IntelCrawler

Point-of-Sale and Modern Cybercrime Detection of “Nemanja” Botnet

FOR PUBLIC RELEASE

May 22nd 2014




IntelCrawler, info@intelcrawler.com (PGP), 13636 Ventura Blvd. #421 Sherman Oaks, CA 91423, www.intelcrawler.com

Table of Contents

Disclaimer

The research, findings, and analysis in this report are based on a combination of open and operative sources.

To protect some victims and open cases, the non-disclosure of operative sources may leave some gaps in the linkage of some parts of the analysis.

This report is solely the opinion of IntelCrawler LLC.

Executive Summary

IntelCrawler, a cyber-threat intelligence company based in Los Angeles, has been investigating various electronic crimes related to the Point-of-Sale (POS) niche for quite a long time, collaborating with cyber intelligence and fraud detection teams of major financial institutions worldwide.

The experience gained and successful cooperation history helped to create a detailed report on modern types of crimes linked with POS in various industries. Criminal gangs worldwide are illegally accessing retailers and small business infrastructures, having significant impact on all parties involved in credit card acceptance, which was confirmed during 2013-2014.

The following report has been created to help merchants, credit card associations, law enforcement and security experts to arrange successful investigations of such types of crime, as well as to maintain the highest level of POS environment information and physical security.

About March 2014, IntelCrawler identified one of the biggest botnets, called "Nemanja," based on compromised POS terminals, accounting systems and grocery management platforms. The assigned name is related to potential roots of bad actors with similar nicknames from Serbia. It included more than 1478 infected hosts from Argentina, Australia, Austria, Bangladesh, Belgium, Brazil, Canada, Chile, China, Czech Republic, Denmark, Estonia, France, Germany, Hong Kong, India, Indonesia, Israel, Italy, Japan, Mexico, Netherlands, New Zealand, Poland, Portugal, Russian Federation, South Africa, Spain, Switzerland, Taiwan, Turkey, UK, USA, Uruguay, Venezuela and Zambia.

The analyzed botnet has affected various small businesses and grocery stores in different parts of the world, making the problem of retailers' insecurity more visible after past breaches.

The results observed during investigation partially form the following report, providing some case studies and extracted fingerprints of compromised systems for further research and risk mitigation. The details from the "Nemanja" botnet were added to IntelCrawler's Intelligence Platform and the "PoS Malware Infection Map" (PMIM)[1] and are provided as security feeds for card associations, payment providers and various vetted parties, consisting of compromised merchants, IP addresses of infected terminals and additional information for fraud prevention.

IntelCrawler welcomes security researchers, threat intelligence analysts, fraud investigations, industry leaders, security vendors, card associations and international LEA for beneficial collaboration and information exchange using secure ways of communications. Contact our team by e-mail info@intelcrawler.com (PGP).

[1] **IntelCrawler PoS Malware Infection Map** - http://intelcrawler.com/about/pmim

Key Findings

The attack landscape of detected attacks showed that the interests of modern bad actors are targeted more at deep penetration of retailers' network environments than a single infection of a compromised POS terminal.

- Most compromised POS terminals, accounting systems and grocery management platforms had antivirus software installed onboard, which shows the inefficiency of it in regard to modern POS malware;

- The "Nemanja" botnet case showed that the bad actors started to join traditional RAM scrapping malware with keylogging modules allowing them to intercept pressed keyboard buttons besides fragments of memory with Track 2 data, as it may help to gain access to other elements of retailers' infrastructures (SQL databases, network file storages, CRM systems, corporate environments, etc.);

- The detection of the installed malware happened after more than 6 months from successful intrusion and infection;

- It is not necessary to install C&C of POS malware on specific bulletproof hosting, because most cybercriminals install it for a short period of time on hacked hosts and then migrate it after deep penetration to payment environments in order to not lose the data.

The nice part of POS fraud, for cyber criminals, includes various ways of committing this crime, including the use of insiders. During the investigation it was found that some bad actors propositioned commercial service employees to install malware during their employment in a famous grocery store.

- Modern retailers' security needs more efficient due-diligence of technicians, third party outsourcing companies and internal staff in order to mitigate POS fraud risks. The "Nemanja" case showed that one of the weak spots in retailers' security was the human factor besides the technical component;

- Physical security is still a huge problem for many enterprises, including retailers and small businesses working with payments. It really helps the bad actors to bypass many security controls and infect payment environments with malware, disabling CCTV, electricity, and other equipment to remain invisible;

- The detection of one of the main bad actors showed a big chain of other cybercriminals involved in various similar types of crimes in other parts of the world.

Types of Crimes

There are several types of crimes which are popular in the modern e-Crime underground with help of POS. Modern cybercrime groups understand that this niche is more cost efficient than classical ATM skimming, and also more mobile, providing pretty similar profit.

The group related to the "Nemanja" botnet was involved in several different, but popular directions of POS-related crimes. It shows how a small group of people can cause significant damage to the payment industry worldwide performing various illegal activities against POS using remote telecommunication channels and physical tampering of the devices.

The modern underground economy has figured out four key types of POS crimes, separating them into "data theft" and "money laundering" categories by their nature. Most of them are carried out with help from an insider, who acts as a partner of the cybercrime group on individual conditions.

