Collaboration

- Florida State University
- National White Collar Crime Center
- Florida Department of Law Enforcement
- Students: SriHarsha Angara, Shalini Israni
- Other Faculty: Zhenhai Duan
Outline

• Purpose of UnMask
• UnMask Architecture
• UnMask Web Interface
• UnMask Database
• UnMask Tool Server
• Email Analysis using UnMask
• Future Work
Purpose of UnMask

- Email investigation is a tedious task
- Analyzing hordes of evidence at once is overwhelming
- Support Digital forensics investigators in investigating email.
UnMask

Clients

Active Directory

Kerberos, LDAP

Authentication doing using LDAP+SSL

HTTPS

JDBC+SSL

UnMask Database

Glassfish-Web Services

Active Directory

Whois Proxy Server

INTERNET

DIG

TRACEROUTE

WHOIS

GEOIP

UnMask Tool Server

INTERNET
• Submit Emails
  • Upload .eml files
  • Cut and Paste raw emails

• View Reports
  • Report on Raw Email
  • Report on Received Headers
  • Report of Email Addresses
  • Report on URL’s
  • Query for additional information or On-Demand tools using Web Services

• Database GUI

• Account Tools

• Administrative Tools
Email Submission Tools

We offer several ways to submit email messages for processing:

- Upload a file
- Cut & Paste

Select a Case

Select a File: Choose File

Submit

Caution

Be sure to include the messages source, including headers when cutting and pasting.

It may take a few minutes before report finishes processing.
Email Submission Tools

We offer several ways to submit email messages for processing:

- Upload a file
- Cut & Paste

Select a Case

Select a File

Caution

Be sure to include the messages source, including headers when possible.
It may take a few minutes before report finish processing.
UnMask-View Reports

Email Reports

In this section, you can view different reports that we have generated. Select a case, and a file to view different types of reports.

View Report

Select a Case

Select a File
Select a Case

View Report
Select a Report to View
Email Reports

In this section, you can view different reports, that we have generated. Select a case, and a file to view different types of reports.

View Report

Select a Case

Select a File

Select a Report to View
Email Reports

In this section, you can view different reports that we have generated. Select a case, and a file to view different types of reports.

Select a Case

HAESHA_Afl

Select a File

- phishingmail_shell.eml
- phishingmail_confirmplease.eml
- phishingmail3.eml

View Report

Select a Report to View
Email Reports

In this section, you can view different reports that we have generated. Select a case, and a file to view different types of reports.

Viewing a File

FileName: phishingmail_confirmplease.eml
Date of Submission: 2009-03-13
Time of Submission: 20:42:25
Back

View Report

Select a Report to View
- View Report on Email
- View Report on Received Header
- View Report on UBI found
- View Report on Email Addresses
Delivered-To: mynameissrirahsha@gmail.com
Received: by 10.103.192.16 with SMTP id u16cs110768mup;
Thu, 15 Jan 2009 09:06:37 -0800 (PST)
Received: by 10.215.14.20 with SMTP id r20meth213665ocal.147.1323039196698;
Thu, 15 Jan 2009 09:06:36 -0800 (PST)
Return-Path: <qilt.ajdutppvlkuphskfays@flashfame.com>
Received: from flashfame.com (flashfame.com [208.95.166.229])
by mx.google.com with ESMTP id 7s135053ywo.46.2009.01.15.09.06.35;
Thu, 15 Jan 2009 09:06:35 -0800 (PST)
Received: SPF: pass (google.com: domain of qilt.ajdutppvlkuphskfays@flashfame.com designates 208.95.166.229 as permitted sender) client-ip=208.95.166.229;
DomainKey-Status: good
Authentication-Results: mx.google.com, spf=pass (google.com: domain of qilt.ajdutppvlkuphskfays@flashfame.com designates 208.95.166.229 as permitted sender) smtp.mail=qilt.ajdutppvlkuphskfays@flashfame.com, domainkeys=pass header.from=StimulusCheck@selfbusinessconcepts.com
DomainKey-Signature: q=dns; a=rsa-sha1; c=nofws;
s=+512; d=sefbusinessconcepts.com;
h=Message-ID:Date:Reply-To:To:Subject:Mime-Version:Content-Type:Content-Transfer-Encoding:X-Plumb:X-Comparing;
b=WQBbAT+uv1BQF2FIR/80TkLXE4MRRffkqF+1bDspNnRNJUS/19FYVeLoahkmc1
3psrBONWjym9Q9q0q7Zjg=
Message-ID: <301498423.132303919266.qilt.ajdutppvlkuphskfays@flashfame.com.1799866189>
Date: Thu, 15 Jan 2009 12:08:32 -0500 (EST)
From: Stimulus Check <StimulusCheck@SelfBusinessConcepts.com>
Reply-To: Stimulus Check <qilt.ajdutppvlkuphskfays@flashfame.com>
To: mynameissrirahsha@gmail.com
Subject: $1,000 stimulus check - get economic relief.
Mime-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-Plumb: Drop a line to qilt.ajdutppvlkuphskfays@flashfame.com for no more
X-Comparing: ev 1 kBo er0Bbg avjM67

