Unofficial ClamAV signature making walkthrough (first draft)

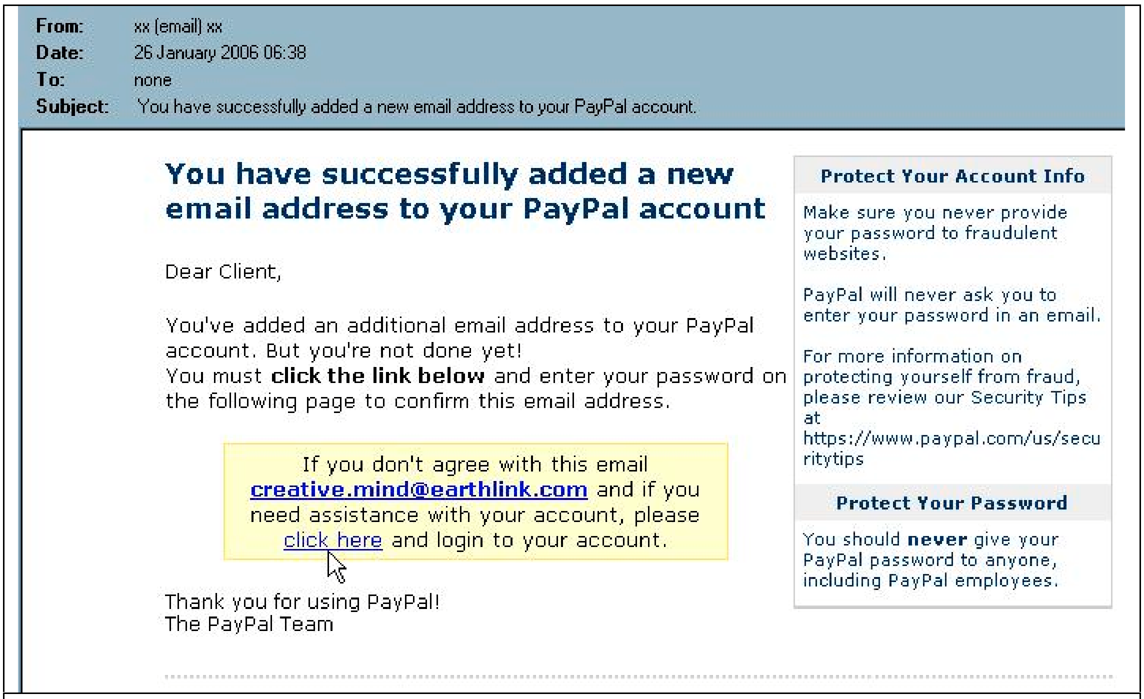
```
+>fraud%Redirect autoreply into the 'fraud' mailbox
From:service@paypal.co.uk
From:@paypal.com
From:@ebay.com
```

Our windows vpop3 email server is set to divert any paypal/ebay from addresses, into a fraud mailbox

```
C:\CLAMAV~1\bin>clamscan c:\tmp
c:\tmp/pay06012700.eml: OK

----------- SCAN SUMMARY -----------
Known viruses: 43872
Engine version: devel-20060126
Scanned directories: 1
Scanned files: 1
Infected files: 0
Data scanned: 0.02 MB
Time: 2.045 sec (0 m 2 s)
```

Scan sample email, from fraud mailbox with **default signatures** from ClamAv



From: xx (email) xx
Date: 26 January 2006 06:38
To: none
Subject: You have successfully added a new email address to your PayPal account.

You have successfully added a new email address to your PayPal account

Dear Client,

You've added an additional email address to your PayPal account. But you're not done yet!
You must **click the link below** and enter your password on the following page to confirm this email address.

If you don't agree with this email creative.mind@earthlink.com and if you need assistance with your account, please click here and login to your account.

Thank you for using PayPal!
The PayPal Team

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at https://www.paypal.com/us/securitytips

Protect Your Password

You should **never** give your PayPal password to anyone, including PayPal employees.

Examine **missed sample** Phishing Email, looking for key phrases that look “out of place”, for example, “**click the link below**” and “**enter your password on the following page**”

