U.S Department of
Homeland Security

United States
Secret Service

Industry Advisory

March 15, 2013
Contact: (202) 406-9330

(Washington, D.C.) – Over the course of the last several months the United States Secret Service has observed an increase in malicious activity targeting payment processers associated with prepaid debit accounts. Attackers engaged in this activity attempt to gain access to victim computer systems through a variety of remote exploits, pursue an aggressive strategy of privilege escalation, and spend an extended period of time mapping network topology and security protocols. The ultimate goal of the attackers is to obtain administrative access to the database systems associated with prepaid accounts.

In a successful event, the attackers are able to manipulate some combination of the balances of the target accounts and the fraud/loss prevention controls utilized by the processer. Subsequently, unauthorized ATM withdrawals are conducted simultaneously in multiple countries throughout the world. In most instances these withdrawals are monitored in real time by the individuals conducting the operation. The following list of strategies should serve as suggestions for payment processers associated with prepaid debit account platforms.

Macro Strategies

- Integrate information security outcomes into all levels of organizational planning.
- Ensure that information technology concerns are adequately addressed in the initial planning phases of all mergers, acquisitions or sales.
- Deploy strategies that take into account the relationship between network security and fraud loss prevention. Often appropriate mechanisms for communication between the two entities are not formalized.
- Develop a formal review framework for after action related to incident response to ensure that vulnerabilities are appropriately addressed and beneficial changes are integrated into current function and future planning.
- Utilize concentric circles of defense to protect the most critical resources on production networks, including database systems.

-more-

Prepaid Platform Specific Strategies

- Utilize multiple alert methods to notify administrators of any changes to rules and restrictions on prepaid databases.
- Require two factor authentication for all remote access into prepaid database systems.
- Utilize duplicative means to collect, preserve and validate database logs. Immediately address any inconsistencies in logs to determine the nature of the issue.
- Disable or delete administrative testing accounts when not in use.
- Ensure that account PINs may not be obtained through manipulation of unrelated aspects of prepaid databases. For example, ensure that a user's phone number cannot be changed in the data base resulting in a PIN reset request sending an SMS to an attacker controlled phone.
- Employ aggressive fraud detection controls on prepaid systems including:
    - Alerts on any accounts that conduct three transactions at separate ATM devices in less than two minutes.
    - Alerts on any accounts that conduct ATM transactions in two separate countries within five minutes.
    - Alerts on any accounts that conduct five balance inquiries within three hours.
    - Alerts on any accounts that attempt to conduct three transactions in excess of the daily limit on the same calendar day.
    - Alerts on any accounts for which the balance is increased beyond an appropriate maximum value consistent with the type of account. For example, any account increased to a balance beyond $250,000.00.
    - Alerts on any accounts utilized to conduct more than an appropriate number of transactions in a one hour period. For example, any account utilized to conduct 30 transactions per hour.

The above listed fraud detection controls are provided as examples only. Fraud detection controls should be specifically tailored to the profile of individual platforms such to minimize false positives while maximizing security. The success of these and any other relies on careful monitoring and constant attention to the circumstances surrounding alerts and the action taken in the aftermath of these indicators.

###