<HTML>
<BODY>
<IMG SRC="http://www.flashfame.com/executive/2g9ko771wxf0cti1vypj7zveyrla4vff4fl/b.gif" WIDTH=1 HEIGHT=1>
<table align="center"><tr><td style="padding: Opt Opt 10px; font-family: Verdana,Arial; font-style: normal; font-variant: normal; font-weight: normal; font-size: 12px; line-height: normal; font-size-adjust: none; font-stretch: normal; color: rgb(74, 0, 0); text-align: center;"><table>
<tr>
<TD width="100%" height="100%" align="center" vAlign=top borderColor+#ff3f78>
</TR>
WHOIS is a query/response protocol which is widely used for querying an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet.

First External Mail Server: from core-k.megalink.com.ua (core-k.megalink.com.ua[195.182.194.1]) by mx.google.com
Report on Received Headers

Email Reports

In this section, you can view different reports that we have generated. Select a case, and file to view different types of reports.

Viewing Report for Received Headers

Internal Received Headers are not shown

```
(core-k.megalink.com.ua
  TRACEROUTE  DIG  GEOP

Received: from core-k.megalink.com.ua [195.182.194.1] by mx.google.com
  TRACEROUTE  DIG  GEOP
)
```

First External Mail Server: from core-k.megalink.com.ua [core-k.megalink.com.ua[195.182.194.1]] by mx.google.com

Additional headers:

```
> >>HEADER<< <opcode: QUERY, status: NOERROR, id: 53612
  flags: qr rd ra; qr: 1 am 1 aa 2 ad: 2
  QUESTIONS:
  core-k.megalink.com.ua., type = ANY, class = IN

  ANSWERS
  core-k.megalink.com.ua. 3600 IN A 105.182.194.1

  AUTHORITY RECORDS
  megalink.com.ua.3600 IN NS ns.megalink.com.ua.
  megalink.com.ua.3600 IN NS ns.dps.uktel.net.

  ADDITIONAL RECORDS
  ns.dps.uktel.net. 186932 IN A 195.5.61.70
  ns.megalink.com.ua. 80531 IN A 195.182.194.3

  Message size: 135 bytes
```

DIG ANY RESULT: core-k.megalink.com.ua.
DIG ANY RESULT: core-k.megalink.com.ua

;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 53812
flags: qr rd ra ; qd: 1 an: 1 au: 2 ad: 2
QUESTIONs:
core-k.megalink.com.ua., type = ANY, class = IN

ANSWERS:
core-k.megalink.com.ua. 3600 IN A 195.182.194.1

AUTHORITY RECORDS:
meagalink.com.ua.3600 IN NS ns.megalink.com.ua.
megalink.com.ua.3600 IN NS ns.dp.ukrtel.net.

ADDITIONAL RECORDS:
ns.dp.ukrtel.net. 166932 IN A 195.5.61.70
ns.megalink.com.ua. 80531 IN A 195.182.194.3

Message size: 135 bytes

GEO IP/COUNTRY RESULT: core-k.megalink.com.ua

City: Dnepropetrovsk
Region: 04
Country: Ukraine
Zipcode: null
Latitude: 0.0
Longitude: 0.0
Area Code: 0
Report on URL's

Viewing Report for URLs Found

<table>
<thead>
<tr>
<th>URL</th>
<th>Text</th>
<th>Network Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.flash">http://www.flash</a> fame.com/preach/2g9ko771vxf0cu/viyljI7zveyria4vflf4f1/1/13909</td>
<td>WHOIS, TRACEROUTE, DIG, GEOP</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.flash">http://www.flash</a> fame.com/inverters/0/2g9ko771vxf0cu/viyljI7zveyria4vflf4f1</td>
<td>WHOIS, TRACEROUTE, DIG, GEOP</td>
<td></td>
</tr>
</tbody>
</table>