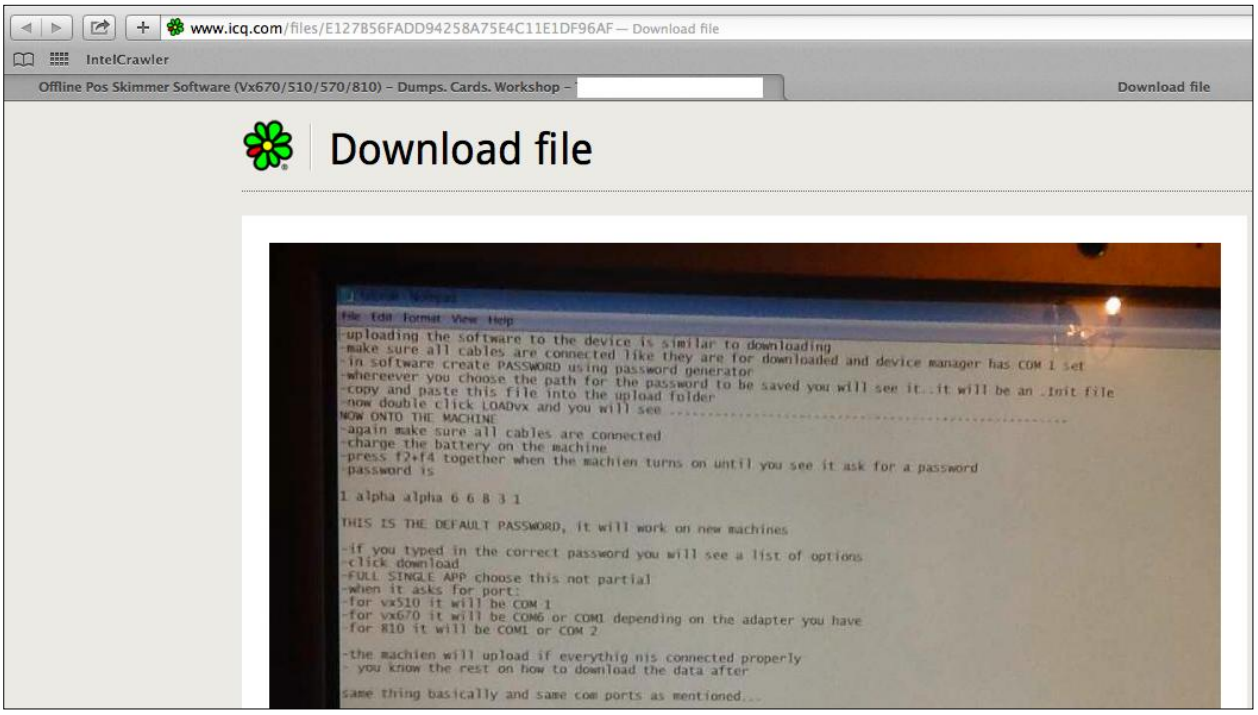
Point-of-Sale Device Tampering

It is one of the first types of crimes which became pretty popular, next to ATM skimming, having less risks in terms of physical security for the organized crime groups.

№	Sign	Details
1	Periodical electricity outage	In order to not be detected, the insiders turn off the electricity in order to disable CCTV and video surveillance systems during installation of a tampered device or the process of its tampering using special electronic "bugs" for data interception
2	Short-term POS devices restart or stop functioning during business hours	The process of device replacement from legitimate to tampered usually takes time, especially in the hands of an inexperienced insider; that's why the delay can be significant and visible
3	Visual design abnormalities	Incorrect manufacturer's name, model and serial number, suspicious additional marks, absence of manufacturer's labels
4	The appearance of portable devices in hands of employees with additional connection cables	In order to extract the data from a tampered device, the bad actor traditionally uses a RS-232 connection through a serial cable to their own laptop or portable device
5	The appearance of new non-registered POS devices	A new tampered device is not registered with its serial and model number
6	Employee due diligence	In some cases, insiders are hired by bad actors remotely as "money mules"; backgrounds of such persons don't need to include experience like POS operator or can have other suspicious signs

Table 1 – The signs of possible insider threat in POS environment

Most tampered devices use special modified firmware which encrypts all the compromised credit card data. In order to extract it, you need to know the exact crypto algorithm and how to do it. Traditionally, it is defined by combinations of various buttons.



Pic.1 - Found tutorial for modified Verifon Vx570/510/570/810 POS terminal on how to extract compromised credit cards from its internal memory (F2+F4, “1 alpha alpha 6 6 8 3 1”)

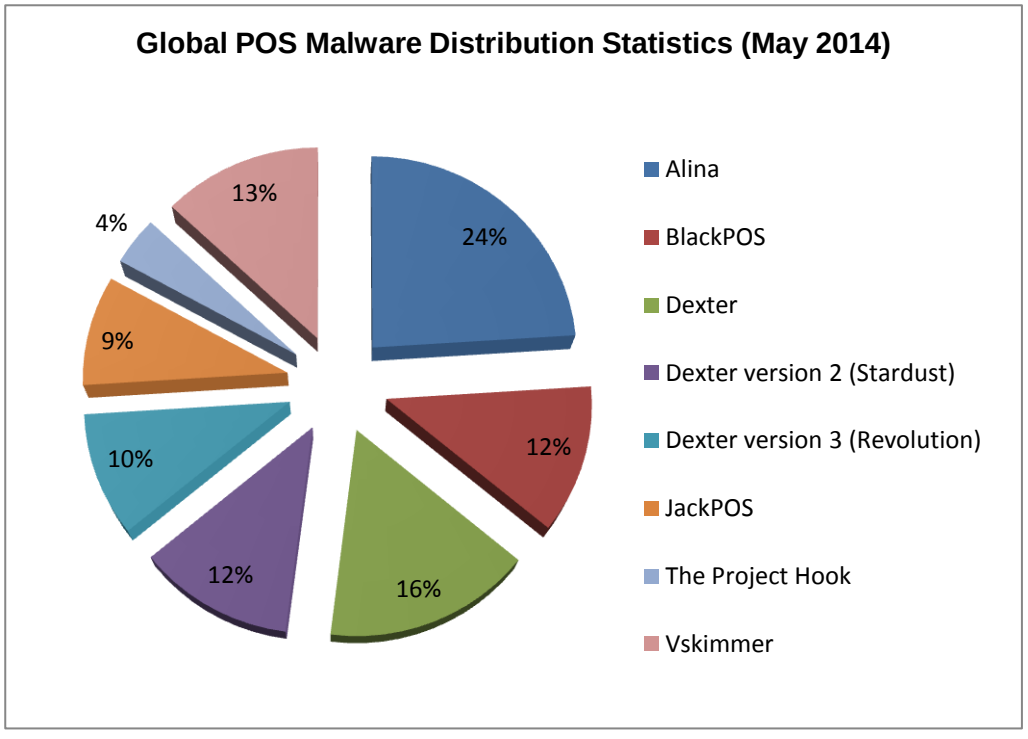
Point-of-Sale Device Infection

Infected POS terminals in various small businesses, stores and retailers have become one of the key sources of compromised credit cards for modern cybercriminals.

