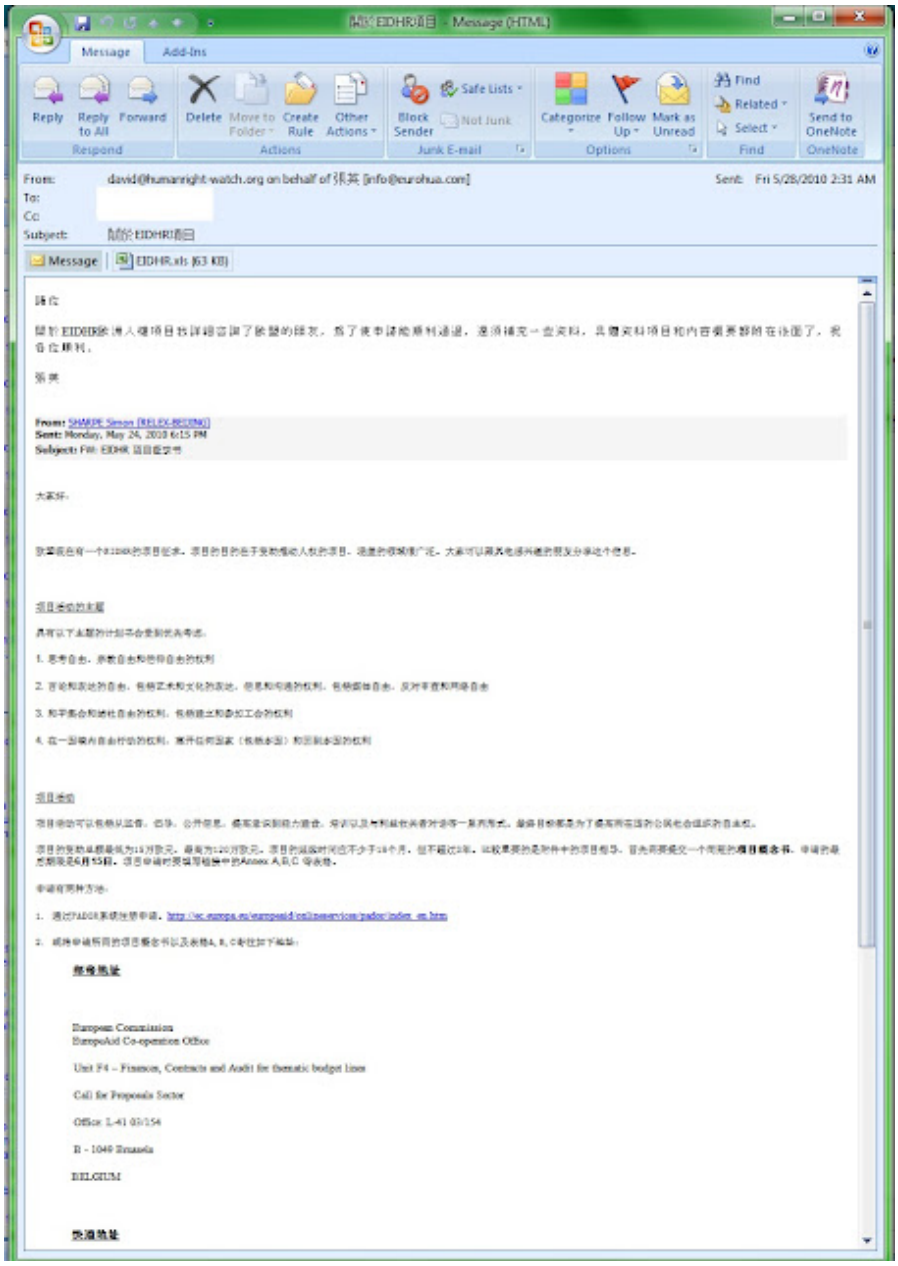
May 28 CVE-2009-3129 XLS for office 2002-2007 with fud keylogger EIDHR from david@humanright-watch.org

CVE-2009-3129 Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer 2003 SP3; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allows remote attackers to execute arbitrary code via a spreadsheet with a FEATHEADER record containing an invalid cbHdrData size element that affects a pointer offset, aka "Excel Featheader Record Memory Corruption Vulnerability."