Viewing a File

File Name: phpisngmail_confrirmpassemail
Date of Submission: 2009-03-13
Time of Submission: 20:42:25

View Report on URL's found

Back

City: Dnepropetrovsk
Region: 04
Country: Ukraine
Zipcode: null
Latitude: 0.0
Longitude: 0.0
Area Code: 0
### Report on URLs

#### Viewing Report for URLs Found

<table>
<thead>
<tr>
<th>URL</th>
<th>Text</th>
<th>Network Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.flashfame.com/preach/2g9ko77lvxf0cuuyj7zveyrla4vf4f1/1/13909">http://www.flashfame.com/preach/2g9ko77lvxf0cuuyj7zveyrla4vf4f1/1/13909</a></td>
<td></td>
<td>WHOIS TRACEROUTE DIG GEOIP</td>
</tr>
<tr>
<td><a href="http://www.flashfame.com/inventers/029gko77lvxf0cuuyj7zveyrla4vf4f1">http://www.flashfame.com/inventers/029gko77lvxf0cuuyj7zveyrla4vf4f1</a></td>
<td></td>
<td>WHOIS TRACEROUTE DIG GEOIP</td>
</tr>
</tbody>
</table>

---

**Select a Case**

- HARSHA_PHI

**Viewing a File**

- **File Name:** phialemail_confirmplease.eml
- **Date of Submission:** 2009-03-13
- **Time of Submission:** 20:42:25

**View Report**

- View Report on URL's found

---

- **Domain Name:** FLASHFAME.COM
- **Registrar** [1440138]:
  - Host: Master_admin@americandigitalalliance.com
  - American Digital Alliance
  - 18796 John J Williams HWY
  - PMB 313
  - Rehoboth Beach
  - DE
  - 19971
  - US

- **Administrative Contact** [1440138]:
  - Host: Master_admin@americandigitalalliance.com
  - American Digital Alliance
  - 18796 John J Williams HWY
  - PMB 313
  - Rehoboth Beach
  - DE
  - 19971
  - US
  - Phone: +1.164672344695

- **Billing Contact** [1440138]:
  - Host: Master_admin@americandigitalalliance.com
  - American Digital Alliance
  - 18796 John J Williams HWY
  - PMB 313
  - Rehoboth Beach
  - DE
  - 19971
<table>
<thead>
<tr>
<th>Source</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return-Path</td>
<td><a href="mailto:ajdutpvixuphlskqys@flashfame.com">ajdutpvixuphlskqys@flashfame.com</a></td>
</tr>
<tr>
<td>From</td>
<td><a href="mailto:StimulusCheck@SelfBusinessConcepts.com">StimulusCheck@SelfBusinessConcepts.com</a></td>
</tr>
<tr>
<td>Reply-to</td>
<td><a href="mailto:rft.ajdutpvixuphlskqys@flashfame.com">rft.ajdutpvixuphlskqys@flashfame.com</a></td>
</tr>
<tr>
<td>To</td>
<td><a href="mailto:mynameisriharsha@gmail.com">mynameisriharsha@gmail.com</a></td>
</tr>
</tbody>
</table>

FileName: phishingmail_confirmplease.eml
Date of Submission: 2009-03-13
Time of Submission: 20:42:25
Report on Email Addresses

Email Reports

In this section, you can view different reports, that we have generated. Select a case, and a file to view different types of reports.

Viewing Report for Email Addresses

<table>
<thead>
<tr>
<th>Source</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return-Path</td>
<td><a href="mailto:ajdutpvxuphlskfqys@flashfame.com">ajdutpvxuphlskfqys@flashfame.com</a></td>
</tr>
<tr>
<td>From</td>
<td><a href="mailto:StimulusCheck@SoftBusinessConcepts.com">StimulusCheck@SoftBusinessConcepts.com</a></td>
</tr>
<tr>
<td>Reply-to</td>
<td><a href="mailto:rft.ajdutpvxuphlskfqys@flashfame.com">rft.ajdutpvxuphlskfqys@flashfame.com</a></td>
</tr>
<tr>
<td>To</td>
<td><a href="mailto:mynameissrirehsa@gmail.com">mynameissrirehsa@gmail.com</a></td>
</tr>
</tbody>
</table>

WHOIS is a query/response protocol which is widely used for querying an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet.