Pic.2 - Infection of POS terminals allows cyber criminals to receive new Track 2 dumps at a high frequency depending on the POS location and flow of customers

There are several popular families of POS malware, such as Alina, BlackPOS, Dexter, JackPOS, and Vskimmer, which are widely spread on the black market.

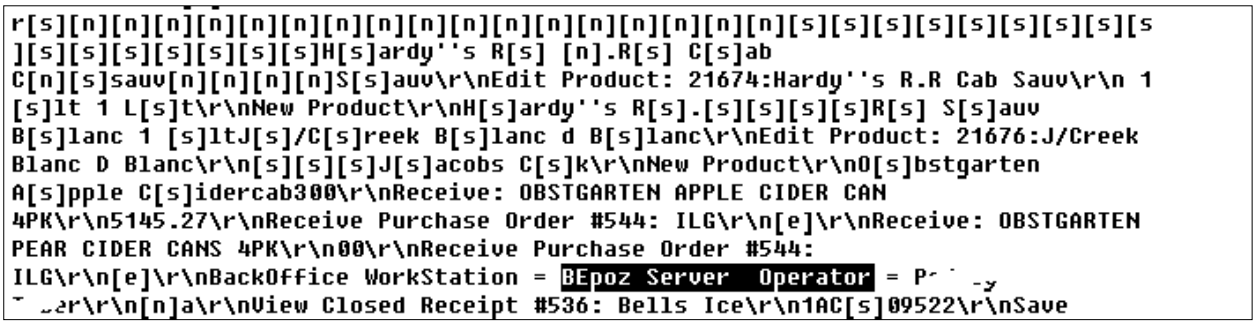
Their function is based on the same principles and are targeted at RAM scrapping under Microsoft Windows. Credit card data is extracted by signatures and predefined templates using regular expressions.



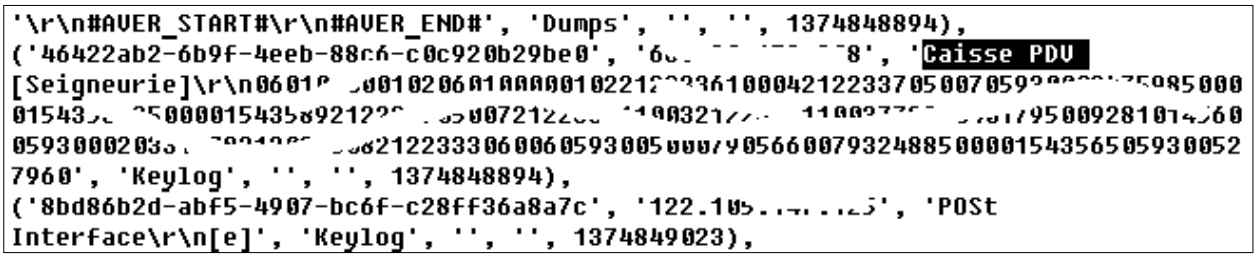
Compromised POS and Accounting Systems' Fingerprints

During the "Nemanja" botnet investigation, thousands of infected compromised POS terminals, accounting systems, and grocery management systems were identified, which helped to collect various fingerprints characterizing the victims. This kind of malware has an advanced option of PC-based terminals and supports a large range of its software.