Update: Noticed an ineresting post by Nart Villeneuve (Internet Censorship Explorer) regarding this malware and decided to update and resurrect the post
July 29, 2010 Human Rights and Malware Attacks

 Download 4f681733fd9e473c09f967fa87c9faef EIDHR.xls and all the files described below as a password protected archive (contact me if you need the password)



From: david@humanright-watch.org [mailto:david@humanright-watch.org] On Behalf Of ??
Sent: Friday, May 28, 2010 2:31 AM
To: XXXXXX
Subject: 關於EIDHR項目

諸位
關於EIDHR歐洲人權項目我詳細咨詢了歐盟的朋友，爲了使申請能順利通過，還須補充一些資料，具體資料項目和內容概要都附在後面了，祝各位順利。
張英

From: SHARPE Simon (RELEX-BEIJING)
Sent: Monday, May 24, 2010 6:15 PM
Subject: FW: EIDHR 项目征求书

大家好：

欧盟现在有一个EIDHR的项目征求。项目的目的在于资助推动人权的项目，涵盖的领域很广泛。大家可以跟其他感兴趣的朋友分享这个信息。

项目活动的主题
具有以下主题的计划书会受到优先考虑：
1. 思考自由，宗教自由和信仰自由的权利
2. 言论和表达的自由，包括艺术和文化的表达，信息和沟通的权利，包括媒体自由，反对审查和网络自由
3. 和平集会和结社自由的权利，包括建立和参加工会的权利
4. 在一国境内自由行动的权利，离开任何国家（包括本国）和回到本国的权利

项目活动
项目活动可以包括从监督，倡导，公开信息，提高意识到能力建设，培训以及与利益攸关者对话等一系列形式。最终目标都是为了提高所在国的公民社会组织的自主权。
项目的资助总额最低为15万欧元，最高为120万欧元。项目的延续时间应不少于18个月，但不超过3年。比较重要的是附件中的项目指导，首先需要提交一个简短的项目概念书，申请的最后期限是6月15日。项目申请时要填写链接中的Annex A,B,C 等表格。
申请有两种方法：
1. 通过PADOR系统注册申请。
http://ec.europa.eu/europeaid/onlineservices/pador/index_en.htm
2. 或将申请所需的项目概念书以及表格A,B,C寄往如下地址：
邮寄地址

European Commission
EuropeAid Co-operation Office
  Unit F4 – Finances, Contracts and Audit for thematic budget lines
  Call for Proposals Sector
  Office: L-41 03/154
  B - 1049 Brussels
BELGIUM

快递地址

European Commission
        EuropeAid Cooperation Office
Unit F4 – Finances, Contracts and Audit for thematic budget lines
  Call for Proposals Sector
  Office: L-41 03/154
        Central Mail Service
        Avenue du Bourget 1
        B-1140 Brussels (Evère)

BELGIUM

关于项目的具体内容在https://webgate.ec.europa.eu/europeaid/onlineservices/index.cfm?do=publi.welcome&nbPubliList=15&orderby=upd&orderbyad=Desc&searchtype=RS&aofr=126352
如果需要更多的信息，请随时与我们联系。谢谢！

