Social Network Phishing

BSidesSATX 21 May 2016

Will Woodson, @wjwoodson, sec@williamwoodson.com

Who am I?

“Will is an Information Security Analyst at a large financial services institution in San Antonio. He has several years of professional experience in security operations and is currently pursuing a graduate degree in cyber security from UTSA.”

What am I talking about?

- Social Networks/Graphs
- Social Engineering/Phishing
- Browser Exploitation
- Multiple routes to Game Over

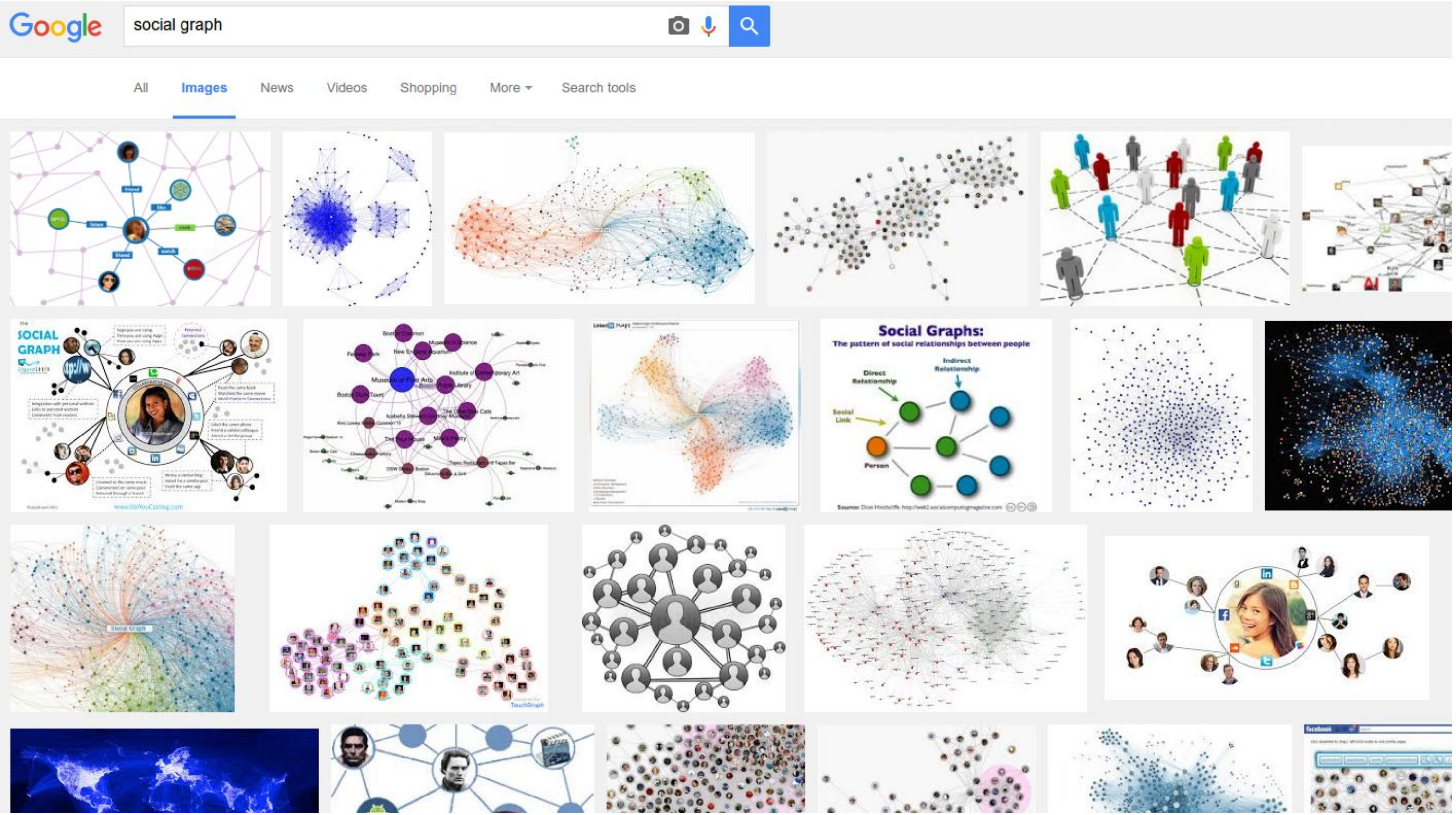
Social Networks

- Social Network
  - “a network of social interactions and personal relationships”
  - A social structure represented as a graph with Individuals as **nodes**, Relationships as **edges.**
  - **Facebook**

- Social Graphs
  - **Nodes** - Individuals, Organizations
    - & places, likes, etc.
  - **Edges** - Relationships, Interactions
  - ***Fields** - Information about nodes. Names, birthdays, etc.

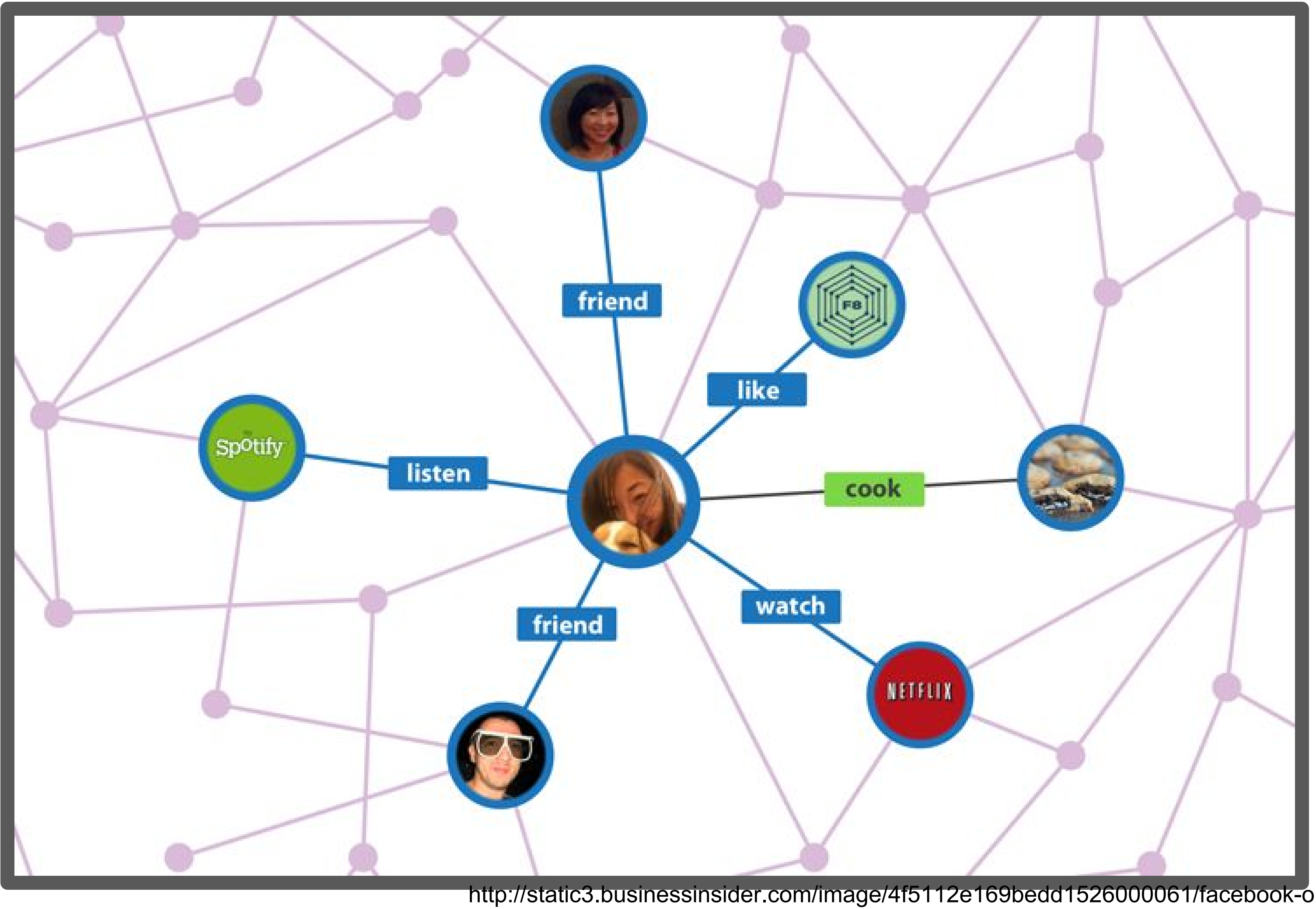
*https://developers.facebook.com/docs/graph-api/overview