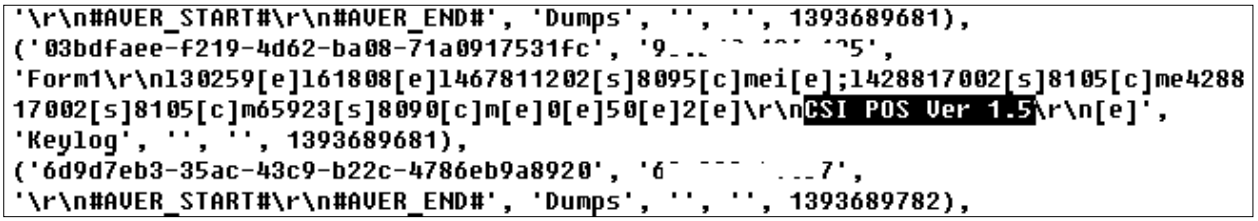
BEpoz Point of Sale System



Caisse PDV



CSI POS Ver 1.5



CxPOS V8.1 - Cybex Systems POS

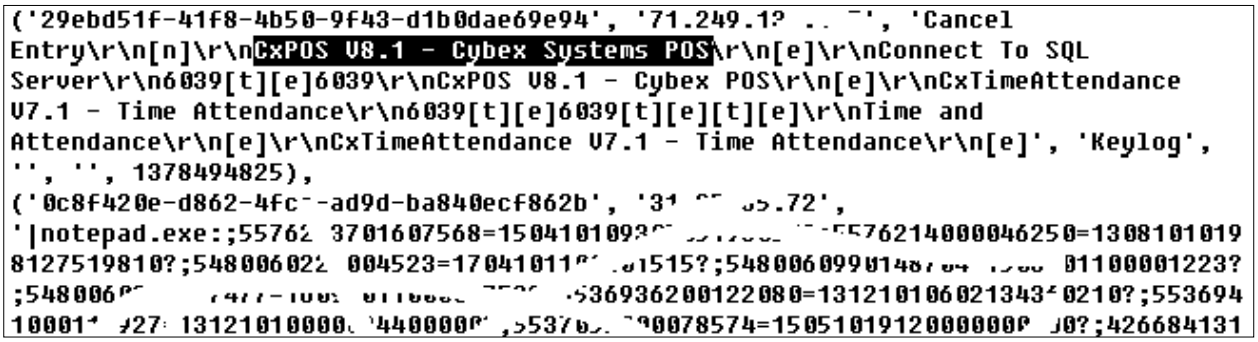
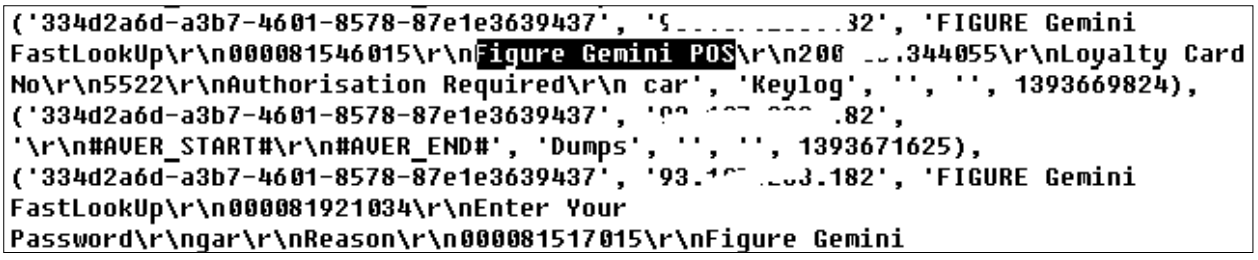
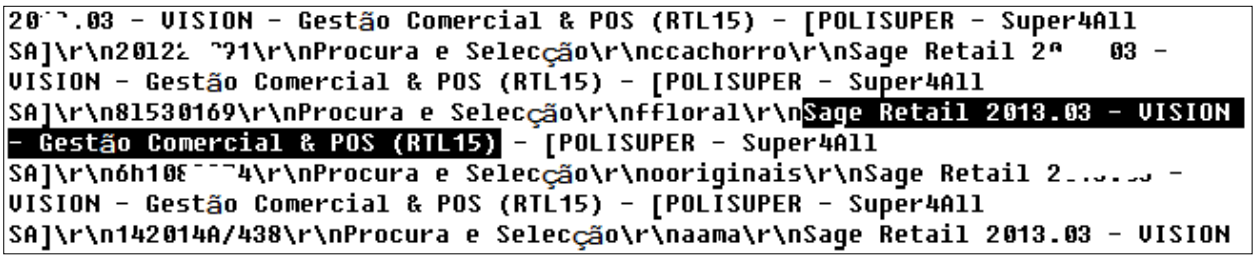