欧盟驻华代表团夏明
See machine translation in the end

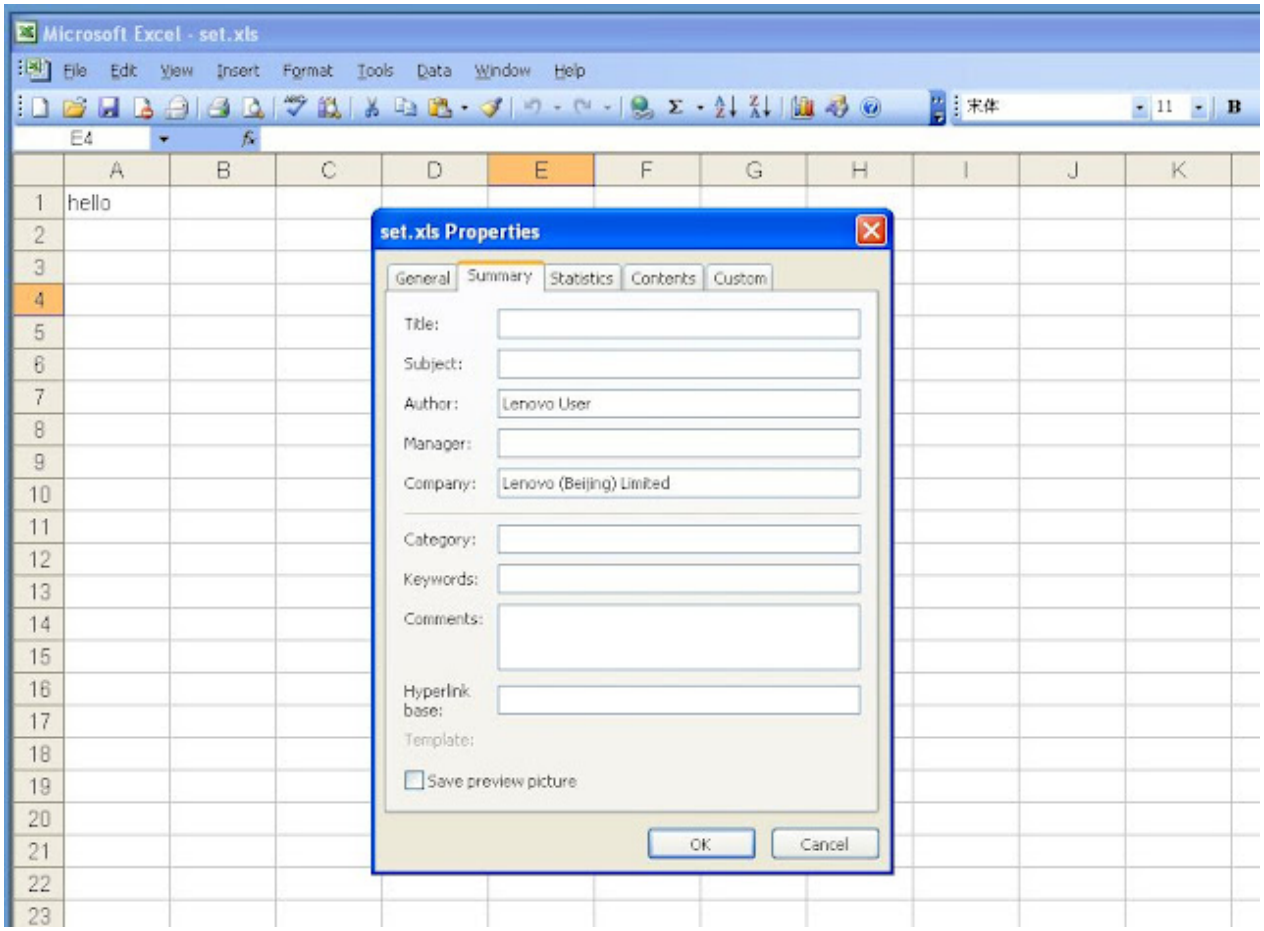
Headers
Received: (qmail 3230 invoked from network); 28 May 2010 06:31:58 -0000
Received: from static-ip-251-116-134-202.rev.dyxnet.com (HELO mx02.diaocha8.com) (202.134.116.251) by XXXXXXXXXXXXXXXXXXX with SMTP; 28 May 2010 06:31:58 -0000
Received: from sppfszwr (unknown [180.98.74.10])
by mx02.diaocha8.com (EMOS V1.5 (Postfix)) with ESMTPA id 37B71109A81
for
Reply-To:
Sender: david@humanright-watch.org
Message-ID:
From: =?utf-8?B?5by16lux?=
To: XXXXXXXXXXXXXXX
Subject: =?utf-8?B?6Zec5pa8RUlESFLpoIXnm64=?=
Date: Fri, 28 May 2010 14:31:10 +0800

Hostname: 180.98.74.10
ISP: CHINANET jiangsu province network
Organization: CHINANET jiangsu province network
State/Region: Jiangsu
City: Suzhou
AS4134