Social Graphs



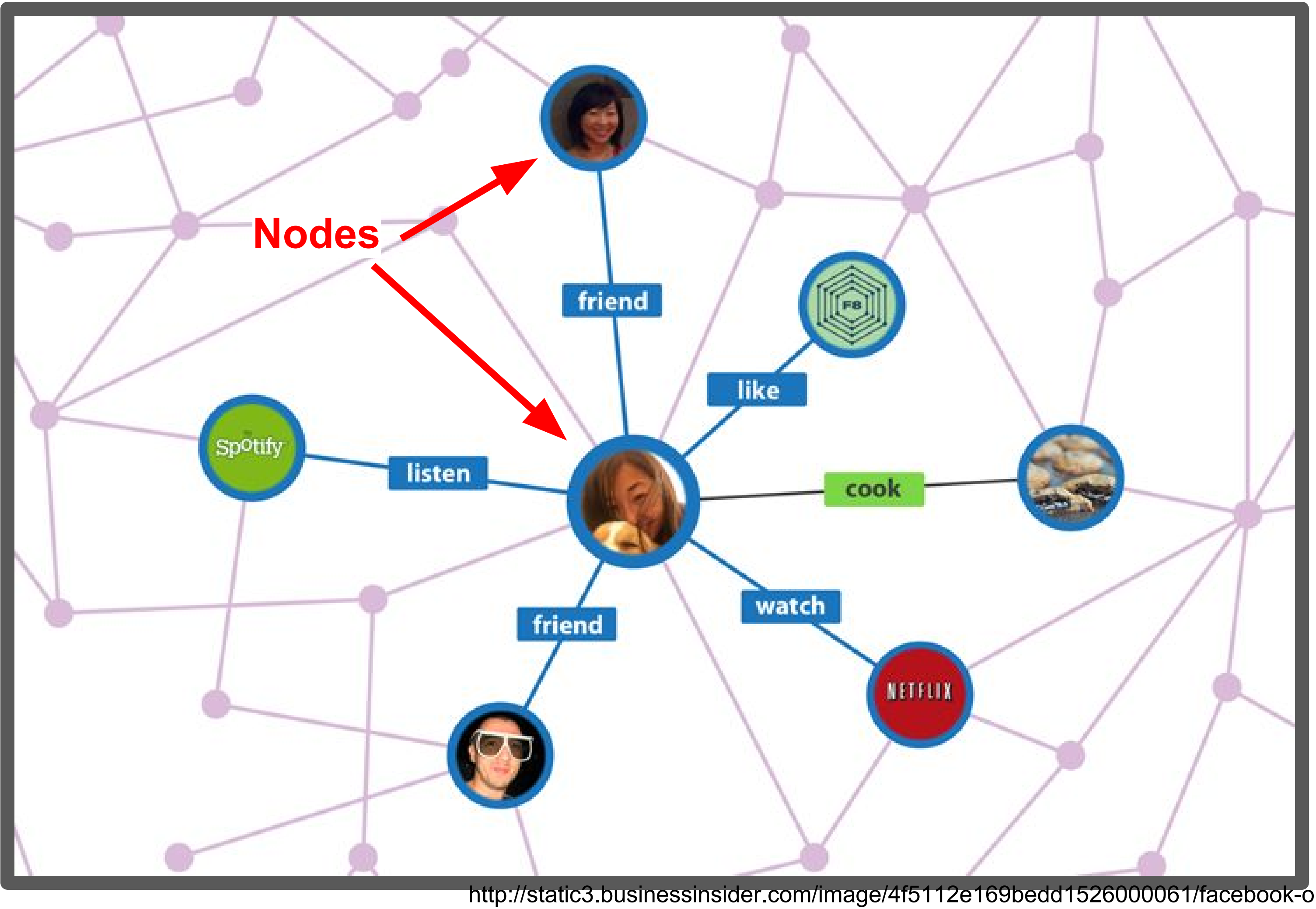
social graph

Soc



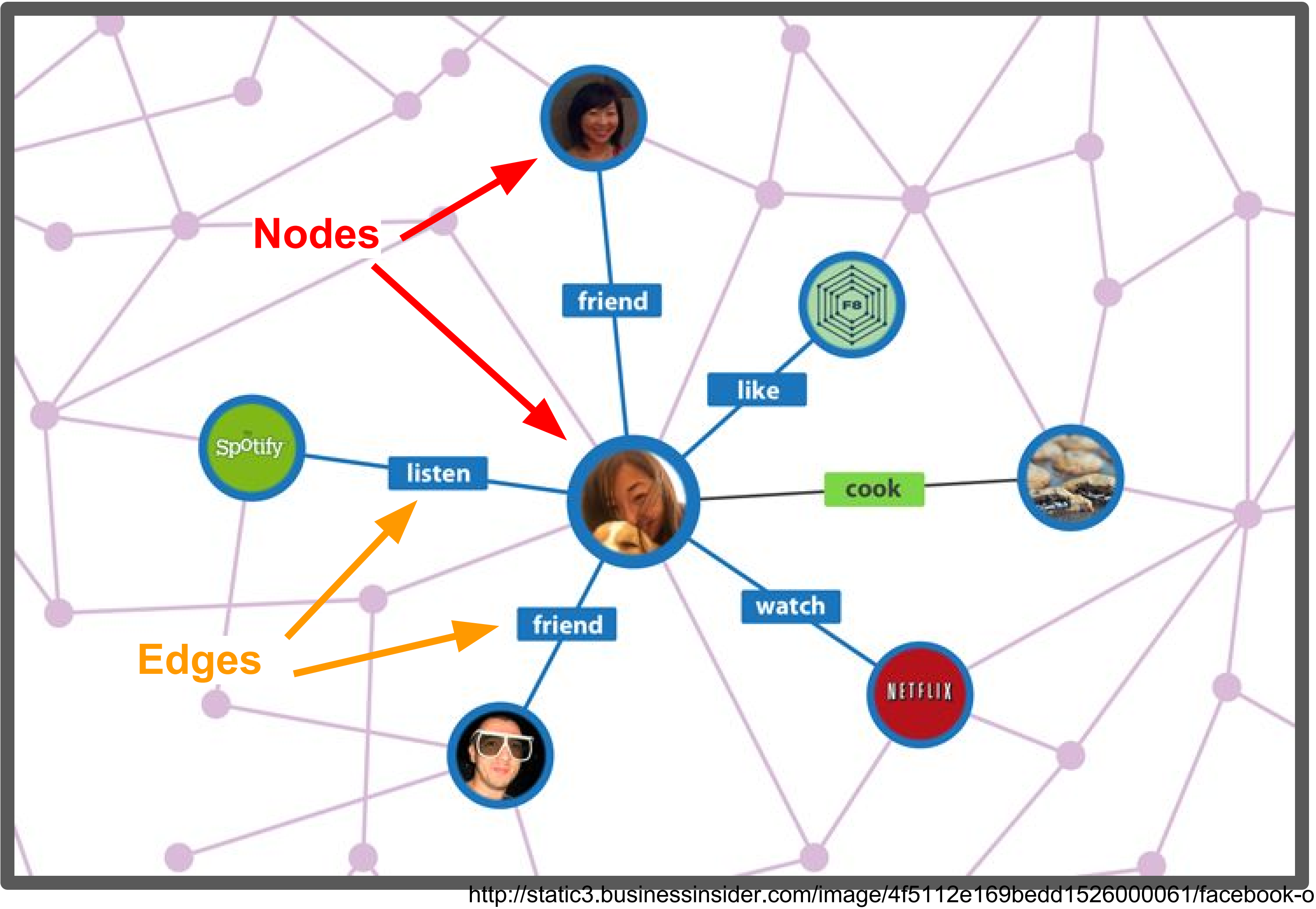
http://static3.businessinsider.com/image/4f5112e169bedd1526000061/facebook-open-graph.jpg

Soc



http://static3.businessinsider.com/image/4f5112e169bedd1526000061/facebook-open-graph.jpg

Soc



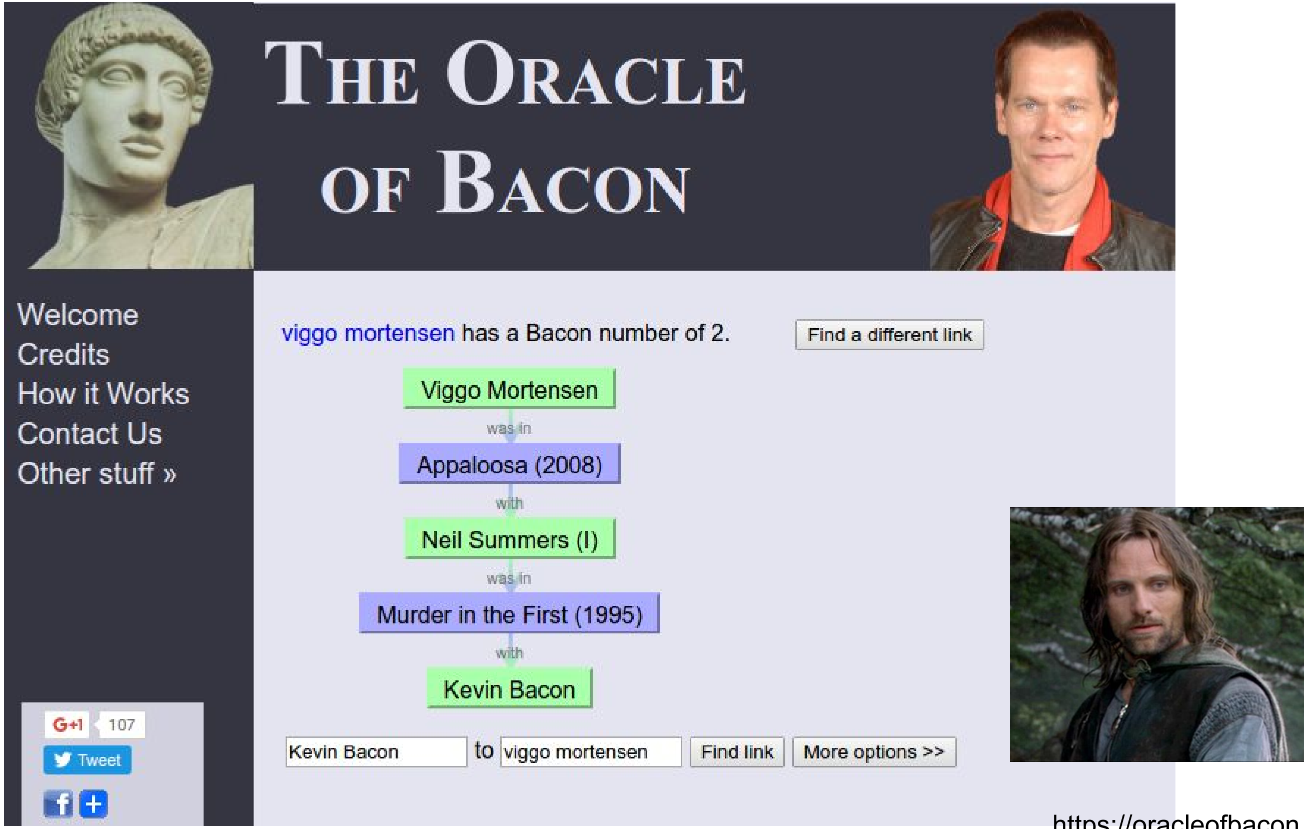
http://static3.businessinsider.com/image/4f5112e169bedd1526000061/facebook-open-graph.jpg

Social Graph Queries

- Who listens to Spotify?
- Who is friends with X?
- What do people who are friends with X listen to?

Very powerful for marketing, useful to us later. But first, bacon.

(Kevin) Bacon Graph



THE ORACLE OF BACON

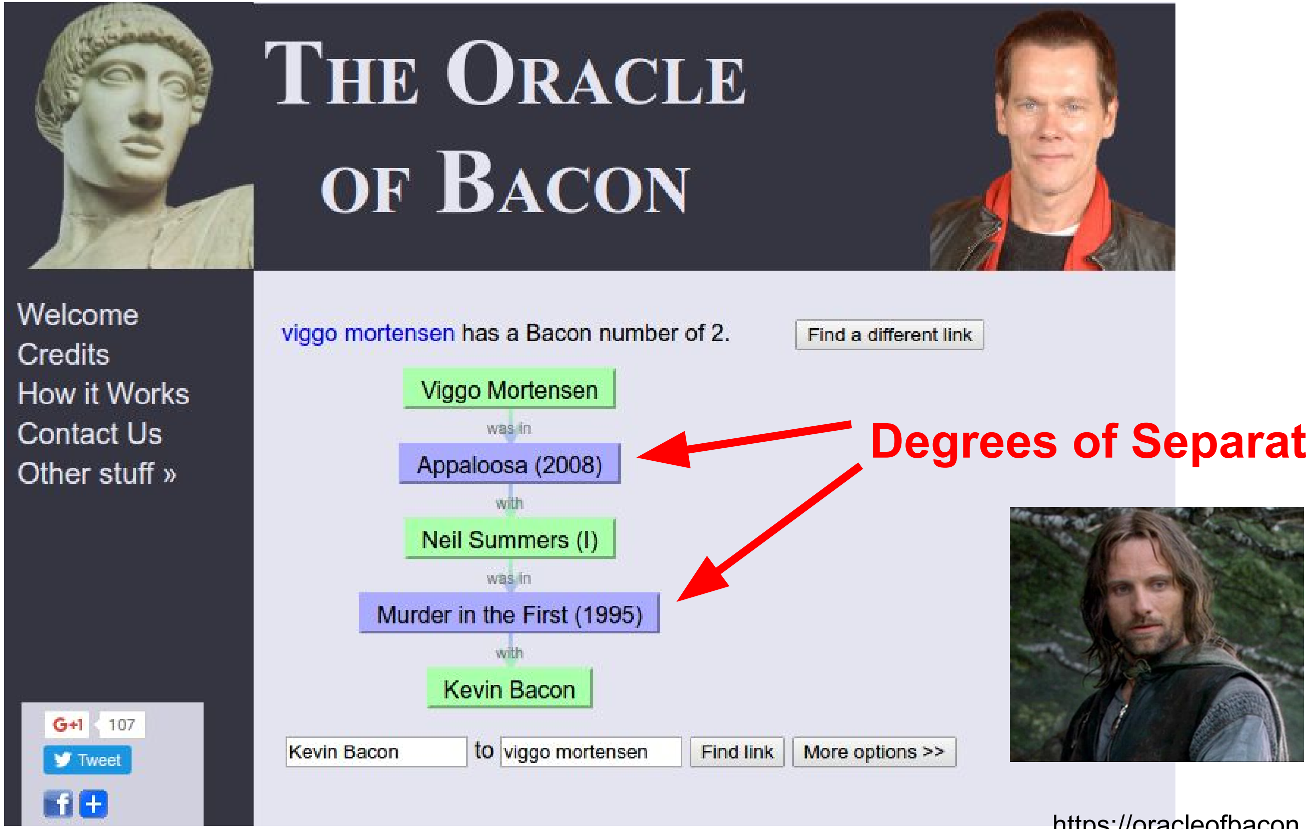
viggo mortensen has a Bacon number of 2.