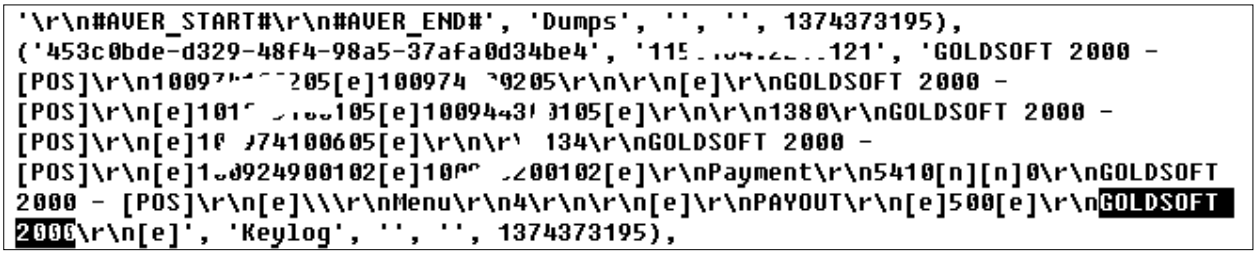
Figure Gemini POS



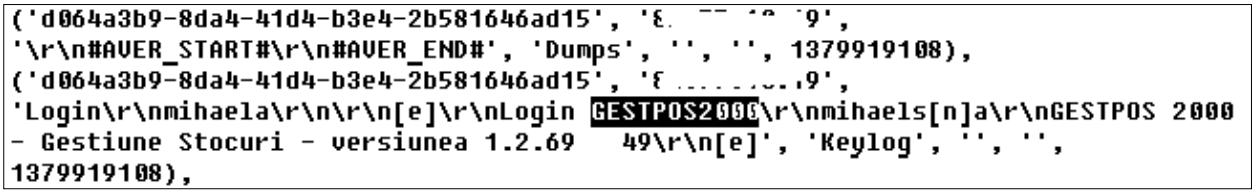
Gestão Comercial + POS VISION



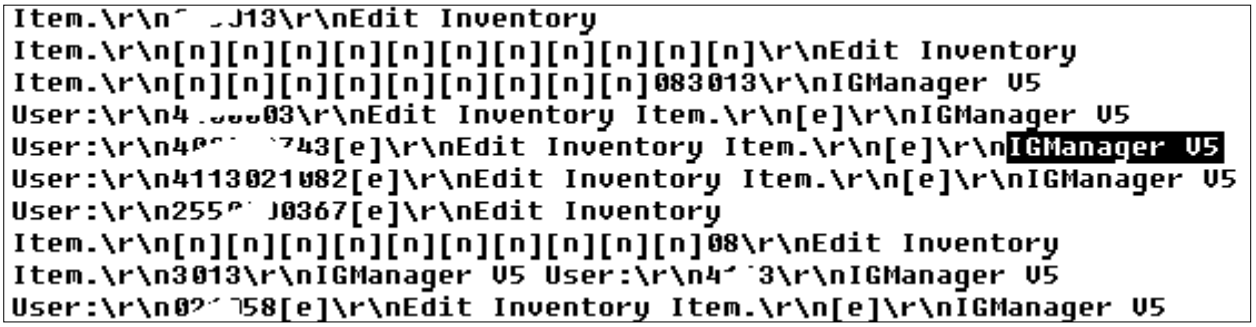
GOLDSOFT 2000 Accounting System



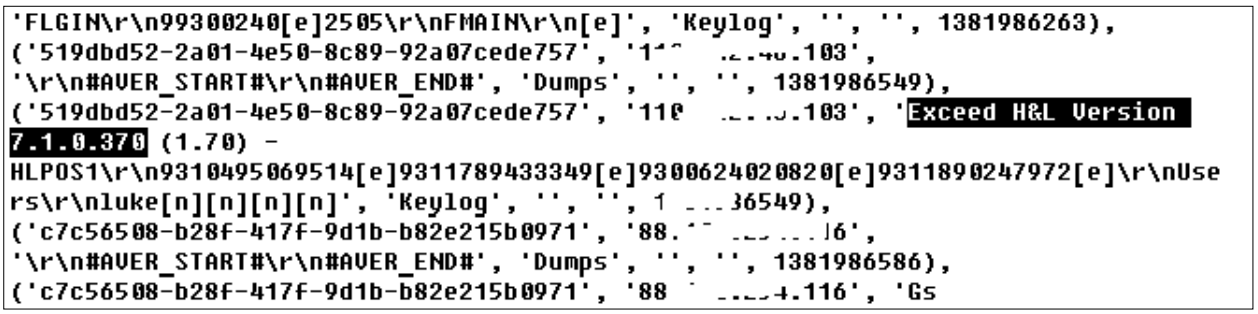
GESTPOS 2000



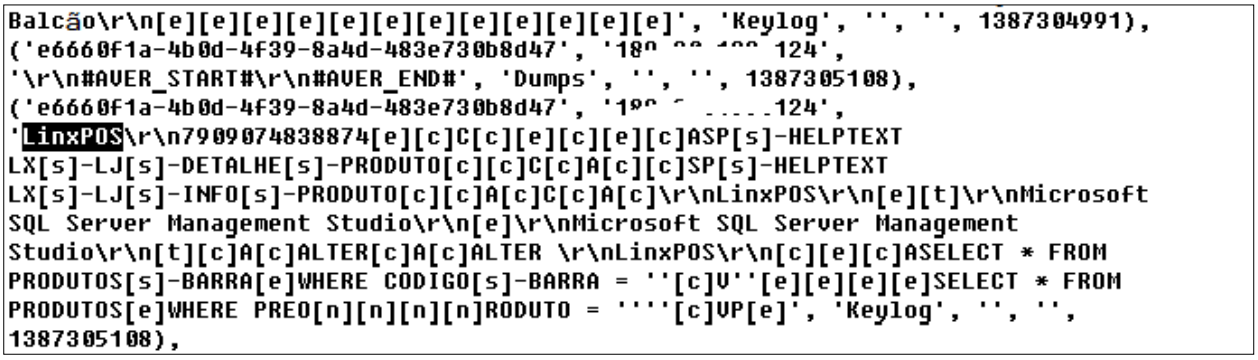
IGManager



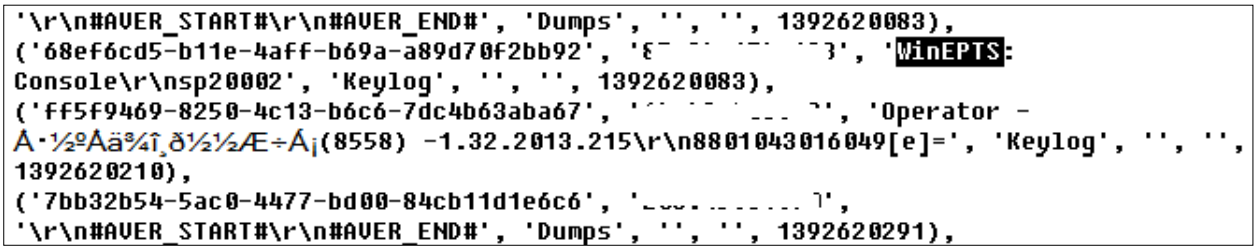
Integrated POS Software Solutions – H&L Australia