-
File EIDHR.xls received on 2010.06.02 04:13:50 (UTC)
http://www.virustotal.com/analisis/8b8960a8556033931901524 39c64ac9fd16655b304d472ecb83422900369a266-1275452030
Result: 17/41 (41.47%)
a-squared 5.0.0.26 2010.06.02 Trojan-Dropper.MSExcel.Agent!IK
AntiVir 8.2.1.242 2010.06.01 TR/Drop.MSExcel.Agent.BC
Antiy-AVL 2.0.3.7 2010.06.01 Trojan/MSExcel.Agent
Authentium 5.2.0.5 2010.06.02 MSExcel/Dropper.B!Camelot
BitDefender 7.2 2010.06.02 Exploit.D-Encrypted.Gen
F-Secure 9.0.15370.0 2010.06.02 Exploit.D-Encrypted.Gen
GData 21 2010.06.02 Exploit.D-Encrypted.Gen
Ikarus T3.1.1.84.0 2010.06.02 Trojan-Dropper.MSExcel.Agent

Jiangmin 13.0.900 2010.05.31 Heur:Exploit.CVE-2009-3129
Kaspersky 7.0.0.125 2010.06.02 Trojan-Dropper.MSExcel.Agent.bc
McAfee-GW-Edition 2010.1 2010.06.02
Heuristic.BehavesLike.Exploit.X97.CodeExec.EBEB
Norman 6.04.12 2010.06.01 ShellCode.B
nProtect 2010-06-01.02 2010.06.01 Exploit.D-Encrypted.Gen
PCTools 7.0.3.5 2010.06.02 HeurEngine.MaliciousExploit
Symantec 20101.1.0.89 2010.06.02 Bloodhound.Exploit.306
TrendMicro 9.120.0.1004 2010.06.02 TROJ_MDROPR.MRV
TrendMicro-HouseCall 9.120.0.1004 2010.06.02 TROJ_MDROPR.MRV
Additional information
File size: 64166 bytes
MD5...: 4f681733fd9e473c09f967fa87c9faef

Excel successfully opens, displaying hello, and a Chinese font set as default. The properties show that it was created on a Lenovo (Beijing) Limited laptop.



Files created

1. D52EF63FDC5C5452D9DA23BD6D4BF0F5 %userprofile%\Local Settings\Temp\1001.tmp11kb 0/41 Virustotal

2. D52EF63FDC5C5452D9DA23BD6D4BF0F5 C:\WINDOWS\ntshrui.dll 11kb 0/41 Virustotal
3. A363ABE09A44176386C50EE887359270 %userprofile%\Local Settings\Temp\set.xls 17kb -clean spreadsheet you see above

Upon reboot, it is copied to system32 as well

File: **ntshrui.dll**
MD5: d52ef63fdc5c5452d9da23bd6d4bf0f5
Size: 10720

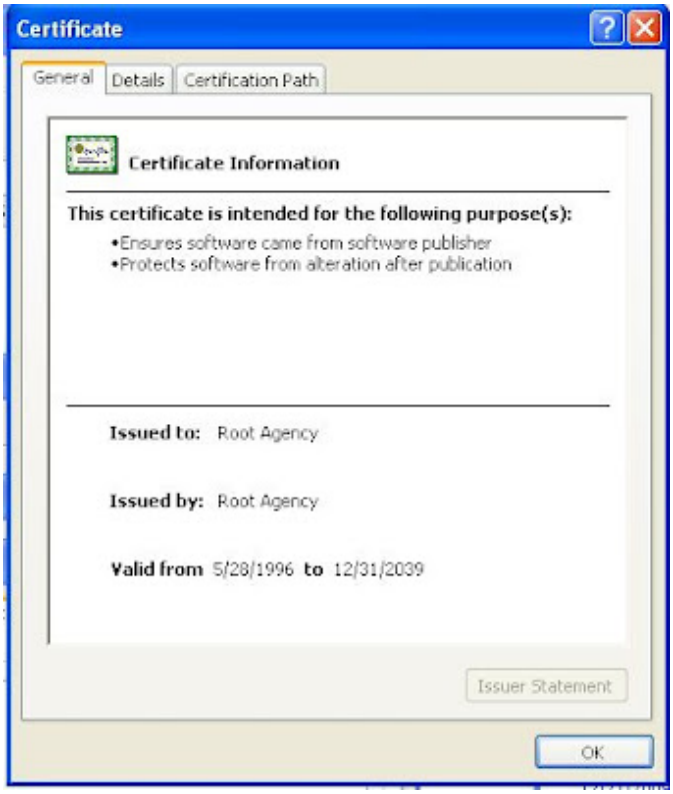
> Handle, Owner, Object,
> 0x01710000 1660: explorer.exe C:\WINDOWS\ntshrui.dll
> 0x76990000 1660: explorer.exe C:\WINDOWS\system32\ntshrui.dll

