUA's Office of Examination and Insurance for guidance to assist small credit unions with addressing such threats. In the first of this series of articles, they identify some top threats to small credit unions.*

According to a recent Government Accountability Office audit report, criminals are increasingly targeting smaller institutions, because the expected payoff is greater relative to larger institutions, whose systems may be more sophisticated and harder to compromise. The report also said that account takeovers largely have shifted from large to medium and small institutions. This article provides an overview of the dynamic cyber threat environment affecting the financial services industry.

## Legacy Applications

Legacy applications and operating systems present an ongoing concern to all types of organizations including credit unions. A legacy system is one for which there is no longer ongoing support by the manufacturer, in particular with regard to security patches which correct critical security vulnerabilities. One prominent recent example is Windows XP, for which Microsoft ended support in April 2014. Similarly, Microsoft Server 2003's support ended in July 2015. Using unsupported operating systems can be an unsafe practice and requires a clear migration or risk mitigation plan supported by a sound risk assessment.

## ATM Skimming and Malware

Criminals will likely step up activities targeting U.S. automated teller machines as merchant point-of-sale terminals and debit/credit card readers transition from accepting magnetic stripe cards to Europay, MasterCard and Visa EMV cards. EMV cards store the accountholder's information on an embedded microchip and are less vulnerable to current ATM skimming techniques.

The skimming method most commonly used by criminals involves installing a device on an ATM that captures the accountholder's information from the card's magnetic stripe. This method may also involve a tiny camera that records the cardholder entering her/his personal identification number. ATM skimmers are becoming more complicated and difficult to detect. Skimmers can now completely encase the front of a cash machine and transmit stolen information to the perpetrator wirelessly.

A new method of ATM skimming has emerged where criminals install malware that compromises the ATM's software, permitting them to withdraw cash directly from the ATM. This method is increasingly being used as it is more profitable than attaching skimming

hardware. The malware can sit undetected in the system for a longer period of time, allowing the thieves to thoroughly and quickly drain funds. Remind customers to be cautious when using any ATM, cash machine or credit authorizing device, such as at a gas pump, and to alert police and/or the credit union or vendor immediately if anything seems suspicious.

**Identify Theft and Account Takeovers**

Identity theft continues to increase due to the massive data breaches of the last couple of years. In one quickly increasing variant of this threat, hackers cross-reference stolen card data to social security numbers from another breached organization. Then they call the financial institution and change the personal identification number, which financial institutions verify with a Social Security number and card number. This enables the crooks to create a fully emulated debit card with PIN, which they can use to withdraw cash from ATMs or sell on the black market. Strong customer verification procedures are necessary to mitigate this threat.

**Pervasive Vulnerabilities**

Heartbleed and the Shellshock bug were recent examples of pervasive vulnerabilities that could lead to wide-scale compromise of websites or network security equipment. The Federal Financial Institutions Examination Council considered these critical vulnerabilities so severe that they issued alerts to the industry[1]. The entire Internet can be scanned relatively quickly, which may identify a large number of these types of vulnerabilities. Therefore, the concern is that a vulnerability could be identified and exploited at a large number of financial institutions in a short period of time. In particular, financial institutions offer online banking services through web servers that require frequent security patching. A comprehensive program to install all pertinent security patches in a timely manner is key to managing these types of vulnerabilities.

**Spear Phishing**

Spear Phishing is a very dangerous type of targeted phishing attack specifically directed to an organization. The attacker's objectives typically include financial gain, trade secrets or military information. An email will come to the victim that appears to be from someone within their organization, often from a position of authority. The message seeks to promote a sense of urgency, such as failing to follow the instructions will result in consequences and/or disciplinary action towards the recipient. Or, the message may appeal to curiosity, by purporting to link the recipient to interesting pictures or websites. Ultimately, the objective is to trick the email recipient to click on a link or to access a malicious file infecting their computer and serving as the initial attack point into the organization's network. Ongoing awareness campaigns are a critical element towards combating this threat.

**Distributed Denial of Service Attacks**

DDoS attacks can interrupt online banking services by launching large volumes of illegitimate web traffic to overwhelm a system's resources. The latest variation on this type of cyber attack may start as an email threat demanding a ransom paid in bitcoins. If the targeted institution does not respond, the attackers may demonstrate the threat via a small scale DDoS attack. Ultimately, the targeted institution may need assistance from a specialized vendor to mitigate a full-scale

[1] The Federal Financial Institutions Examination Council is a federal interagency organization that prescribes uniform principles, standards, and report forms for the federal examination of financial institutions. The National Credit Union Administration is one of the nine member agencies.

attack. Law enforcement recommends financial institutions not pay ransoms, because they may encourage repeat attacks.

**Ransomware and Destructive Malware**

These types of cyber threats use popular communication tools to spread malware, including worms sent through email and instant messages, Trojan horses dropped from web sites and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities to infiltrate systems. In the case of Ransomware, compromised systems may have their data encrypted with a ransom demanding payment for the password necessary to decrypt and regain access to the data. Angst about the ransom payment may be further increased by demanding it in bitcoin. Many encryption algorithms now exist which are not feasible to crack, so the probability of permanent data loss is high.

Destructive malware is even more insidious, as the malicious intent is typically to permanently destroy the victim's data without any negotiation or recovery opportunity, such as ransom payment. Proper backup and recovery procedures are critical towards mitigating these types of attacks. Again, paying a ransom offers no guarantee, but rather may encourage the behavior.

**To learn more about cyber security, including resources for small businesses through the U.S. Department of Homeland Security, visit its website at** http://www.dhs.gov/national-cyber-security-awareness-month.

**The next article in this series will focus on what NCUA is doing to help credit unions address cyber threats.**