NEW LUSYPOS MALWARE FOR SALE IN THE UNDERGROUND

December, 2014

RSA recently tracked a new malware application dubbed LusyPOS advertised for sale in Russian speaking underground forums. The cybercriminal describes LusyPOS as a 'dump grabbing' (steals Track1/2 credit card data) POS malware that attacks POS systems based on the Windows platform.

The forum post states that all sales will be done via an escrow service, and lists the following features:

– Coded in C

– Grabs Track 1/Track 2 of a credit card dump

– Works with Windows POS systems

– TOR http Admin panel

– Luna checker for CC numbers

– Multiple users supported

Two different packages are offered, based on the technical expertise level of the cybercriminal:

Pro Package (for those already experienced with 'dump grabbers')

– All re-builds are free

– Unlimited support via Jabber chat

– $2,000 per binary with installation on user's hosting

– $2,200 per binary with installation on fraudster's hosting

Newbie Package (for new users)

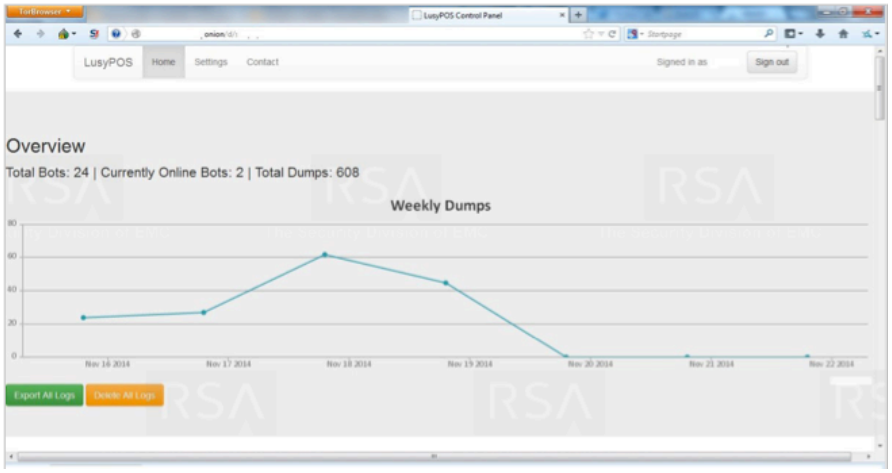
– Full help in initial setup

RSA

– Fully functional and pre-configured control panel and hosted application – ready for immediate use
– An introductory tutorial to the whole process
– Tips and additional knowledge sharing
– Additional tools for hacking POS machines at an additional price
– Online support always available. May involve an additional fee, according to the level of knowledge/help required

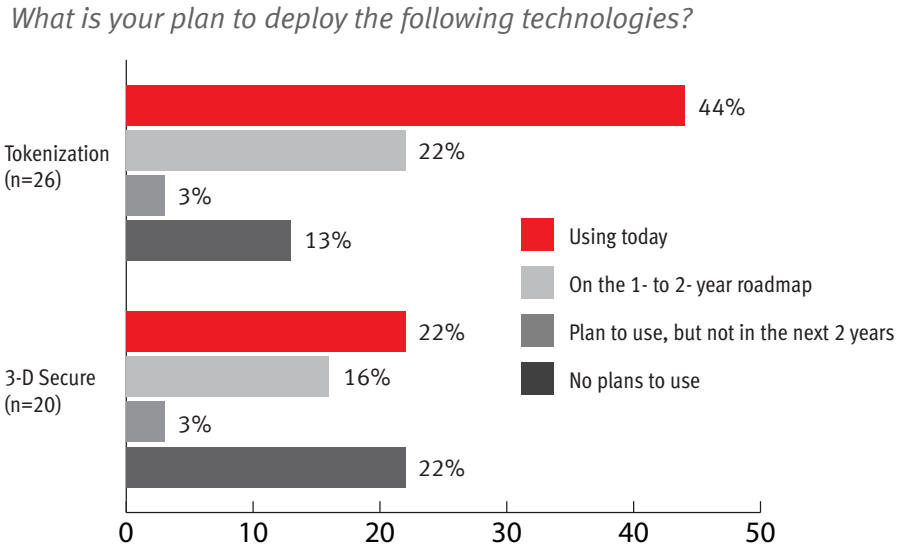
The cybercriminal posted alleged screenshots of the Admin panel of the LusyPOS malware, displaying information on currently active bots and alleged CC data that has been stolen. We do not know at this time if any of the details shown in the screenshots are real or contrived by the developer as part of advertising his malware kit.