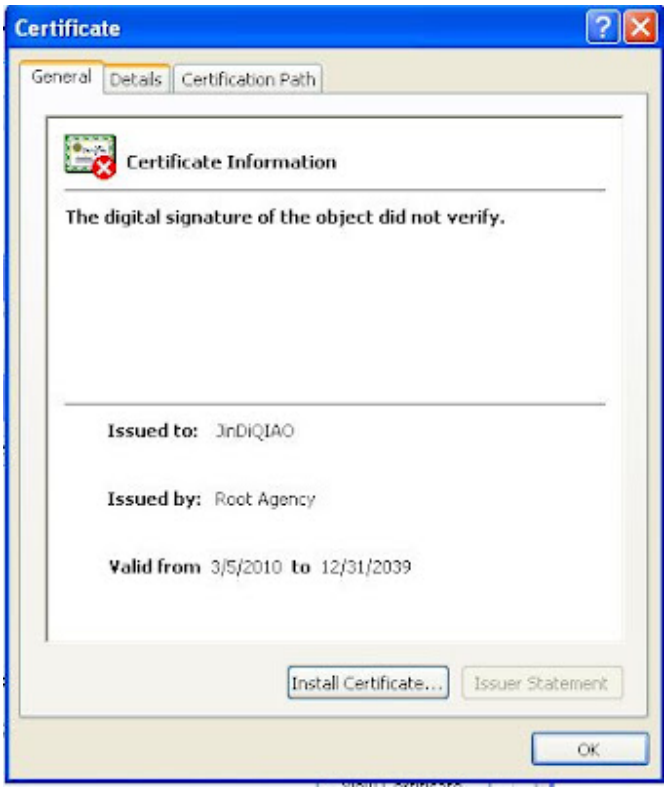
> Virustotal
> http://www.virustotal.com/analisis/accaf7b5ca9d35fe9c7e8442fc7baeaaeef5702d3c65522314edf3e0495ed398-1275476466
> File ntshrui.dll received on 2010.06.02 11:01:06 (UTC)
> Result: 0/41 (0%)
> Additional information
> File size: 10720 bytes
> MD5...: d52ef63fdc5c5452d9da23bd6d4bf0f5