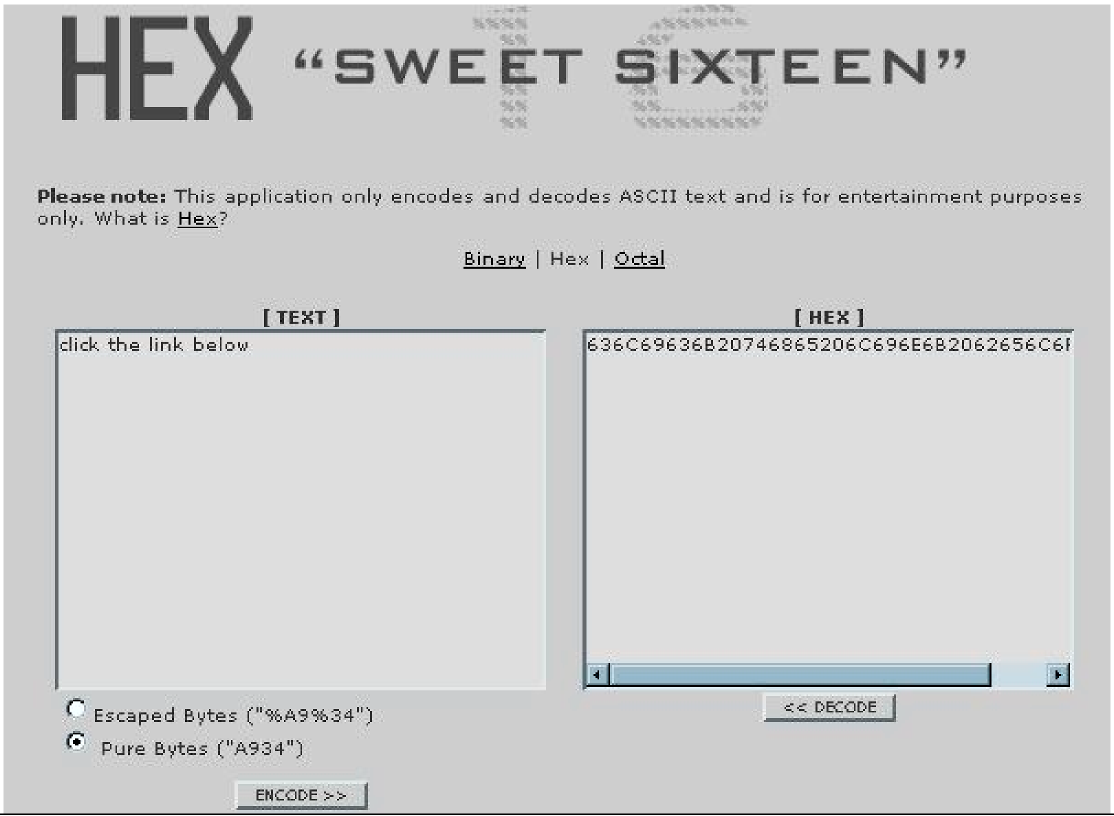
```
Subject:  You have successfully added a new email address to your PayPal account.
Date: Thu, 26 Jan 2006 08:38:58 +0200
MIME-Version: 1.0
Content-Type: text/html;
charset="Windows-1251"
Content-Transfer-Encoding: 7bit
```

```
<br/>You must <span class="emphasis">click the link below</span> and enter your password on the following page to confirm this email address.</font></p>
```

Example format of email:

a) headers show it’s html format, so would be good to create signature to **match html format only**.

b) “click the link below” and “enter your password on the” are separated by html tags, so need to be skipped



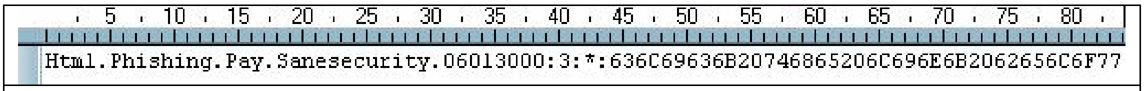
Please note: This application only encodes and decodes ASCII text and is for entertainment purposes only. What is Hex?

[TEXT]
click the link below

[HEX]
636C69636B20746865206C696E6B2062656C6F

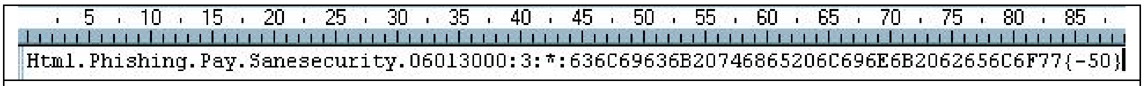
○ Escaped Bytes ("%A9%34")
● Pure Bytes ("A934")

1. Go to http://nickciske.com/tools/hex.php
2. Paste in "click the link below" (convert text to lowercase if email is html format (normalised))
3. Select "Pure Bytes ("A934")" and Click Encode button.