Figure 1: Admin panel Overview screen posted by the fraudster – allegedly showing number of bots, and total number of CC 'dumps'.



It is no surprise to see the continued growth of POS malware springing up. Particulary, the U.S. is at most risk for these opportunistic attacks as migration to the EMV standard has just started, and most cardholders in the U.S. still carry cards that use the magnetic stripe. However, merchants are taking notice after the flurry of high profile POS retail breaches in the last 12 months, and investing in additional technology, such as tokenization, to protect cardholder data as a result. In fact, two-third of merchants in a recent survey stated they are already using or plan to implement tokenization technology in the next 12 months (see Figure 2; Source: Aite Group).

Figure 2: Top of mind security solutions for retailers looking to add protection for cardholder data.



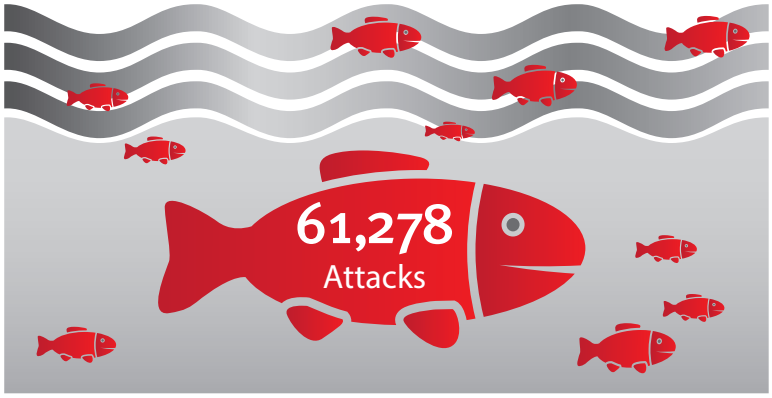
How will cybercriminals react to the coming of EMV in the U.S.? It is likely we will see a rapid growth in POS malware variants in 2015 as cybercriminals look for opportunistic attacks to steal massive caches of card data before EMV becomes the standard for all U.S. payment cards.

DECEMBER 2014

Source: RSA Anti-Fraud Command Center

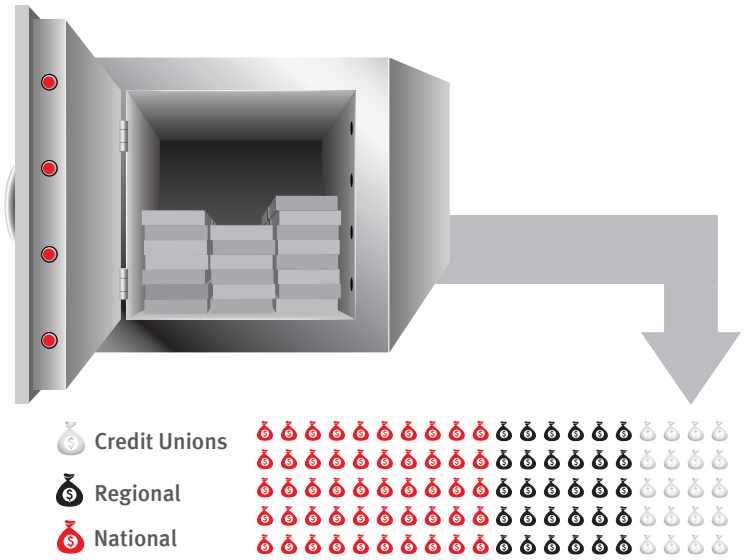
Phishing Attacks per Month

RSA identified 61,278 phishing attacks in November, marking a 76% increase from October. This sharp increase is no surprise due to the high volumes of online shopping during the holiday season. Based on this figure, RSA estimates phishing cost global organizations $594 million in losses.