The file ntshrui.dll is digitally signed - signature is invalid

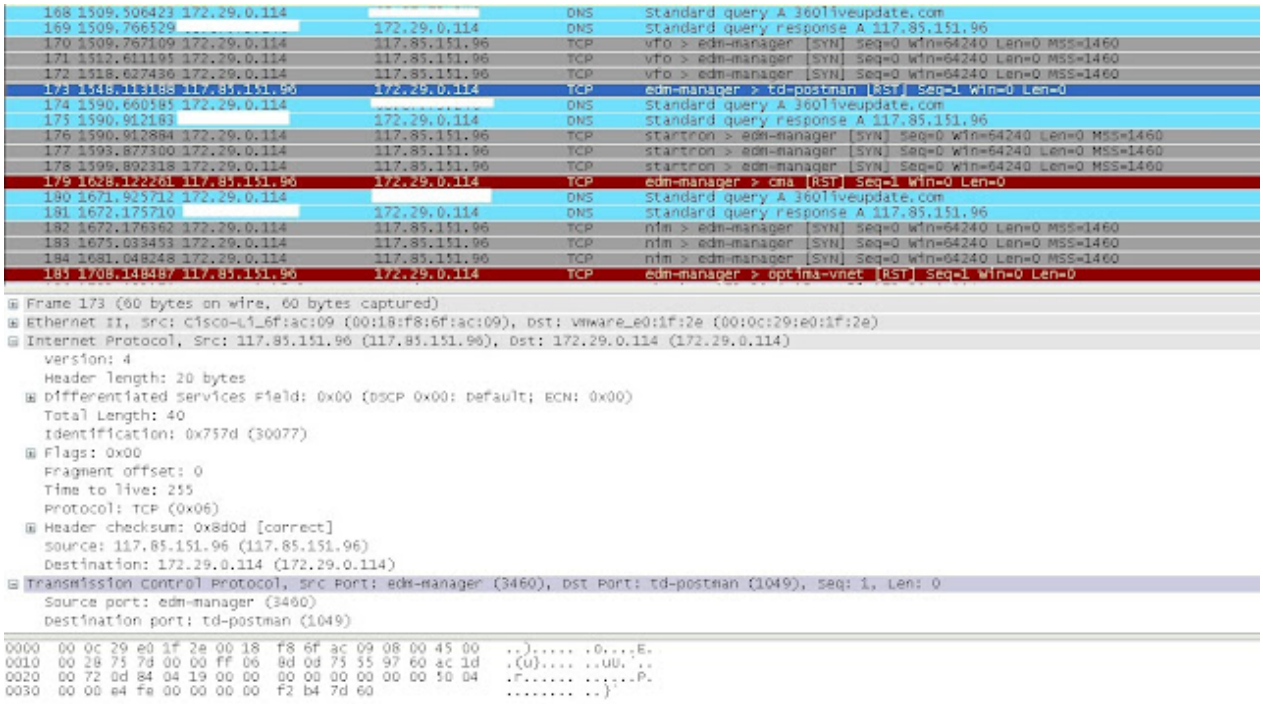
JinDiQIAO@hotmail.com

Certificate is issued by Root Agency





TCP Traffic to **117.85.151.96:3460 360liveupdate.com**



360liveupdate.com 117.85.151.96

360liveupdate.com is a domain controlled by two name servers at oray.net.
Having a total of four IP numbers. All four of them are on different IP networks.
The name server peanutmail.newpeanut.idc stated in SOA record is not in the list of name servers. 360liveupdate.com has one IP number.
ctt.hk, 8jy.cn, ghcn.cn, 33cc.cn, jhcp.cn and at least 56 other hosts share name servers with this domain.
360liveupdate.com is hosted on a server in China.
Reputation is not yet known.It is not listed in any blacklists.Search for 360liveupdate.com.

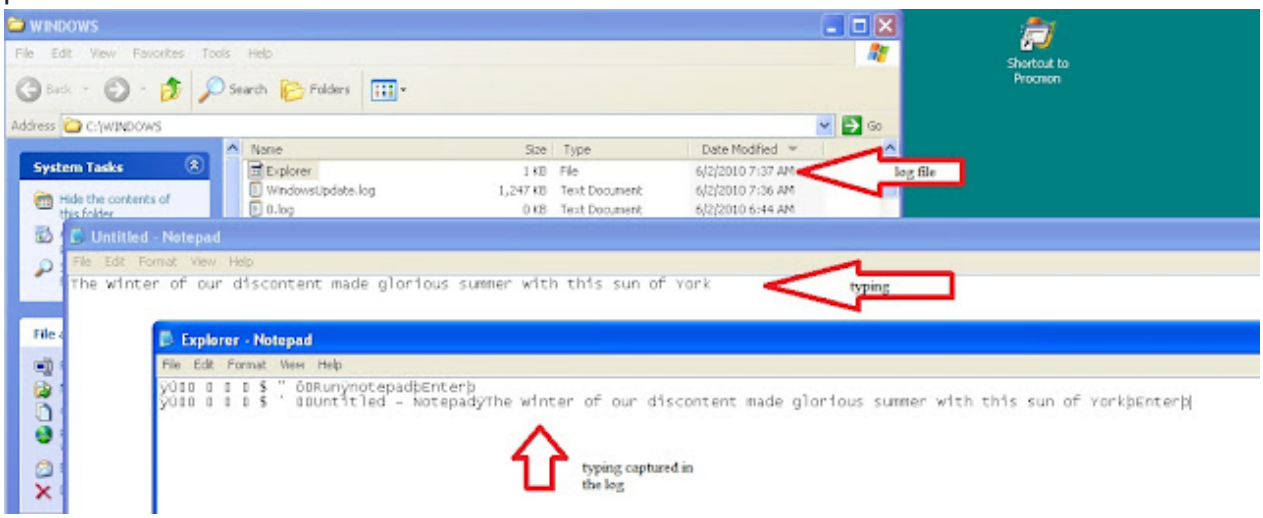
http://www.robtex.com/dns/360liveupdate.com.html#whois

```
Domain Name: 360LIVEUPDATE.COM
Registrar: XIN NET TECHNOLOGY CORPORATION
Whois Server: whois.paycenter.com.cn
Referral URL: http://www.xinnet.com
Name Server: NS1.ORAY.NET
Name Server: NS2.ORAY.NET
Status: ok
Updated Date: 29-jul-2009
Creation Date: 29-jul-2009
Expiration Date: 29-jul-2010
```