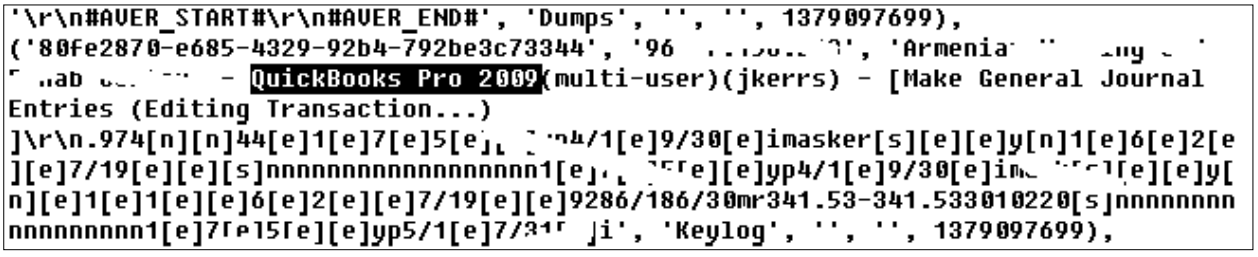
LinxPOS



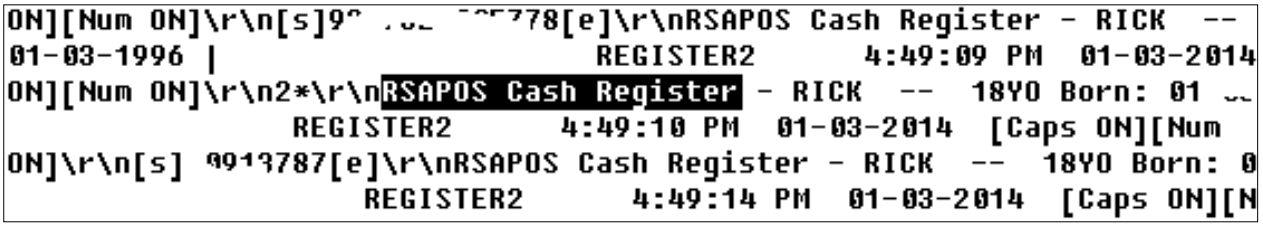
NCR WinEpts Software Solution



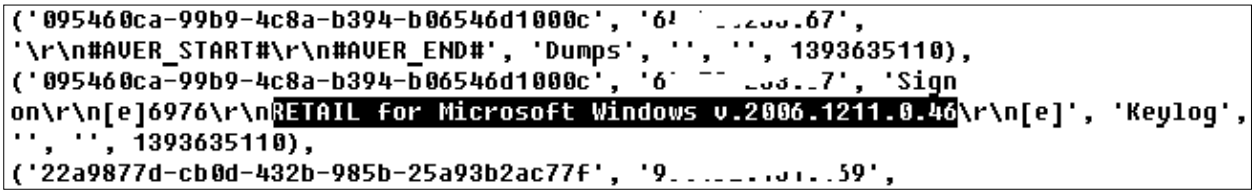
QuickBooks Pro Accounting Software



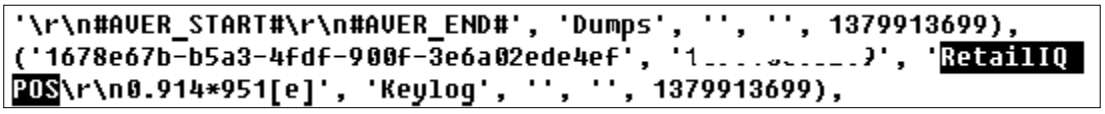
RSAPOS - Retail Systems



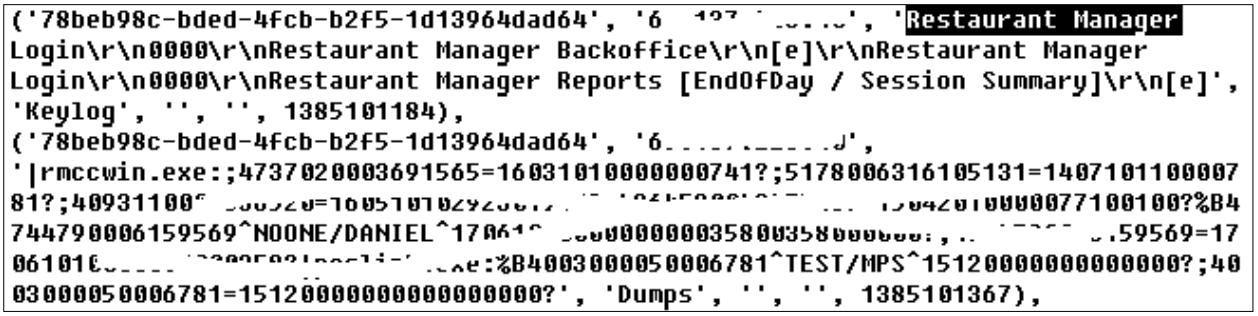
RETAIL for Microsoft Windows v.2006.1211.0.46