Viggo Mortensen
was in
Appaloosa (2008)
with
Neil Summers (I)
was in
Murder in the First (1995)
with
Kevin Bacon

Kevin Bacon to viggo mortensen

https://oracleofbacon.org/movielinks.php

(Kevin) Bacon Graph



viggo mortensen has a Bacon number of 2.

Viggo Mortensen

was in

Appaloosa (2008)

with

Neil Summers (I)

was in

Murder in the First (1995)

with

Kevin Bacon

Kevin Bacon to viggo mortensen

Degrees of Separation (2)

https://oracleofbacon.org/movielinks.php

Tools: Maltego

Paterva
A new train of thought

Maltego CE

Maltego CE is used by security professionals worldwide and ships with Linux Kali out-the-box.

What is Maltego?

Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.

Maltego uses the idea of transforms to automate the

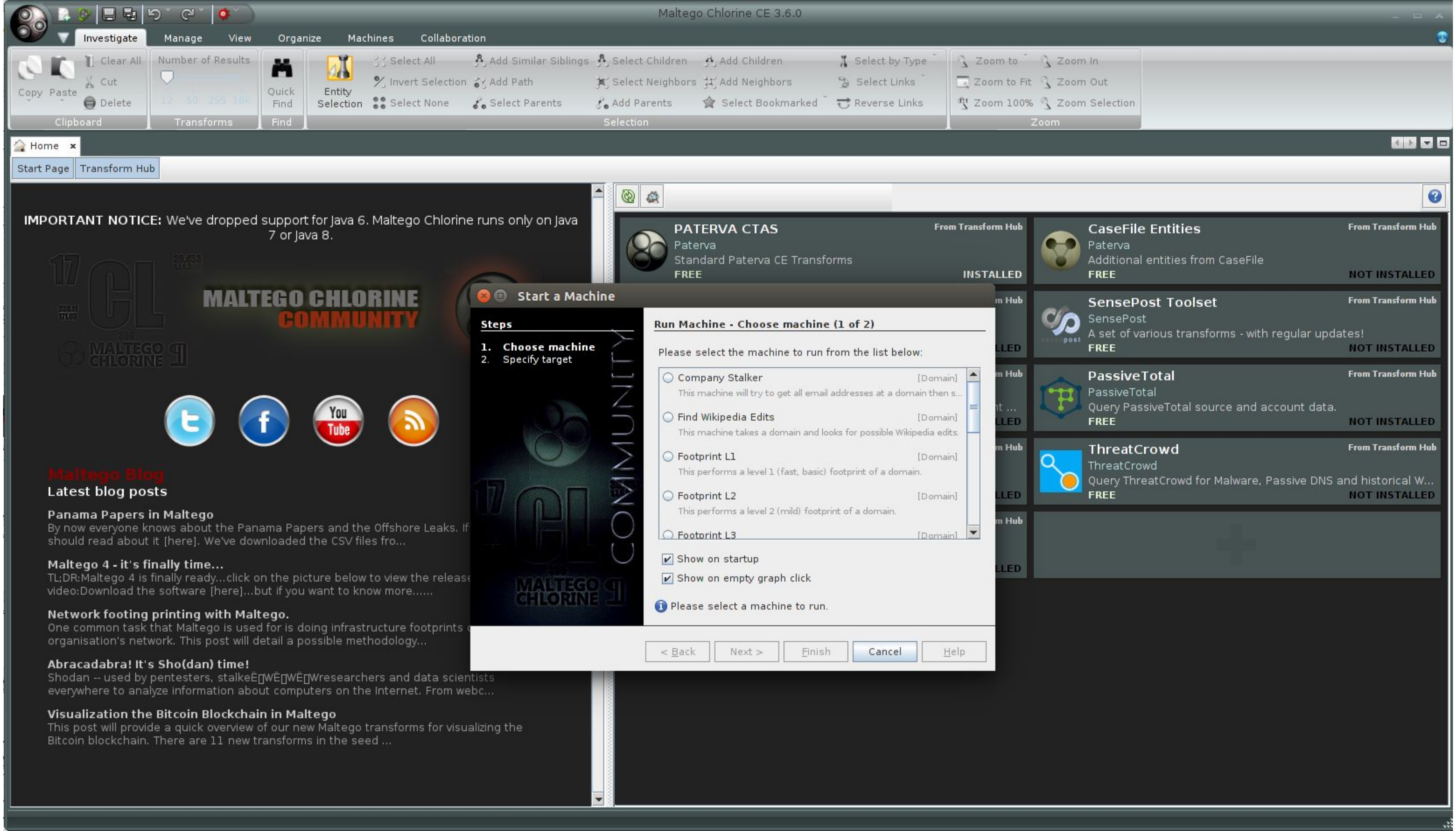
https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

Tools: Maltego

“The focus of Maltego is analyzing real-world relationships between information that is publically accessible on the Internet. This includes footprinting Internet infrastructure as well as gathering information about the people and organisation who own it.”

Maltego can be used to determine the relationships between the following entities:

- People
- Names
- Email addresses
- Aliases
- Groups of people (social networks)
- Companies
- Organizations….



IMPORTANT NOTICE: We've dropped support for Java 6. Maltego Chlorine runs only on Java 7 or Java 8.

Maltego Blog

Latest blog posts

Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If
should read about it [here]. We've downloaded the CSV files fro...

Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release
video:Download the software [here]...but if you want to know more......

Network footing printing with Maltego.
One common task that Maltego is used for is doing infrastructure footprints
organisation's network. This post will detail a possible methodology...

Abracadabra! It's Sho(dan) time!
Shodan -- used by pentesters, stalkeË▯WË▯WË▯Wresearchers and data scientists
everywhere to analyze information about computers on the Internet. From webc...

Visualization the Bitcoin Blockchain in Maltego
This post will provide a quick overview of our new Maltego transforms for visualizing the
Bitcoin blockchain. There are 11 new transforms in the seed ...

Start a Machine

Steps

1. **Choose machine**
2. Specify target

Run Machine - Choose machine (1 of 2)

Please select the machine to run from the list below:

○ Company Stalker [Domain]
This machine will try to get all email addresses at a domain then s...

○ Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.

○ Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.

○ Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.

○ Footprint L3 [Domain]

☑ Show on startup

☑ Show on empty graph click

Please select a machine to run.

< Back | Next > | Finish | Cancel | Help

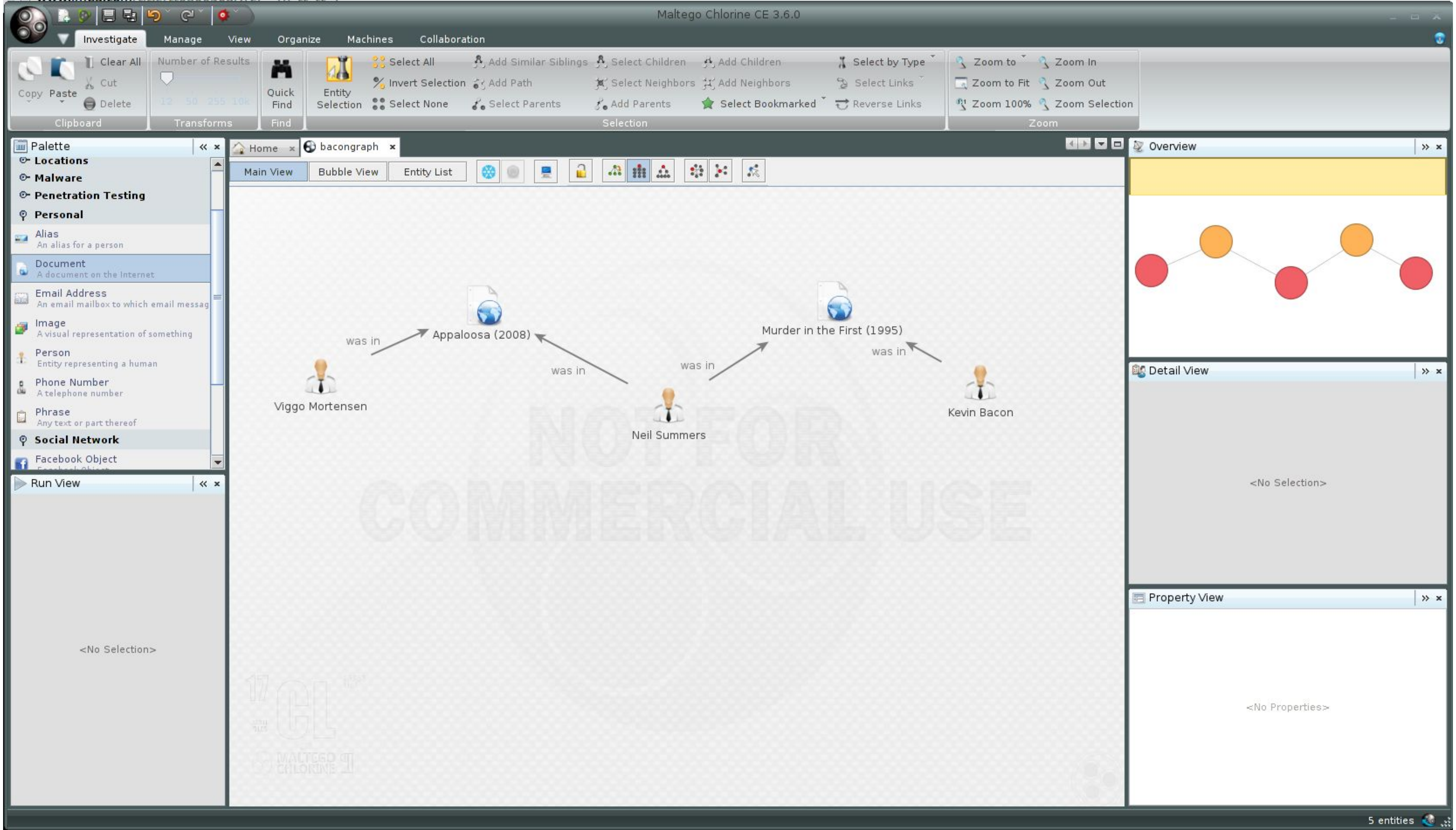
PATERVA CTAS From Transform Hub
Paterva
Standard Paterva CE Transforms
FREE INSTALLED