Domain Name: FLASHFAME.COM

Registrant [1440138]:
- Host: Master admin@americandigialliance.com
  - American Digital Alliance
  - 18766 John J Williams HWY
  - PMB 313
  - Rehoboth Beach
  - DE
  - 19971
  - US

Administrative Contact [1440138]:
- Host: Master admin@americandigialliance.com
  - American Digital Alliance
  - 18766 John J Williams HWY
  - PMB 313
  - Rehoboth Beach
  - DE
  - 19971
  - US
  - Phone: +1.616462244995

Billing Contact [1440138]:
- Host: Master admin@americandigialliance.com
  - American Digital Alliance
  - 18766 John J Williams HWY
  - PMB 313
  - Rehoboth Beach
  - DE
  - 19971
  - US
Account Management Tools

The Account Manager offers several features for managing your user account:

- Change Password
- Edit Directory Information
- Coming Soon
- Disable Account
- Coming Soon

Reset Password

New password: [Enter password]

Confirm password: [Enter password again]

Submit

Caution

Several settings in the Windows Active Directory can affect the success or failure of a password change. Such as: password history, maximum password age, minimum password age, minimum password length, complexity requirements.

When changing these settings remember to issue the command gpupdate in order to propagate the changes.
UnMask- Account Tools

Administrative Management Tools

The Administrative Manager offers several features for managing user accounts:

- Change Users Password
- Create New User
- Disable Accounts
- Add Web Service Location

Add New Services

Location Name:

Domain Name:

Port:

SSL: ON

Add Web Service

Caution

Several settings in the Windows Active Directory can affect the success or failure of a password change. Such as: password history, maximum password age, minimum password age, minimum password length, complexity requirements.

When changing these settings remember to issue the command gpupdate in order to propagate the changes.
### Domain names found in the database

<table>
<thead>
<tr>
<th>Domain</th>
<th>Source</th>
<th>Time of upload</th>
<th>Related Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmail.com</td>
<td></td>
<td>2009-07-08 16:25:42</td>
<td>db_gui_show_dig, db_gui_show_traceroute, db_gui_show_whos, db_gui_show_email, db_gui_show_geoip</td>
</tr>
<tr>
<td>hotmail.com</td>
<td></td>
<td>2009-07-08 16:25:42</td>
<td>db_gui_show_dig, db_gui_show_traceroute, db_gui_show_whos, db_gui_show_email, db_gui_show_geoip</td>
</tr>
</tbody>
</table>

### URLs found in the database

<table>
<thead>
<tr>
<th>URL</th>
<th>Display Text</th>
<th>Source</th>
<th>Time of upload</th>
<th>Related Data</th>
</tr>
</thead>
</table>
UnMask- Web Interface

- Ajax driven for seamless experience
- Efficient Streaming technology for faster processing
- UnMask follows good security and software design paradigms.
- UnMask uses Kerberos and LDAP for authentication and authorization.
- UnMask stores all of its forensic data in the UnMask Database.
UnMask- Web Interface

• UnMask Web Services:
  • On-demand tools
  • Information sharing architecture
  • Remote querying of servers and services (e.g. FDLE, FBI or AT&T, Comcast etc)
  • Runs on Glassfish Server

• UnMask Database GUI
  • Abstraction of SQL
  • Better Co-relational analysis

• Fully functional administrative interface and account tools

• Runs on Apache Tomcat 5.5/6
UnMask Database

• Raw emails are streamed directly from end-user into UnMask Database.

• Parses the raw emails into
  • Received Headers
  • Email addresses
  • URL’s

• Calls the UnMask Tool Server for getting network based results
  • Whois
  • Dig
  • Traceroute
  • GEOIP
UnMask Database

• Authenticates all users using LDAP over SSL
• Follows a least privilege policy model
• Contains a personal storage unit
  • Web Services results are stored
  • Database correlation analysis results are stored
• Runs on Postgresql 8.4
Legend for triggers
1. trg_email
2. trg_email_address
3. trg_uri_whois
4. trg_uri_dig_any
5. trg_uri_traceroute
6. trg_uri_country
UnMask Tool Server

- Listens to commands from UnMask Database
- Conforms to the UUTC protocol
- Runs the following Unix Based tools
  - Whois
  - DIG
  - Traceroute
  - GEOIP
Email Analysis using UnMask

- A little about our email data
  - Real phishing conversations with phishers
  - Engage a phisher in a conversation by making him/her believe that we are a naïve user.