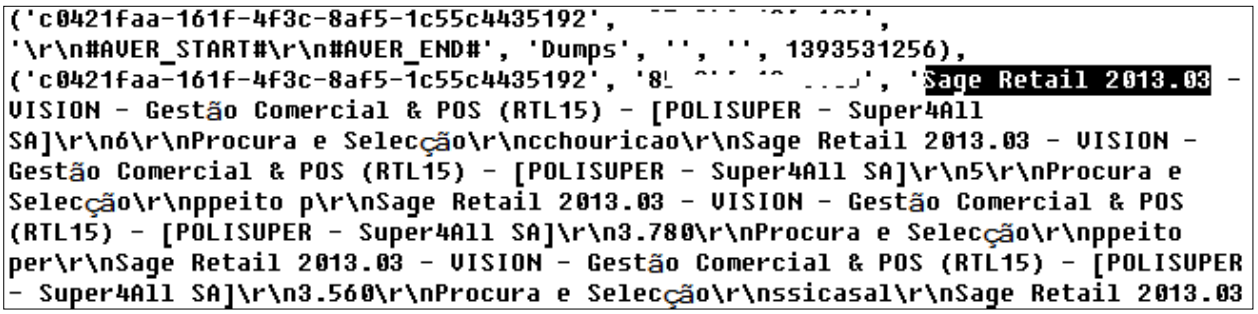
RetailIQ POS



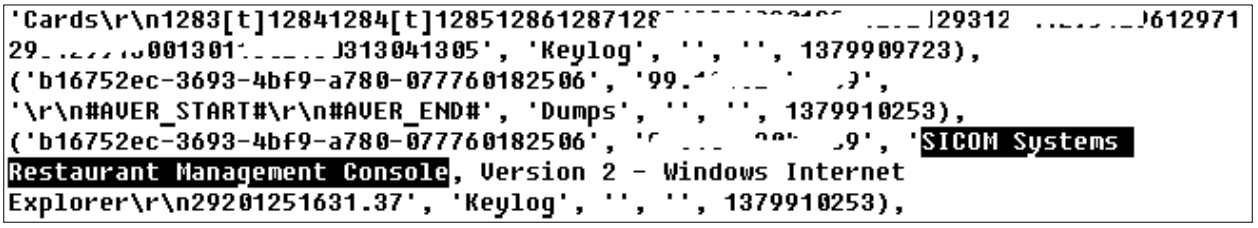
Restaurant Manager



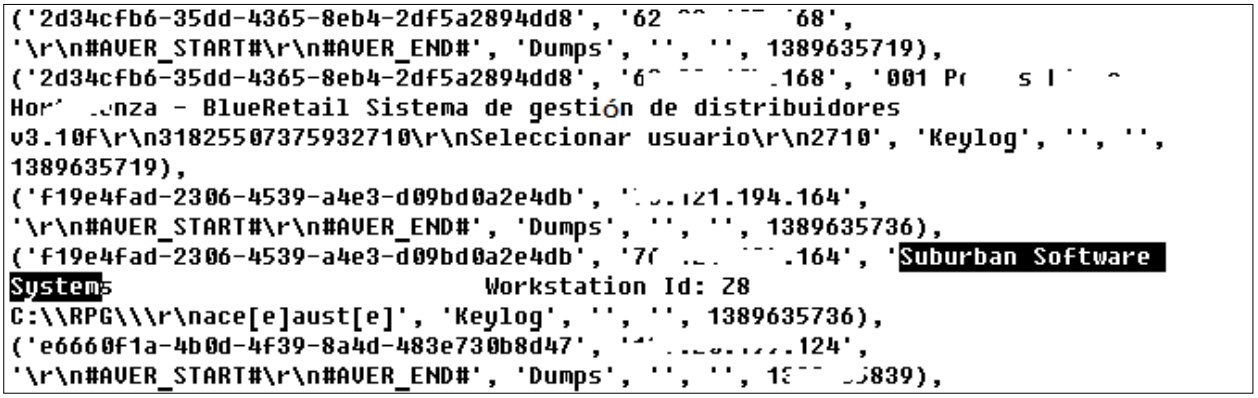
Sage Retail 2013.03



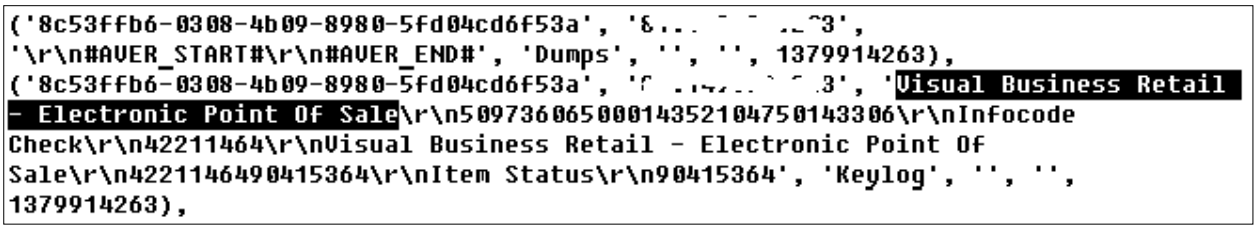
SICOM Systems Restaurant Management Console



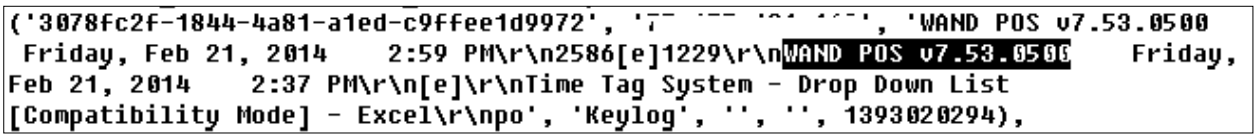
Suburban Software System



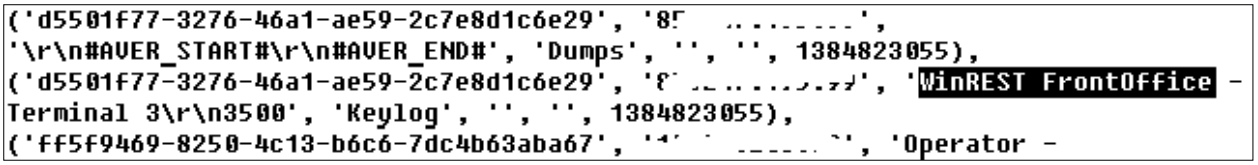
Visual Business Retail - Electronic Point Of Sale



WAND POS



WinREST FrontOffice



WinSen Electronic Manager

Note: *The provided list of examples of compromised systems with their fingerprints in the analyzed botnet doesn't mean that these software products have vulnerabilities or are insecure for further use. This example shows that famous retailers, accounting and grocery management systems used in different countries were affected by various types of POS malware.*

Money Laundering Using POS

Fraudsters actively use POS terminals registered on their own "grey" merchants for stolen credit card cashouting – "Dump + PIN cashout services."

Traditionally, fraudsters used "money mules" hired remotely in order to record compromised Track 2 data to credit card templates and to use them doing orders in various shops.

Pic. 3 – The bad actors record stolen Track 2 data to "white plastic"

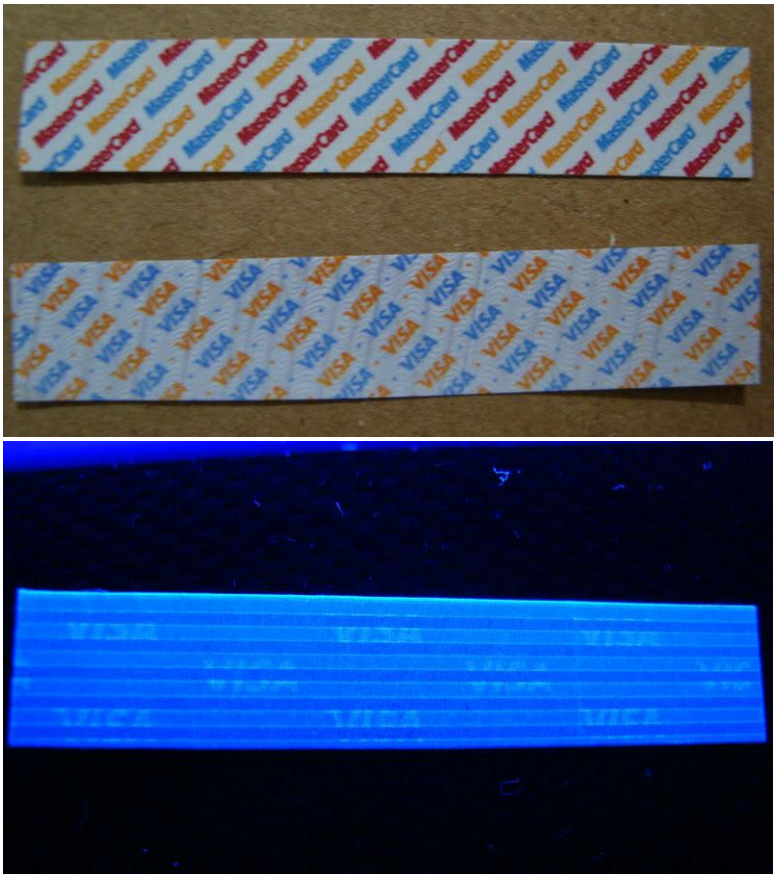
In order to avoid suspicion, they have managed to create individual designs for each card, embossing their own names and printing holograms of card associations, which is still a large secondary market.

Members of the gang involved in the "Nemanja" botnet used their own contacts in the underground in order to buy high-quality credit card templates for further swiping. Sometimes the use of such kinds of materials doubles the price of a compromised card, but bad actors vitally need it.

Pic. 4 – Fake holograms are still one of the most demanded types of product for "carders," including POS fraudsters

Pic. 5 –High-quality fake credit card hologram

The quality of accessories for stolen credit cards became really high, which made this type of underground more open using the ability to grab credit card dumps from POS systems absolutely remotely using malware without any need to be near it physically.