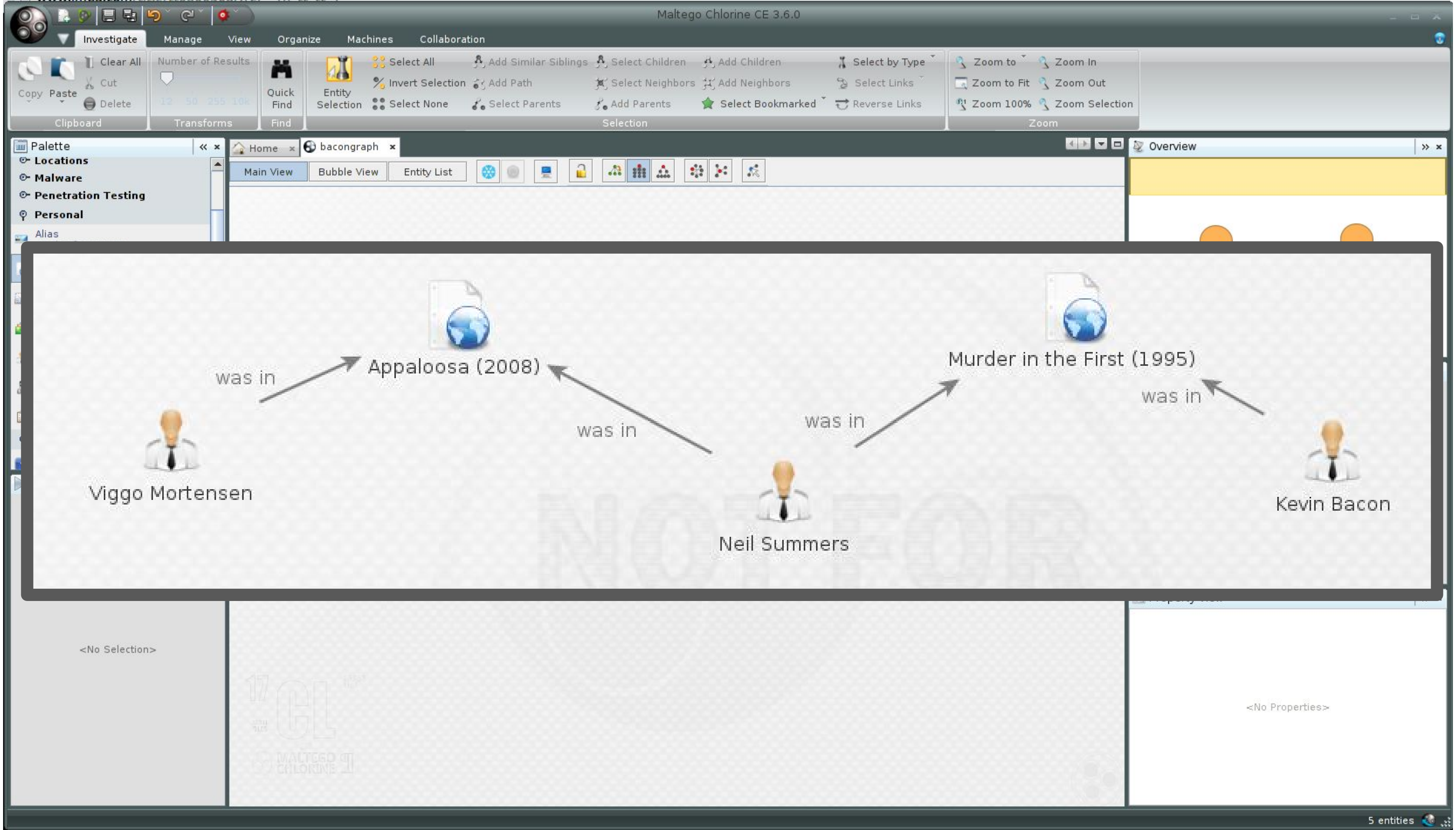
CaseFile Entities From Transform Hub
Paterva
Additional entities from CaseFile
FREE NOT INSTALLED

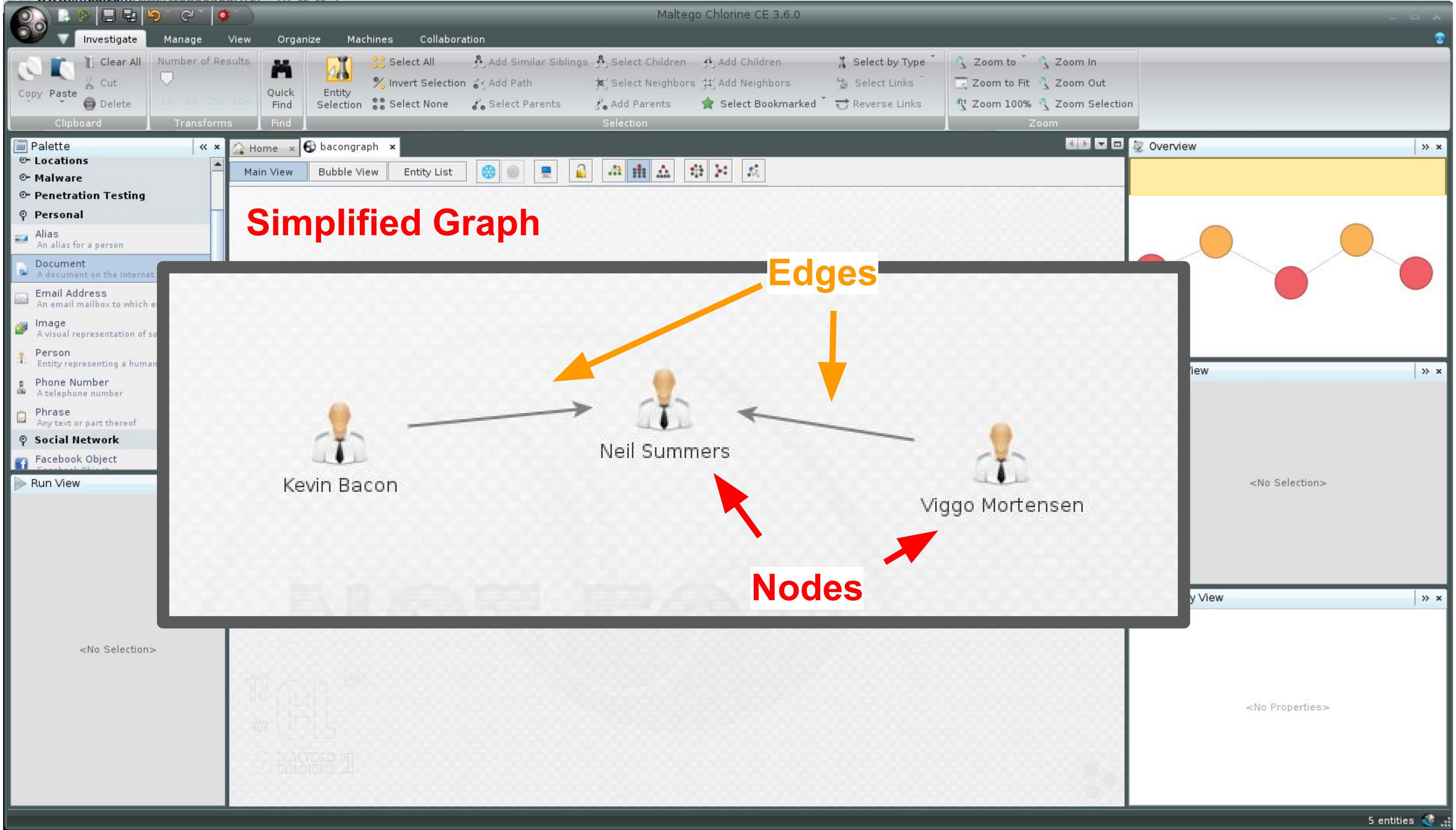
SensePost Toolset From Transform Hub
SensePost
A set of various transforms - with regular updates!
FREE NOT INSTALLED

PassiveTotal From Transform Hub
PassiveTotal
Query PassiveTotal source and account data.
FREE NOT INSTALLED

ThreatCrowd From Transform Hub
ThreatCrowd
Query ThreatCrowd for Malware, Passive DNS and historical W...
FREE NOT INSTALLED

