Northwest Credit Union Association
Idaho • Oregon • Washington

Skimming Alert

ATM Jackpotting Reported in Pacific Northwest.

The FBI is working a case regarding recent ATM jackpotting and card skimming that has impacted institutions in Washington. The Portland and Seattle FBI offices are teaming up to identify institutions that have been impacted by this crime ring in Washington, and possibly in Oregon. The FBI shared the following message:

Beginning on or about December 11, 2017, a group of unidentified persons have used computer malware to cause at least five drive-up Diebold Opteva 750 ATMs in western Washington to dispense all of the available funds from the ATM (ATM Jackpotting). Note: Diebold ATMs may not be the only attacked machines. The persons may have been in the region as early as October 2017.

Thefts have occurred at financial institutions in Clark, Skagit, Snohomish, and King Counties primarily between 9pm-12am. Based on surveillance images provided, all of the incidents appear to have been committed by the same individuals. As of December 22, 2017, the thieves have either made multiple trips to the same ATM over one hour or lingered at the ATM machine for over 20 minutes.

The thefts appear to entail opening the ATM service door with a key, removing the hard disk from the ATM computer, installing malware onto the disk, rebooting the ATM, and finally making a series of 10 or more withdrawals, approximately 30 seconds between each withdrawal, until all cash had been dispensed.

Based on the best current information available the following are suggestions for securing or thwarting these thefts. Financial institutions should take any precautions necessary to safeguard their ATMs.

1) Full disk encryption on ATM computers could prevent the malware from being effective.

2) Install a silent alarm triggered when the ATM service door is opened.

3) It appears the thieves reboot the ATMs during the theft. Alerts through the bank network implemented with reboots of the ATM could allow for bank security personnel to contact the police.

4) A vehicle sensor similar to those used in parking garages could detect a vehicle lingering for more than a set amount of minutes without leaving and could trigger an alert.

If any institutions are victimized in this way, contact the Seattle FBI at 206.622.0460.

Credit unions in Oregon can contact the Portland FBI office at 503.729.7585.

#CUobsessed

Katie Clark CUCE, BSACS
Regulatory & Compliance Analyst
Northwest Credit Union Association
503.350.2221 • 800.995.9064 x221
www.nwcua.org

Copyright © 2018 Northwest Credit Union Association
Idaho Office: 2710 W Sunrise Rim Rd, Suite 100 • Boise, ID 83705
Oregon Office: 13221 SW 68th Pkwy, Suite 400 • Tigard, OR 97223
Washington Office: 18000 International Blvd, Suite 350 • SeaTac, WA 98188

If you would like to stop receiving ALL emails from us, go here.
To sign up for other mailing lists, go here.
Please send any comments about this email to webmaster@nwcua.org.

Powered by informz