United States Secret Service [INFO]

October 29, 2018

[INFO] Information Only Alert – GIOC Reference #18-048-I
TLP Green

Unlimited Cash-Out Operations

Cyber criminals continue to target financial institutions (FI) and processors with malware to access internal banking infrastructure enabling the large-scale theft of funds from ATMs. The malware manipulates system controls to inflate account balances and remove daily transaction limits enabling the criminals to withdraw a nearly unlimited amount of cash. These operations, commonly referred to as unlimited operations, are very lucrative if successful. For example, a recent unlimited operation netted fraudsters over $6 million dollars in less than an hour. Unlimited cash-out operations are not new. In 2011, The U.S. Secret Service (USSS) New York Field Office led a successful investigation relating to a $14M cash-out operation in which a number of high value targets were apprehended from across the globe. The USSS has arrested, or provided the necessary intelligence to apprehend, scores of criminals around the world who participate in cash-out operations. Although unlimited cash-out operations are not new, the increased frequency of attacks is worth highlighting.

For an unlimited cash-out operation to be successful, cyber criminals need to activate a large network of cashers. Cashers are the criminals who physically go to the ATMs to make the withdrawals. Consequently, these operations can be difficult to manage because the network of cashers has to be sufficiently large to handle scores of simultaneous worldwide cash outs.

The Secret Service disrupts these cash-out operations thru our large network of partners tied to the Secret Service's Electronic Crimes Task Forces (ECTF) around the world. The Secret Service provides actionable intelligence in real time to the targeted businesses and FIs. The Secret Service will not issue broad alerts to the financial sector which could potentially compromise our partners and the investigation. Instead, the Secret Service will contact only the targeted business or FI to provide the available intelligence relating to a potential attack in order to mitigate potential loss. If the Secret Service is unable to directly contact the targeted business or FI, we will communicate through a trusted stakeholder already engaged with targeted victim.

By taking advantage of our aggressive intelligence collection operations, the Global Investigative Operations Center (GIOC) worked with Field Office and Headquarters

GLOBAL INVESTIGATIVE OPERATIONS CENTER
WASHINGTON, D.C.

[INFO] - Indicates informational or educational content.

components to disrupt four attempted worldwide-unlimited operations since September. These efforts prevented around $20 million in intended losses. Each of the four attempted operations involved dozens of casher crews armed with stolen payment card data in over 20 countries. The cyber criminals targeted both domestic and international FIs. The targeted domestic FIs did not suffer a loss in the most string of recent attacks. Since cash-out operations normally take place after business hours and on weekends, the GIOC and USSS personnel detailed at the NCTFA remain engaged with private industry stakeholders around the clock to provide any actionable intelligence related to this persistent threat.

The GIOC will also be engaging offices where the cash-out activity occurred in an effort to obtain the evidence needed to identify and apprehend the cash-out crews foreign and domestic.

If your office receives any intelligence relating to pending unlimited ATM cash-out operations, please contact the GIOC at gioc@usss.dhs.gov or 202-406-6009 immediately.

GLOBAL INVESTIGATIVE OPERATIONS CENTER
WASHINGTON, D.C.

[INFO] - Indicates informational or educational content.