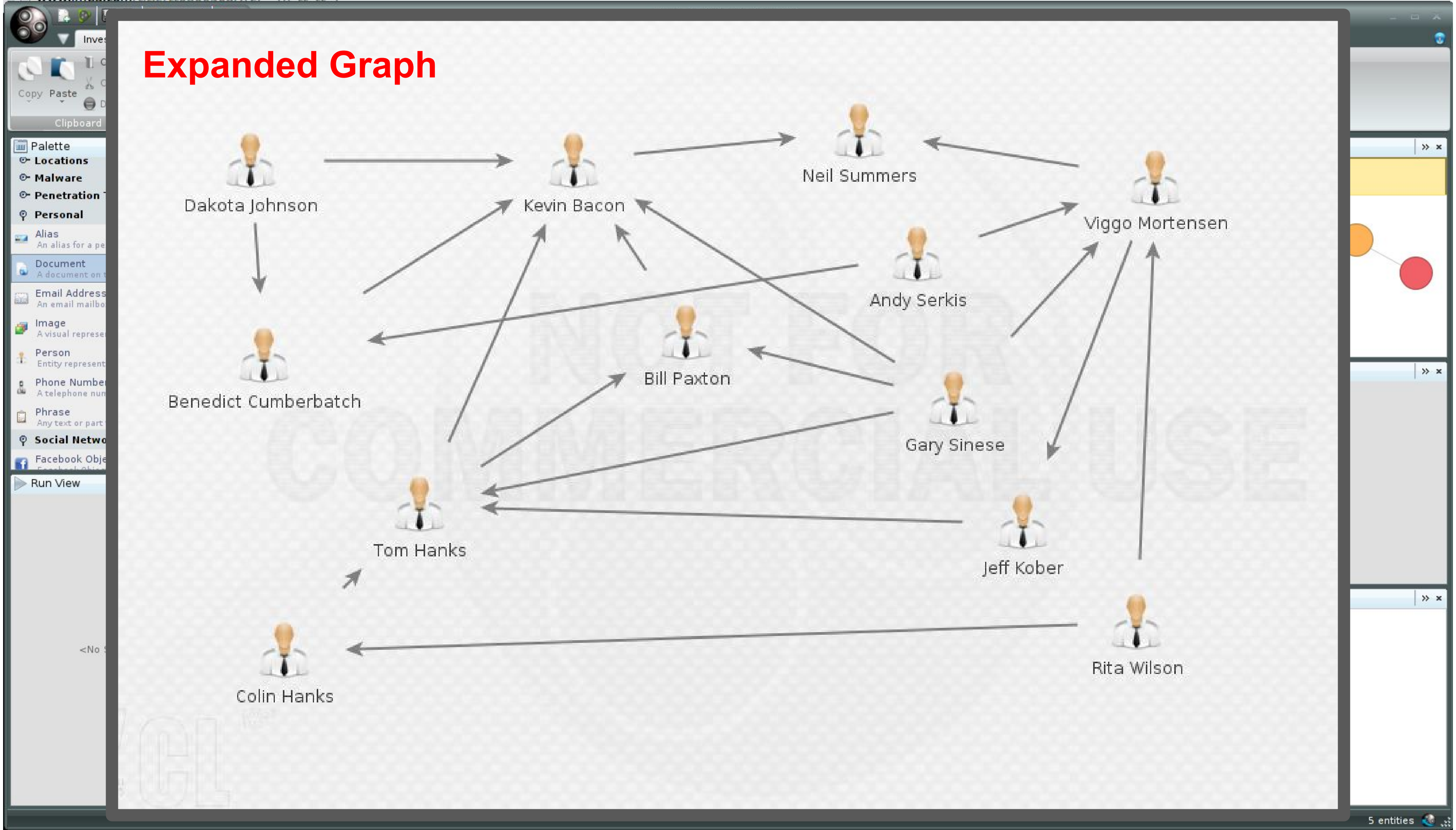

Maltego Chlorine CE 3.6.0
Investigate
Manage
View
Organize
Machines
Collaboration
Copy
Paste
Clear All
Cut
Delete
Clipboard
Number of Results
12
50
255
10k
Transforms
Quick Find
Find
Entity Selection
Select All
Invert Selection
Select None
Add Similar Siblings
Add Path
Select Parents
Select Children
Select Neighbors
Add Parents
Add Children
Add Neighbors
Select Bookmarked
Select by Type
Select Links
Reverse Links
Selection
Zoom to
Zoom to Fit
Zoom 100%
Zoom In
Zoom Out
Zoom Selection
Zoom
Palette
Locations
Malware
Penetration Testing
Personal
Alias
An alias for a person
Document
A document on the Internet
Email Address
An email mailbox to which email messag
Image
A visual representation of something
Person
Entity representing a human
Phone Number
A telephone number
Phrase
Any text or part thereof
Social Network
Facebook Object
Run View
<No Selection>
Home
bacongraph
Main View
Bubble View
Entity List
Viggo Mortensen
was in
Appaloosa (2008)
was in
Neil Summers
was in
Murder in the First (1995)
was in
Kevin Bacon
NOT FOR COMMERCIAL USE
MALTEGO CHLORINE
Overview
Detail View
<No Selection>
Property View
<No Properties>
5 entities


Maltego Chlorine CE 3.6.0
Investigate
Manage
View
Organize
Machines
Collaboration
Copy
Paste
Clear All
Cut
Delete
Clipboard
Number of Results
Transforms
Quick Find
Find
Entity Selection
Select All
Invert Selection
Select None
Add Similar Siblings
Add Path
Select Parents
Select Children
Select Neighbors
Add Parents
Add Children
Add Neighbors
Select Bookmarked
Select by Type
Select Links
Reverse Links
Selection
Zoom to
Zoom to Fit
Zoom 100%
Zoom In
Zoom Out
Zoom Selection
Zoom
Palette
Locations
Malware
Penetration Testing
Personal
Alias
Home
bacongraph
Main View
Bubble View
Entity List
Overview
Appaloosa (2008)
Murder in the First (1995)
was in
was in
was in
was in
Viggo Mortensen
Neil Summers
Kevin Bacon
<No Selection>
<No Properties>
5 entities



Simplified Graph

Expanded Graph



(Kevin) Bacon Graph

Degrees of Separation	# of People (IMDB)
0	1
1	2,769
2	305,215
3	1,021,901
4	253,177
5	20,060
6	2,033
7	297
8	25
9	7

http://blogs.ams.
org/mathgradblog/2013/11/22/degrees-kevin-
bacon/#sthash.LJt34d46.dpbs

(Kevin) Bacon Graph

Degrees of Separation	# of People (IMDB)
0	1
1	2,769
2	305,215
3	1,021,901
4	253,177
5	20,060
6	2,033
7	297
8	25
9	7

http://blogs.ams.org/mathgradblog/2013/11/22/degrees-kevin-bacon/#sthash.LJt34d46.dpbs

Social Engineering

“Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access...”

Social Engineering

- Pretext - Scenario to engage target in a manner that increases the chance they will divulge information or perform actions that would be unlikely in ordinary circumstances.
- Impersonation

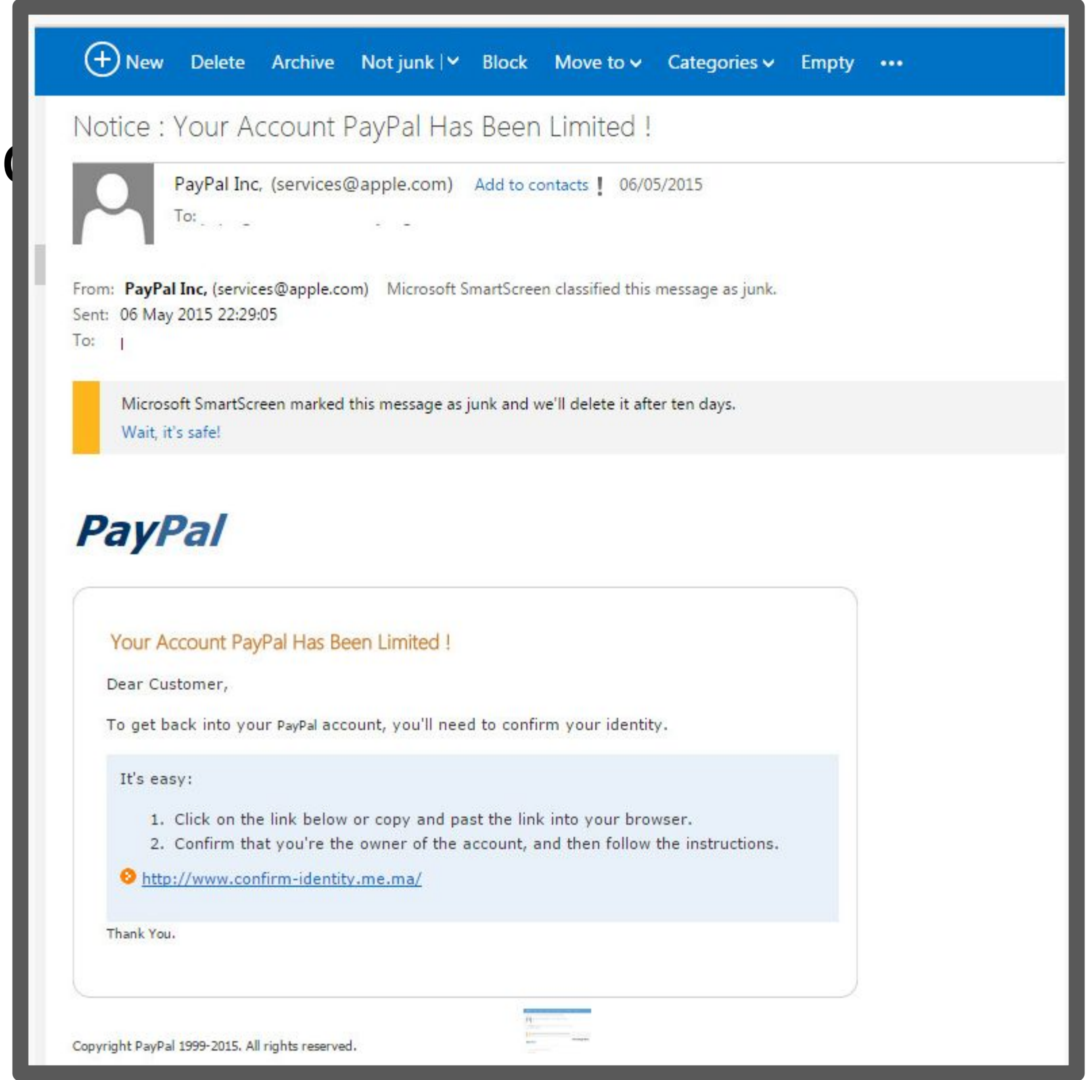
- Bait - enticement, relies on the curiosity or greed of the target.

Phishing

“Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.”

- Spear phishing

Phish - ho



Notice : Your Account PayPal Has Been Limited !

PayPal Inc, (services@apple.com) 06/05/2015

To:

From: **PayPal Inc,** (services@apple.com) Microsoft SmartScreen classified this message as junk.

Sent: 06 May 2015 22:29:05

To:

Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.

Your Account PayPal Has Been Limited !

Dear Customer,

To get back into your PayPal account, you'll need to confirm your identity.

It's easy:

1. Click on the link below or copy and past the link into your browser.
2. Confirm that you're the owner of the account, and then follow the instructions.

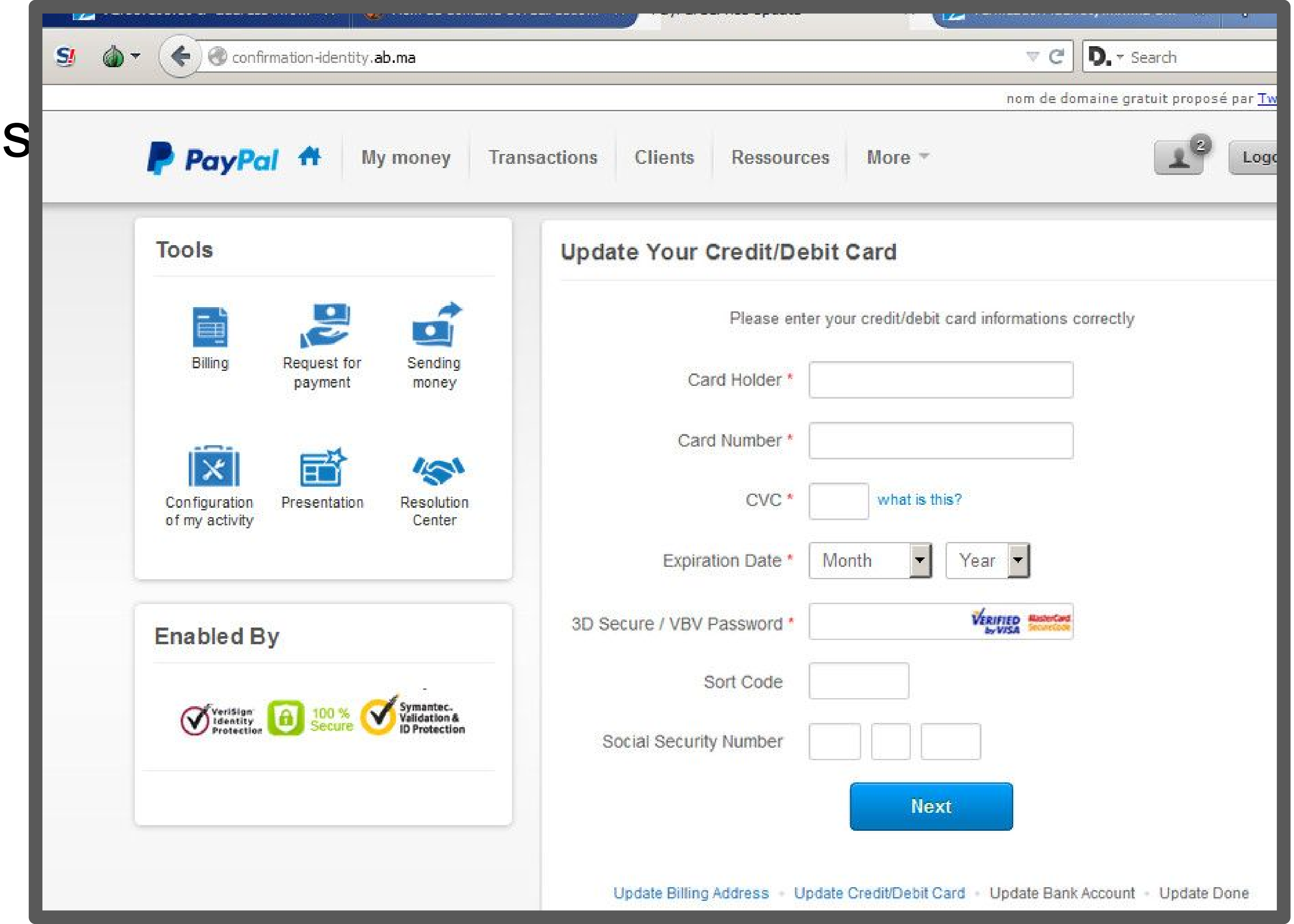
http://www.confirm-identity.me.ma/

Thank You.