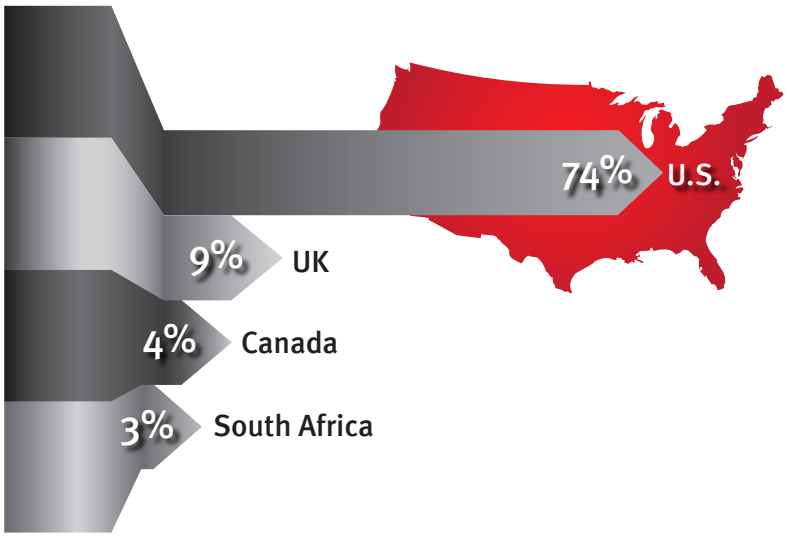
US Bank Types Attacked

Regional banks and credit unions were targeted by half of all phishing volume in November. Phishing volumes have started to even out as cybercriminals look to target smaller financial institutions that might not have the resources to address these attacks.



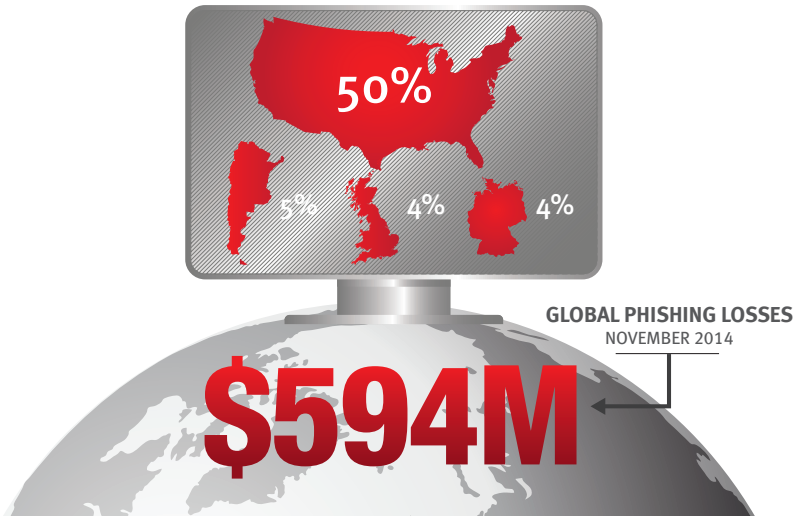
Top Countries by Attack Volume

The U.S accounted for nearly 75% of attack volume in November, followed by the UK, Cananda and South Africa.



Top Hosting Countries

Ten percent of all phishing attacks were hosted in Latin America in November, specifically Argentina, Colombia, and Brazil.



CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.emc.com/rsa

www.emc.com/rsa

RSA