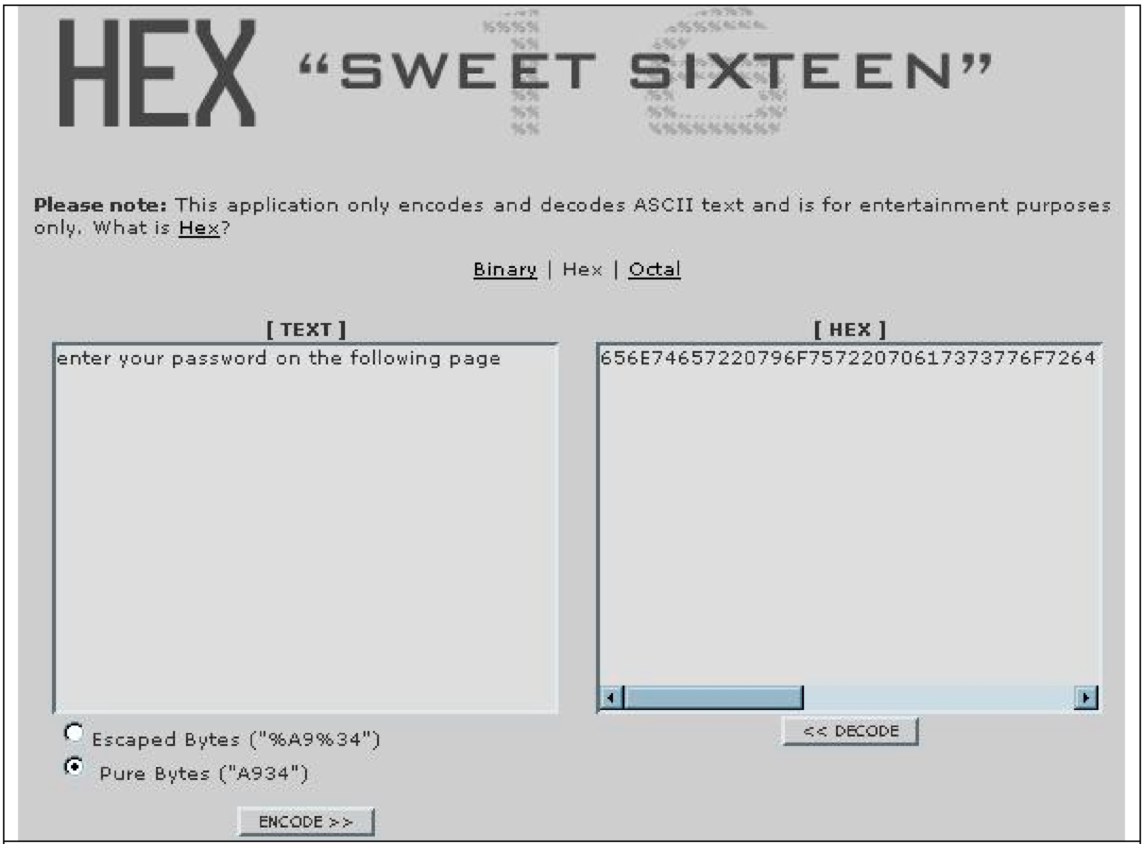
```
Html.Phishing.Pay.Sanesecurity.06013000:3:*:636C69636B20746865206C696E6B2062656C6F77
```

1. Create test database, eg: phishtest.ndb
2. Create unique "header", eg Html.Phishing.Pay.Sanesecurity.06013000:3:*:
3. Past in first page of pattern "636C69636B20746865206C696E6B2062656C6F77"



```
Html.Phishing.Pay.Sanesecurity.06013000:3:*:636C69636B20746865206C696E6B2062656C6F77{-50}
```

1. Need to skip some html tags (possible tags too)
2. Add to pattern "{-50}"



Please note: This application only encodes and decodes ASCII text and is for entertainment purposes only. What is Hex?

[TEXT]: enter your password on the following page

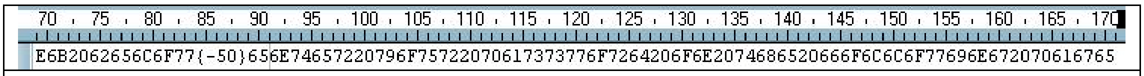
[HEX]: 656E74657220796F757220706173737776F7264

○ Escaped Bytes ("%A9%34")
● Pure Bytes ("A934")

1. Need to match text, "enter your password on the following page"
2. Go to http://nickciske.com/tools/hex.php

3. Paste in "enter your password on the following page" (convert text to lowercase if email is Html format (normalised))

4. Select "Pure Bytes ("A934")" and Click Encode button



```
E6B2062656C6F77{-50}656E74657220796F757220706173737776F7264206F6E2074686520666F6C6C6F77696E672070616765
```

Past in the rest of pattern:
656E74657220796F757220706173737776F7264206F6E2074686520666F6C6C6F77696E67207061676 5

Html.Phishing.Pay.Sanesecurity.06013000:3:*:636C69636B20746865206C696E6B2062656C6F77{-50}656E74657220796F757220706173737776F7264206F6E2074686520666F6C6C6F77696E672070616765

Full signature is ready for testing

```
C:\CLAMAV~1\bin>clamscan c:\tmp
c:\tmp/pay06012700.eml: Html.Phishing.Pay.Sanesecurity.06013000 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 43873
Engine version: devel-20060126
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.01 MB
Time: 2.312 sec (0 m 2 s)
```

New signature matches.

Html.Phishing.Pay.Sanesecurity.06013000:3:*: 636c69636b20746865206c696e6b2062656c6f77 {-50} 656e74657220796f75722070617373776f7264206f6e2074686520666f6c6c6f77696e672070616765
Tidy up signature: a) convert all hex to lowercase b) format date to YYMMDD format, with 00 as reference number, in case more than one type in a day

1. Use GoogleGroups to search news.admin.net-abuse.sightings, for good keywords like "ebay","paypal","bank" etc. http://groups.google.co.uk/groups?q=ebay+sightings&start=0&scoring=d&hl=en& 2. http://www.dslreports.com/phishtrack 3. http://www.millersmiles.co.uk/
Goods Sources of current phishing attempts