Pic. 6 – Fake holder stripes look real, and confirm the level of quality

Money Laundering Using mPOS

The case of the “Nemanja” botnet showed a pretty interesting scheme of money laundering using mPOS terminals, which was used by one of the key members.

There appeared to be quite a large market for mobile POS solutions, which helps to create mobile checkout stations from anywhere. It provides the ability for a customer transaction to be documented by a smartphone or tablet instead of a traditional checkout register.

Pic. 7 – Using mobile POS money laundering became more mobile

During 2013, several underground services which provide an opportunity to buy registered corporate banking accounts and legal entities together with mobile POS terminals were uncovered. Each POS terminal is registered as a legal entity such as a private company or an individual entrepreneur, through which it is possible to process some “grey” amounts of money and to legalize it through the chain of specially prepared banking accounts.

The owners of such sophisticated money laundering services guarantee that the received money won’t be blocked close to a month, but they don’t have any responsibility for any illegitimate actions with provided device.

Criminals provide a full set of money laundering activities – incorporation documents on legal entity, corporate credit cards or cards registered to money mules, if the scheme is planned to be used for serious cashout through ATMs, after stolen money is loaded to Point-of-Sale, linked banking account with remote control and attached credit card to it, SIM-card to the account.

The manufacturing period of such activities is close to 3 weeks according to the terms of these underground services, probably because the criminals need time to prepare everything correctly. The minimum pricing of such kinds of work starts from 4,000 USD to 10,000 USD. There is also an option to registered Point-of-Sale on your details, if you have already prepared your own entities for underground economy business.

The uncovered organized crime group uses a very wide range of mPOS equipment:

- Paybyway;
- SumUP;
- SimplePay;
- Lifepay;
- Pay-Me;
- 2CAN.

Some of the named devices are very widely spread in Austria, Germany, Brazil, South Africa and United Kingdom for mobile acquiring services. The differences between them is in the timeframes of receiving the funds (sometimes, it takes two days; others work instantly) and the geography of payment processing, including payment limits, as some of them work through foreign banking institutions, which helps criminals to process stolen cards from different countries. The services started in September 2012 and are still active, gathering lots of interest from fraudsters.

Investigation Case Studies

There are several types of crimes which are popular in modern the e-Crime underground with help of POS. Modern cybercrime groups understood that this niche is more cost efficient than classical ATM skimming, and more mobile, providing a pretty similar impact.

Australia
Using the "drive-by-download" attack, the bad actors have distributed the "Pony" loader which was used for uploading POS malware on specific compromised stations.

Germany
The bad actors infected a hotel booking system which was connected to a POS terminal. The infection was done because of a weak password security policy and insecure RDP access. Besides payment data, various personal identifiable information including ID scans were stolen.

South Africa
Bad actors infected POS terminals 6 months before successful detection of one of the infected stations. The infection was done potentially using an insider or weaknesses in the network perimeter and remote administration protocols.

USA
Lots of POS terminals installed in stores, car wash stations, and gas stations were infected by the "Nemanja" malware, some of which were self-deleted after some period of time.

№	Recommendation
1	After the insider is detected, allow him to gather new credit card data, using his own prepared cards in order to track further the fraud lifecycle for cybercrime chain detection and monitoring
2	Create an image of detected tampered POS devices in order to not lose possible digital evidence and compromised data archives
3	Create an image of detected infected POS terminal using a hardware write-block device (forensics disk controller) and a "bit-by-bit" hard drive duplicator copy
4	Detect a C&C server after the malicious code is extracted from infected POS terminal and make cross-checking procedures across your network environment to detect other potentially compromised hosts using destination IP addresses of outgoing network packets in HTTP/FTP traffic
5	We don't recommend you to bruteforce any encryption algorithms on tampered or infected POS terminals, as the bad actors develop special ways to self-delete active malware or compromised credit card data

Table 2 – Recommendations for Incident Response and Investigations

Conclusion

Past incidents showed a lot of attention from modern cyber criminality to retailers and small business segments having POS terminals. We predict the increasing number of new data breaches in both sectors in the coming years, as well as the appearance of new types of specific malicious code targeted at retailers' back-office systems and cash registers.

Card associations should expect this trend of POS infections in developing countries in the near future, because of a high significant lag in retailers' information security. Current statistics also point at not falling interest to countries with a high social grade and developed payment industry, such as AUS, EU, US, CA and UK. IntelCrawler predicts that very soon modern POS malware will become a part of online-banking trojans and other harmful software acting as a module, which may be used along with keylogger and network sniffing malware.

The details from the "Nemanja" botnet were added to the IntelCrawler Intelligence Platform and "PoS Malware Infection Map" (PMIM)[2] and are provided as security feed for card associations, payment providers and various vetted parties, consisting of compromised merchants, IP addresses of infected terminals and additional information for fraud prevention.

About Infected Point-of-Sale Terminal[3] Feed

It comprises a list of compromised payment terminals and network hosts installed in various small businesses and retailers. IntelCrawler has unique experience in investigations of POS related e-Crimes and aggregates various information about the distribution of malware targeted at RAM Scrapping, such as Alina, BlackPOS, Dexter, JackPOS, VSkimmer and its modifications.

Some parts of this data are illustrated on the PoS Malware Infection Map with details on the approximate number of compromised credit cards, geography and IP addresses of identified infected network hosts. The feed can be delivered through secure customers' portal or encrypted e-mail notifications in various formats (XML, JSON, CVS, RAW).

This feed is a part of AML & Fraud Intelligence, a block of services targeting comprehensive analysis of potential risks to financial institutions, insurance companies, investment groups, private companies and corporations in terms of money laundering and fraud risks.

IntelCrawler welcomes security researchers, threat intelligence analysts, fraud investigations, industry leaders, security vendors, card associations and international LEA for beneficial collaboration and information exchange using secure ways of communications. Contact our team by e-mail at: info@intelcrawler.com (PGP).

[2] **IntelCrawler's PoS Malware Infection Map** - http://intelcrawler.com/about/pmim
[3] **IntelCrawler's Compromised PoS Terminals Feed** - http://intelcrawler.com/about/posfeed