January 26, 2018

**[ACTION] Action Alert – GIOC Reference #18-007-A**

The GIOC received credible information that bad actors are activating cash out crews to attack Diebold front loading ATMs, specifically 500 and 700 series, using Ploutus D malware around the United States in the next 10 days. ATMs running Windows XP are particularly vulnerable. It is recommended that ATMs operate an up to date version of Windows 7 to defeat this specific type of attack. At least one attempted attack, as outlined below, occurred in Louisiana in the last 24 hours.

The targeted stand-alone ATMs are routinely located in pharmacies, big box retailers, and drive thru ATMs. During previous attacks, fraudsters dressed as ATM technicians and attached a laptop computer with a mirror image of the ATM’s operating system along with a mobile device to the targeted ATM. The attackers use an endoscope to obtain access to the ATM’s toggle to sync their laptop computer with the security features of the ATM. Once this is complete, the ATM is controlled by the fraudsters. The ATM will appear to be Out of Service to potential customers. At this point, cash out crews communicate with co-conspirators remotely controlling the ATMs to initiate the ATM cash withdrawals. In previous Ploutus D attacks, the ATM continuously dispensed at a rate of 40 bills every 23 seconds. Once the dispense cycle starts, the only way to stop it is to press cancel on the keypad or the cassette runs out of cash. The cash out crew/money mule takes the dispensed cash and places it in a large bag. After the cash is taken from the ATM and the mule leaves, the technicians return to the site and remove their equipment. The last thing the fraudsters do before leaving the site is to plug the Ethernet cable back in.

The following pages, obtained from a private partner with knowledge of this style of attack, contain a detailed description of the steps taken by the fraudsters to perpetrate this attack.

Please reach out to the GIOC at gioc@usss.dhs.gov if your office receives credible information relating to this attack.

Any questions relating to this alert can be directed to ATSAIC Matt O’Neill, 202-406-6242, matthew.oneill@usss.dhs.gov.