- Classification of Emails
  - First Contact: Email that was sent as part of a phishing campaign
  - Secondary Response: Email that was received from the phisher after a response had been sent to the first contact email.
Set of Phishing Emails

Select a Case

Select a File

- oCSO@yahoo.eml
- oCSO@yahoo_2.eml
- oCSO@yahoo_3.eml
- oCSO@yahoo_4.eml

Query for Additional Information
I am delighted to inform you that the Guarantee Trust Bank Plc (GTB) Management through the office of Mr. President have decided to call back all approved fund payment through offshore payment center following directives from UNITED NATIONS temp: WORLD BANK and have concluded arrangements to pay your beneficiary/contractual fund by cash through Diplomatic Agent. The Agent will be delivering the cash in a Machine sealed consignment to your door step as my bank have temporarily stopped further payment via wire transfer this quarter. Diplomatic. In this regard, we are going to send your inheritance/contractual part-payment of USD10.5Million only to you via our accredited Diplomatic Agent shipping company and we have secured every needed document to cover the delivery of the money. Note: The money is coming to you on 2 security proof boxes. The boxes are &lt;DIV&gt;

sealed with synthetic nylon seal and padded with machine. The boxes are coming with a Diplomatic agent who will accompany the boxes to your house address. All you need to do now is to reconfirm to me, the following:&lt;/DIV&gt;

&lt;DIV&gt;
1) Full Name&lt;/DIV&gt;
&lt;DIV&gt;
2) Full house address&lt;/DIV&gt;
&lt;DIV&gt;
3) Your mobile phone&lt;/DIV&gt;
&lt;DIV&gt;
4) Any form of identification. The Diplomat attached will travel with it. He will call you immediately he arrives your country's airport.&lt;/DIV&gt;
&lt;DIV&gt;
First Contact Email

Received Headers

have generated. Select a case, and a file to view different types of reports

Received: from mky-mail.ecoil.com.cn (211.144.100.138) by mx.google.com
Received: from User (41.217.85.13) by mky-mail.ecoil.com.cn
First External Mail Server: from mky-mail.ecoil.com.cn (211.144.100.138) by mx.google.com

Select a Case

sir oelle_chikelu

Viewing a File

FileName: oCSO@yahoo.eml
Date of Submission: 2010-07-28
Time of Submission: 15:13:48
Back
Query for Additional Information
Lookup Saved Information

View Report

View Report on Received Header

------------------------------------------
GEO IP/COUNTRY RESULT: 211.144.100.138---------------

City: Shanghai
Region: 23
Country: China
Zipcode: null
Latitude: 0.0
Longitude: 0.0
Area Code: 0
### Received Headers

<table>
<thead>
<tr>
<th>Received: from</th>
<th>76.13.13.25</th>
<th>67.186.8.83</th>
<th>67.186.8.101</th>
<th>127.0.0.1</th>
<th>41.217.66.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>byn1.bullet.mail.ac4.yahoo.com</td>
<td>byt4.bullet.mail.ac4.yahoo.com</td>
<td>byt3.bullet.mail.gg1.yahoo.com</td>
<td>byomp105.mail.gg1.yahoo.com</td>
<td>byweb114203.mail.gg1.yahoo.com</td>
<td></td>
</tr>
</tbody>
</table>

First External Mail Server: from n1a.bullet.mail.ac4.yahoo.com (n1a.bullet.mail.ac4.yahoo.com[76.13.13.64]) bymx.google.com

---

**Geo IP/Country Result**: 76.13.13.64

- **City**: Sunnyvale
- **Region**: CA
- **Country**: United States
- **Zipcode**: 94089
- **Latitude**: 0.0
- **Longitude**: 0.0
- **Area Code**: 608
Some Experimental Properties of these Phishing Emails

- **First Contact (FC):**
  - “From” address is not responsive
  - “Reply-to” address is alive
  - First external mail server is suspicious
    - E.g. Content claims email is from Nigeria, first external mail server is from Eastern European country or Asian country.
    - Using taken down quickly and not pingable

- **Secondary Response (SR):**
  - “Reply-to” and “From” addresses are same and alive
  - First external mail server usually from trackable source.
  - First external mail server of all SR’s in a related case come from same country.
UnMask

• One of a kind application for analyzing emails.

• Provides a secure environment for law enforcement agents to analyze cases of emails.

• Gathers and stores all the forensic data within minutes.

• Has been recently experimentally deployed at National White Collar Crime Center (NW3C).
UnMask-Future Work

• Email Attachments analysis

• Desktop version for smaller law-enforcement offices

• Release of UnMask 3.0
Questions?

Sudhir Aggarwal
Department of Computer Science
E-Crime Investigative Technologies Laboratory
Florida State University
Tallahassee, Florida 32306-4530
sudhir@cs.fsu.edu