POINTER-OF-SALE MALWARE

and the
SEVEN STAGES ATTACK MODEL

RECON
Attacker(s) determine:
1. POS vendor and system architecture
2. Enterprise network topology

LURE
Email or web attack lure
Yes
No

REDIRECT
Redirect victim to attacker’s website.

DROPPER FILE
Install dropper or custom malware on victim’s machine. Malware will eventually install on POS systems to scrape RAM memory (POSRAM).

CALL HOME
POSRAM captures and sends credit card data to an off-site server

DATA THEFT
Criminals have account data on credit/debit cards. These will be offered for sale on the black market.

POSSAM = Point-of-Sale Terminal RAM Scraper
RAM = Random Access Memory
POS = Point-of-Sale

HOW POSRAM* WORKS

POSRAM* system is infected with memory (RAM) scraping malware

During a POS transaction, encrypted customer data is retrieved

POSRAM software uses the briefly unencrypted customer data

Malware scrapes the temporarily unencrypted customer data from memory (RAM*)

Stolen credit card data is written to a text file which is later sent to off-site server

* Source: Websense Security Labs

VISIT:
http://securitylabs.websense.com

AND:
www.websense.com/sevenstages

© 2014 Websense, Inc. All rights reserved. Websense, TKER and the Websense logo are registered trademarks of Websense, Inc. in the United States and various countries. All other trademarks are the properties of their respective owners.