Copyright PayPal 1999-2015. All rights reserved.

https://blog.malwarebytes.org/cybercrime/2015/05/your-account-paypal-has-been-limited-phishing-scam/

Phis



Tools

Enabled By

Update Your Credit/Debit Card

Please enter your credit/debit card informations correctly

Card Holder *

Card Number *

CVC * what is this?

Expiration Date * Month Year

3D Secure / VBV Password *

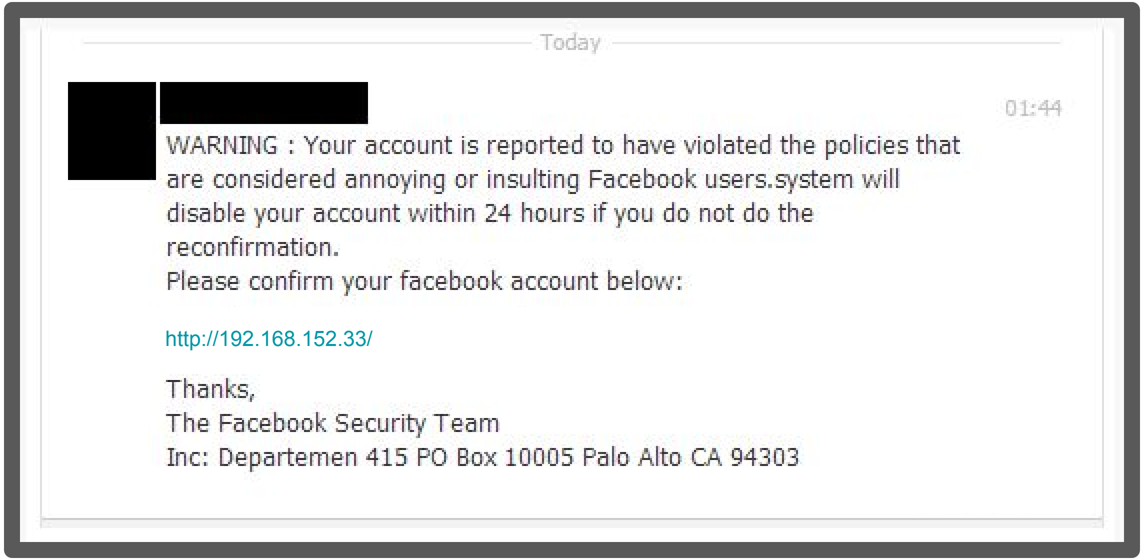
Sort Code

Social Security Number

Next

Update Billing Address · Update Credit/Debit Card · Update Bank Account · Update Done

Phish - hook



Today

[redacted] [redacted]

01:44

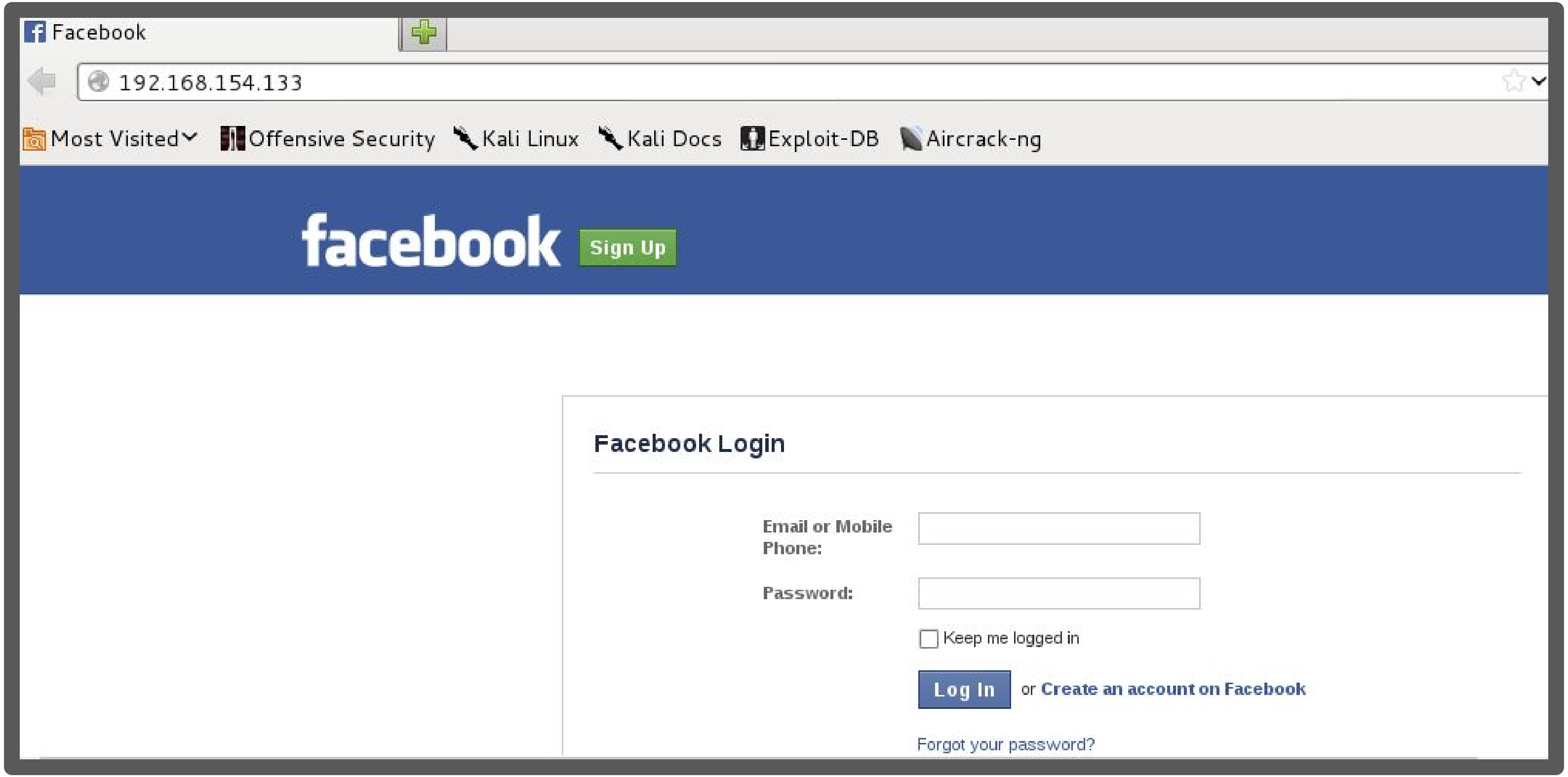
WARNING : Your account is reported to have violated the policies that are considered annoying or insulting Facebook users.system will disable your account within 24 hours if you do not do the reconfirmation.
Please confirm your facebook account below:

http://192.168.152.33/

Thanks,
The Facebook Security Team
Inc: Departemen 415 PO Box 10005 Palo Alto CA 94303

https://blog.threattrack.com/phishing-scam-spreads-via-facebook-pm/

Phish - landing



Facebook

192.168.154.133

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

facebook Sign Up

Facebook Login

Email or Mobile Phone:

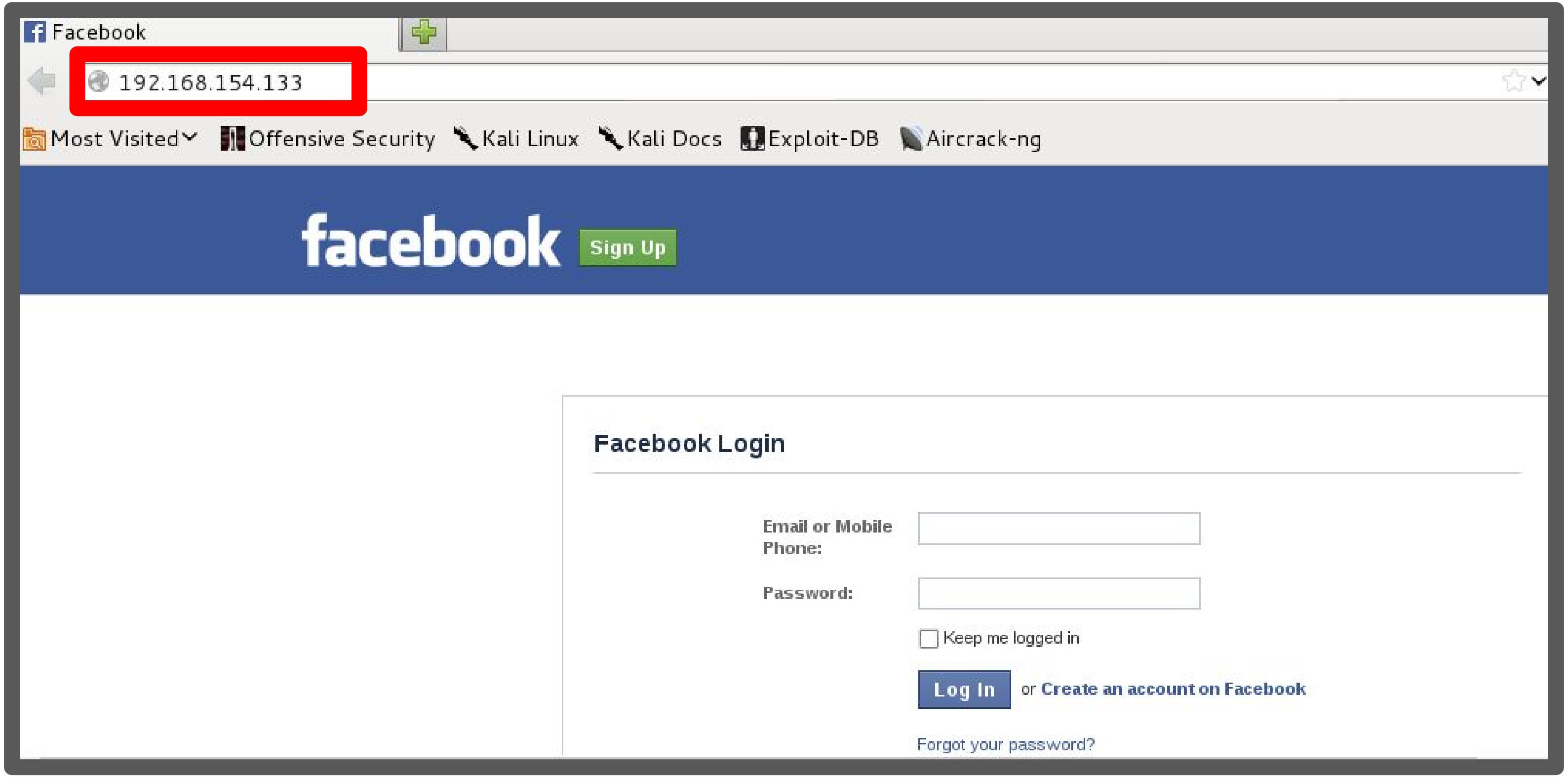
Password:

□ Keep me logged in

Log In or Create an account on Facebook

Forgot your password?