Hostname: 117.85.151.96
ISP: CHINANET jiangsu province network
Organization: CHINANET jiangsu province network
Type: Broadband
State/Region: Jiangsu
City: Wuxi

==========

Keylogging
In a few minutes after the reboot, we find a file named Explorer in the **%systemroot%** Explorer is a text log of all explorer.exe activities. This is a common type of keylogger, see the picture below



Vicheck results

https://www.vicheck.ca/malware.php?hash=4f681733fd9e473c09f967fa87c9faef

==========

From: david@humanright-watch.org [mailto: david@humanright-watch.org] On Behalf Of?? Sent: Friday, May 28, 2010 2:31 AMTo: XXXXXXSubject: About EIDHR ProjectOf youEIDHR European project on detailed consultation with my friends in the EU, in order to apply a smooth, they still need to add some information, specific items of information and content outline are attached to the back, and wish you well.Zhang YingFrom: SHARPE Simon (RELEX-BEIJING)Sent: Monday, May 24, 2010 6:15 PMSubject: FW: EIDHR project request for proposalsHello, everybody:
The EU now has a EIDHR projects seek. The purpose of the project is funded projects to promote human rights, covering a wide area. We can share with other interested friends to this information.
The theme of project activitiesThe plan has the following themes will be given priority:1. Thinking, freedom of religion and belief and freedom2. Freedom of speech and freedom of expression, including arts and cultural expression, information and communication rights,

including media freedom, freedom against censorship and network3. Peaceful assembly and freedom of association rights, including the right to establish and join trade unions4. In a country the right to freedom of movement, to leave any country (including their own) and the right to return to their

Project activitiesProject activities can range from monitoring, advocacy, public information, raising aware of capacity building, training, and dialogue with stakeholders and a series of forms. Ultimate goal is to improve the country's civil society organizations autonomy.The minimum total project funding of 15 million euros, up 120 million euros. Project duration should be less than 18 months, but not more than 3 years. More important is the annex of the project steering, first need to submit a brief project concept book, the application deadline is June 15. Project application to fill out the link in the Annex A, B, C and so on form.There are two ways to apply:1. PADOR system through the application for registration. http://ec.europa.eu/europeaid/onlineservices/pador/index_en.htm2. Or to apply for the Project Idea and the Form A, B, C Mailing Address:Mailing address

European CommissionEuropeAid Co-operation Office

Unit F4 - Finances, Contracts and Audit for thematic budget lines

Call for Proposals Sector

Office: L-41 03/154

B - 1049 BrusselsBELGIUM

Express Address

European Commission

EuropeAid Cooperation OfficeUnit F4 - Finances, Contracts and Audit for thematic budget lines

Call for Proposals Sector

Office: L-41 03/154

Central Mail Service

Avenue du Bourget 1

B-1140 Brussels (Evère)BELGIUM

Details on the project in https: / / webgate.ec.europa.eu / europeaid / onlineservices / index.cfm? Do = publi.welcome & nbPubliList = 15 & orderby = upd & orderbyad = Desc & searchtype = RS & aofr = 126352If you need more information, please feel free to contact us. Thank you!

EU Delegation Ming Xia