Phish - landing



Facebook Login

Email or Mobile Phone:

Password:

□ Keep me logged in

Log In or Create an account on Facebook

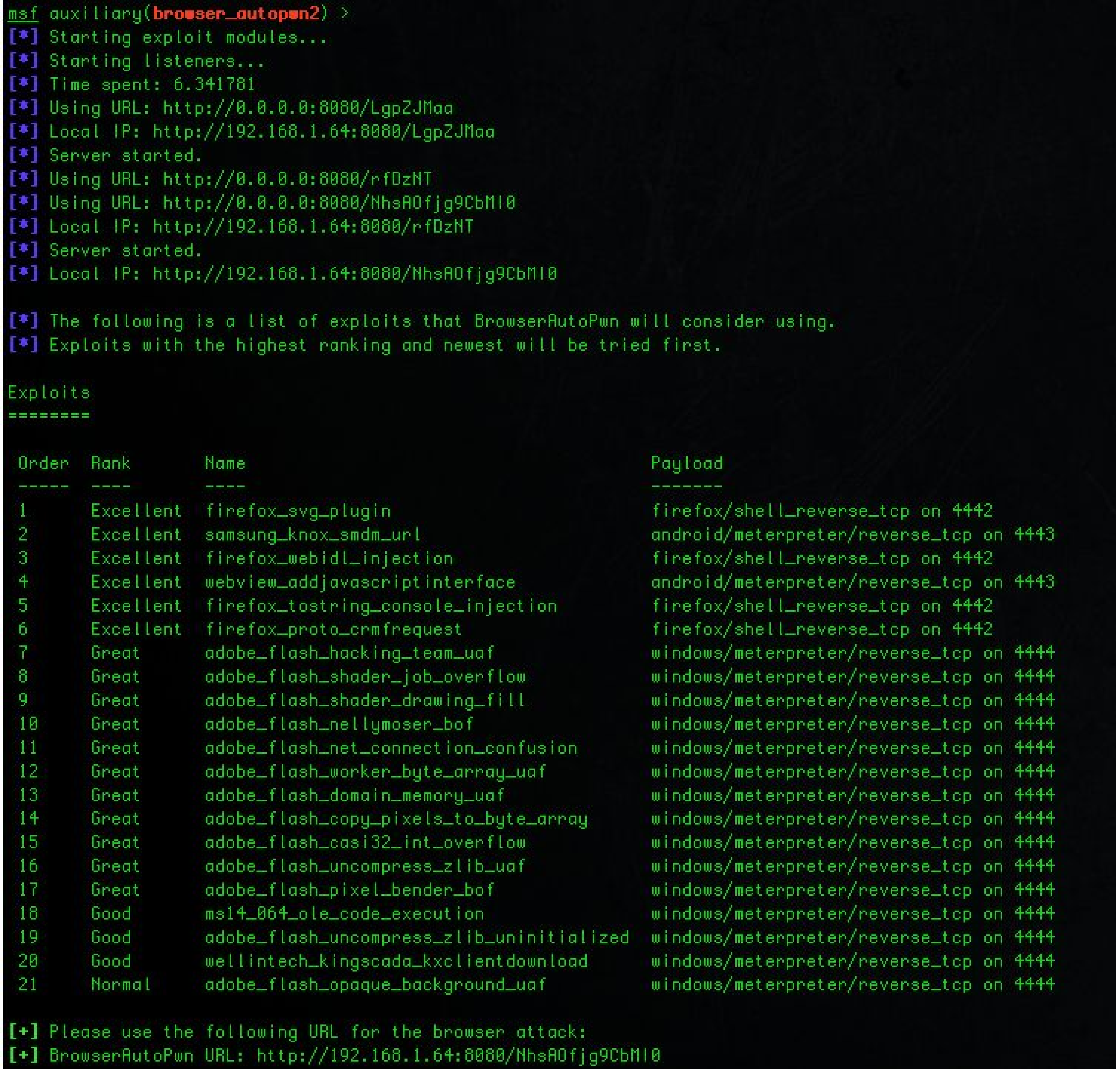
Forgot your password?

Tools: payloads

Why limit ourselves to gathering credentials?

- Metasploit BrowserAutoPwn
  - Use one of many common exploits to compromise browser/plugins
  - browser hijack
  - RAT install
- BeEF
  - credential phish
  - browser hijack
  - & much more

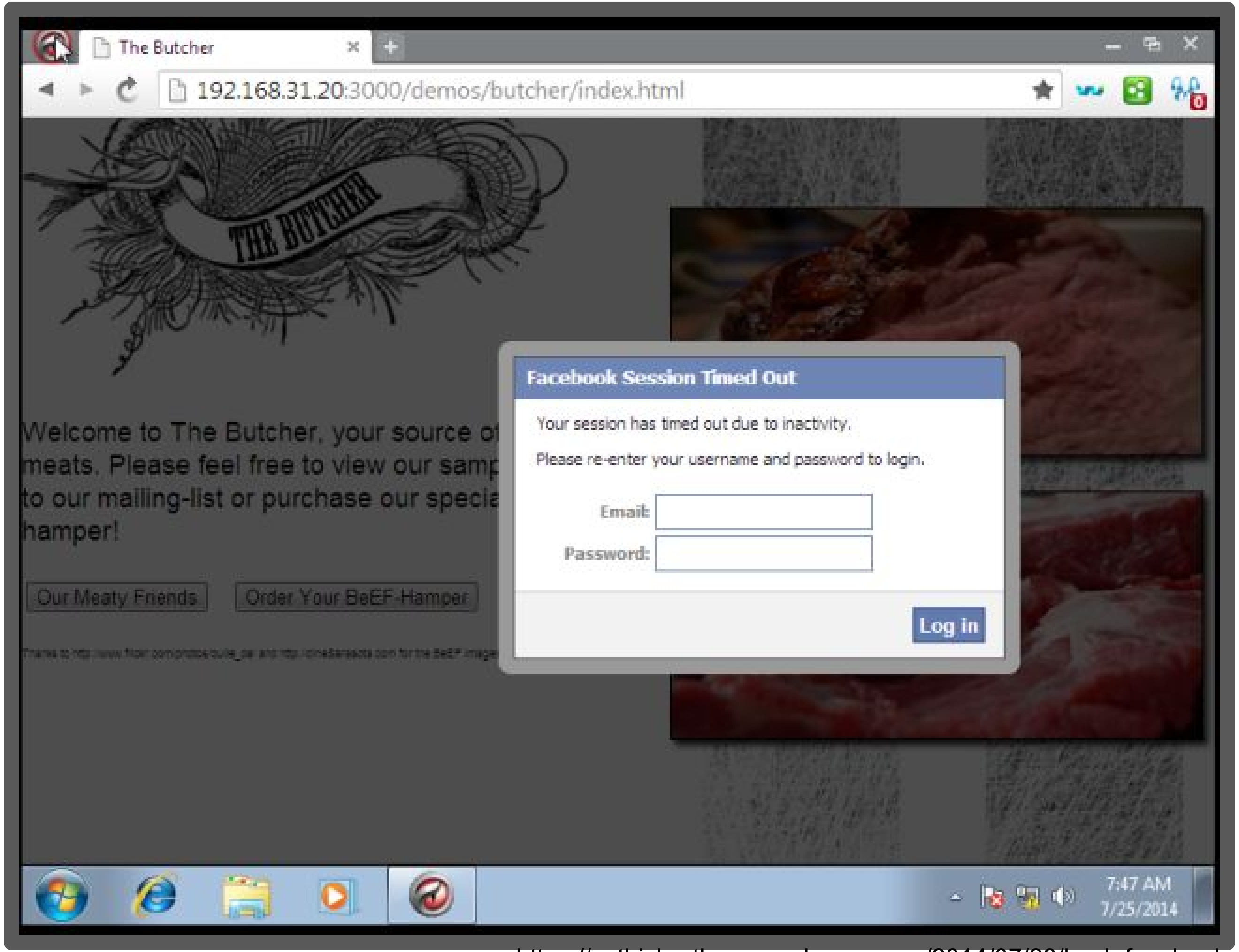
Tools: pay



```
msf auxiliary(browser_autopwn2) >
[*] Starting exploit modules...
[*] Starting listeners...
[*] Time spent: 6.341781
[*] Using URL: http://0.0.0.0:8080/LgpZJMaa
[*] Local IP: http://192.168.1.64:8080/LgpZJMaa
[*] Server started.
[*] Using URL: http://0.0.0.0:8080/rfDzNT
[*] Using URL: http://0.0.0.0:8080/NhsAOfjg9CbMI0
[*] Local IP: http://192.168.1.64:8080/rfDzNT
[*] Server started.
[*] Local IP: http://192.168.1.64:8080/NhsAOfjg9CbMI0

[*] The following is a list of exploits that BrowserAutoPwn will consider using.
[*] Exploits with the highest ranking and newest will be tried first.

Exploits
========

 Order  Rank       Name                                        Payload
 -----  ----       ----                                        -------
 1      Excellent  firefox_svg_plugin                          firefox/shell_reverse_tcp on 4442
 2      Excellent  samsung_knox_smdm_url                       android/meterpreter/reverse_tcp on 4443
 3      Excellent  firefox_webidl_injection                    firefox/shell_reverse_tcp on 4442
 4      Excellent  webview_addjavascriptinterface              android/meterpreter/reverse_tcp on 4443
 5      Excellent  firefox_tostring_console_injection          firefox/shell_reverse_tcp on 4442
 6      Excellent  firefox_proto_crmfrequest                   firefox/shell_reverse_tcp on 4442
 7      Great      adobe_flash_hacking_team_uaf                windows/meterpreter/reverse_tcp on 4444
 8      Great      adobe_flash_shader_job_overflow             windows/meterpreter/reverse_tcp on 4444
 9      Great      adobe_flash_shader_drawing_fill             windows/meterpreter/reverse_tcp on 4444
 10     Great      adobe_flash_nellymoser_bof                  windows/meterpreter/reverse_tcp on 4444
 11     Great      adobe_flash_net_connection_confusion        windows/meterpreter/reverse_tcp on 4444
 12     Great      adobe_flash_worker_byte_array_uaf           windows/meterpreter/reverse_tcp on 4444
 13     Great      adobe_flash_domain_memory_uaf               windows/meterpreter/reverse_tcp on 4444
 14     Great      adobe_flash_copy_pixels_to_byte_array       windows/meterpreter/reverse_tcp on 4444
 15     Great      adobe_flash_casi32_int_overflow             windows/meterpreter/reverse_tcp on 4444
 16     Great      adobe_flash_uncompress_zlib_uaf             windows/meterpreter/reverse_tcp on 4444
 17     Great      adobe_flash_pixel_bender_bof                windows/meterpreter/reverse_tcp on 4444
 18     Good       ms14_064_ole_code_execution                 windows/meterpreter/reverse_tcp on 4444
 19     Good       adobe_flash_uncompress_zlib_uninitialized   windows/meterpreter/reverse_tcp on 4444
 20     Good       wellintech_kingscada_kxclientdownload       windows/meterpreter/reverse_tcp on 4444
 21     Normal     adobe_flash_opaque_background_uaf           windows/meterpreter/reverse_tcp on 4444

[+] Please use the following URL for the browser attack:
[+] BrowserAutoPwn URL: http://192.168.1.64:8080/NhsAOfjg9CbMI0
```

https://community.rapid7.com/community/metasploit/blog/2015/07/16/the-new-metasploit-browser-autopwn-strikes-faster-and-smarter--part-2

Tools:



Welcome to The Butcher, your source of meats. Please feel free to view our samp to our mailing-list or purchase our specia hamper!

Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email:

Password:

https://sathisharthars.wordpress.com/2014/07/28/hack-facebook-credentials-using-beef/

Browser Exploits

- Some commonly used browser/plugin exploits (2010-2015)

CVE	Name	Software	Version
CVE-2010-0188	PDF Libtiff / Lib	Adobe PDF	PDF < 9.3.1
CVE-2011-3402	TrueType Font - Duqu	Windows	WIN XP-2008 via IE
CVE-2012-1889	XML	Windows	WIN XP-7, Srv2003-2008
CVE-2013-0025	SLayoutRun Use After Free Vulnerability	IE	IE 8
CVE-2013-0074 CVE-2013-3896	Silverlight Double Dereference	Silverlight	Silverlight < 5.1.20913.0
CVE-2012-3993	Firefox COW XrayWrapper pollution	Firefox	FF<17, ESR 10.x before 10.0.8
CVE-2013-0422	JMB/MBEAN and Reflection API	Java	< Java 7u11
CVE-2013-0634	Buffer overflow via crafted SWF	Flash	SWF<10.3.183.51 (win)
CVE-2013-1347	IE UAF	IE	IE 8

CVE	Name	Software	Version
CVE-2013-2463	w click2play bypass. Java Raster	Java	Java < 7u21 - 6u45
CVE-2013-2465	Memory Corruption	Java	Java < 7u21 - 6u45
CVE-2013-2471	Java Raster	Java	Java < 7u21 - 6u45
CVE-2013-2551	IE VML Use-after-free vulnerability	IE	
CVE-2013-2883	Use after free, MutationObserver	Chrome	< 28.0.1500.95
CVE-2013-3897	memory corruption via crafted JavaScript code		IE < 11
CVE-2013-3918	IE InformationCardSigninHelper	IE	IE < 10
CVE-2013-5329	on Flash 11.9.900.117 Memory Corruption	Flash	<11.7.700.252,<11.9.900.152
CVE-2013-7331	IE XMLDOM ActiveX information disclosure	Windows	< 8.1
CVE-2014-0322	Use-after-free via JavaScript code, CMarkup, and the onpropertychange attribute	IE	IE 9. 10
CVE-2013-1493	Java CMM	Java	Java < 7u15 - 6u41
CVE-2013-1710	Firefox CRMF	Firefox	FF < 23, ESR 17.x before 17.0.8
CVE-2013-2423	Java Type	Java	Java < Java7u17
CVE-2013-2424	JMX ,"insufficient class access checks"	Java	Java < 7u17 - 6u43, 5u41

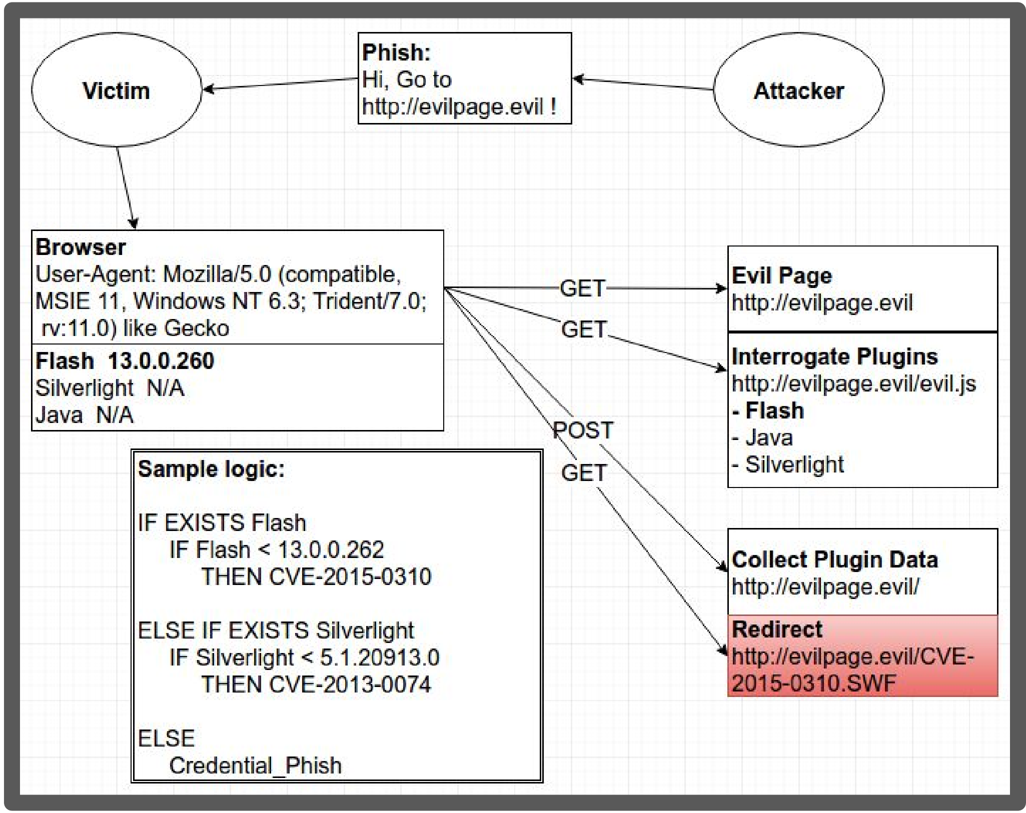
CVE	Name	Software	Version
CVE-2014-0569	Flash casi32	Flash	< 13.0.0.250, <15.0.0.189 (Win, OSX); <11.2.202.411 (Lin)
CVE-2014-1776	Use-after-free, CMarkup::IsConnectedToPrimaryMarkup function	IE	< IE 11
CVE-2014-6332	IE "Unicorn", OleAut32 SafeArrayRedim	Windows	IE 3-11
CVE-2014-8439	invalid pointer dereference	Flash	<13.0.0.258, <15.0.0.239 (Win, OSX) ;<11.2.202.424 (Lin)
CVE-2014-8440	memory corruption	Flash	<13.0.0.252,14.x ,15.0.0.223 (Win,OX); < 11.2.202.418 (Lin); + A.Air
CVE-2015-0310	memory randomization circumventon	Flash	< 16.0.0.287, all < 14-15x, < 13.0.0.262 (winOS) , 11.2.202.438 (Lin)
CVE-2015-0311		Flash	< 16.0.0.287, all < 14-15x, < 13.0.0.262 (winOS)
CVE-2015-0313		Flash	<13.0.0.269, 14.x, 15.x, <16.0.0.305; Linux <11.2.202.442
CVE-2015-0336		Flash	<13.0.0.277, 14.x, 15.x, <17.0.0.134; Linux <11.2.202.451
CVE-2015-0359		Flash	<13.0.0.281, 14.x- 17.x before 17.0.0.169
CVE-2014-0497	Integer underflow	Flash	< 11.7.700.261, 11.8.x-12.0.0.44 (Win, OSX); < 11.2.202.336 (Lin)
CVE-2014-0502	Flash SharedObject double-free	Flash	<11.7.700.269, 11.8.x- 12.0.0.70(Win, OSX), < 11.2.202.341 (Lin) +
CVE-2014-0515	Flash Pixel Bender	Flash	< 11.7.700.279, < 11.8.x, <13.0.0.206 (Win, OSX); < 11.2.202.356 (Lin)

http://contagiodata.blogspot.com/

Exploit Rule Flow

Exploit Kits, BeEF Autorun Rules Engine, MSF Browser AutoPwn.

- Change behavior based on browser characteristics
    - Flash exploit against Flash
    - IE exploit against IE
    - Windows auth popup on Windows
    - Facebook popup if refered by Facebook



Phish:
Hi, Go to
http://evilpage.evil !

Browser
User-Agent: Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko

Flash 13.0.0.260
Silverlight N/A
Java N/A

Evil Page
http://evilpage.evil

Interrogate Plugins
http://evilpage.evil/evil.js
- Flash
- Java
- Silverlight

Collect Plugin Data
http://evilpage.evil/

Redirect
http://evilpage.evil/CVE-2015-0310.SWF

Sample logic:

```
IF EXISTS Flash
    IF Flash < 13.0.0.262
        THEN CVE-2015-0310

ELSE IF EXISTS Silverlight
    IF Silverlight < 5.1.20913.0
        THEN CVE-2013-0074

ELSE
    Credential_Phish
```

Multiple routes to Game Over

Social network targeted phishing and exploitation campaign.
Putting it all together:

1. OSINT - Open Source Intelligence Gathering
2. Establish Friend-of-Friend relationship (2nd degree)
3. Compromise Friend (1st degree)
4. Compromise Primary Target

Multiple routes to Game Over

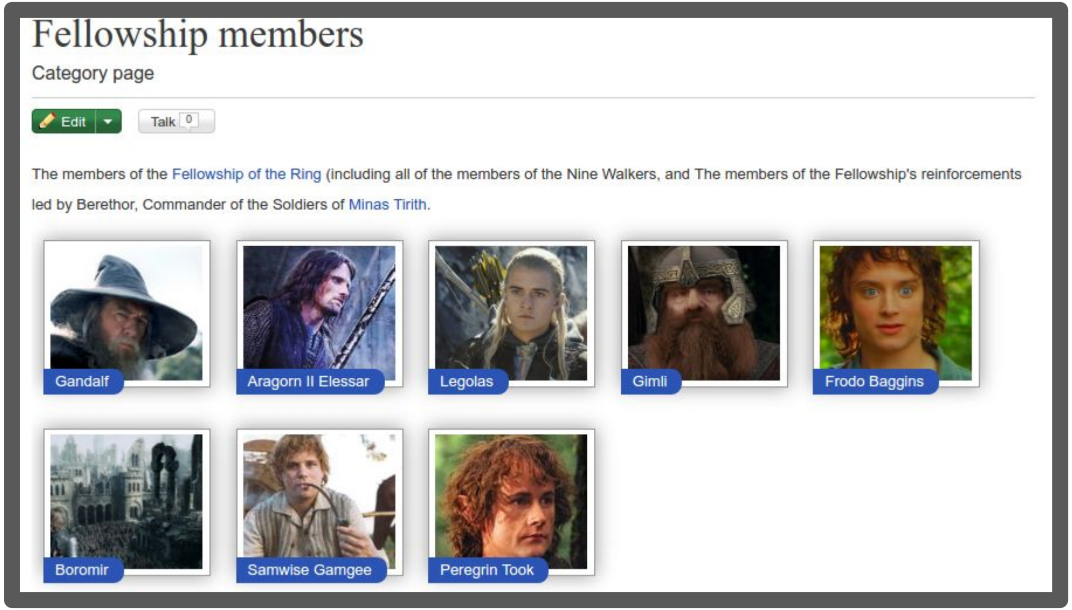
Primary Target: Aragorn II, the son of Arathorn II and Gilraen. King Elessar Telcontar (TA 2931 - FO 120), 26th King of Arnor, 35th King of Gondor, High King of Gondor and Arnor Reunited, The Dúnadan, etc.

- Highly Secured Palantir Tower of Ecthelion Network. Has **Facebook**.
- Tower Guard.
- FO ~50
- “No New Friends”

Multiple routes to Game Over

OSINT - Open Source Intelligence Gathering

1. Google search results, public records, public pages
2. “Public” pages (behind login page/ open of Social Network)



Fellowship members

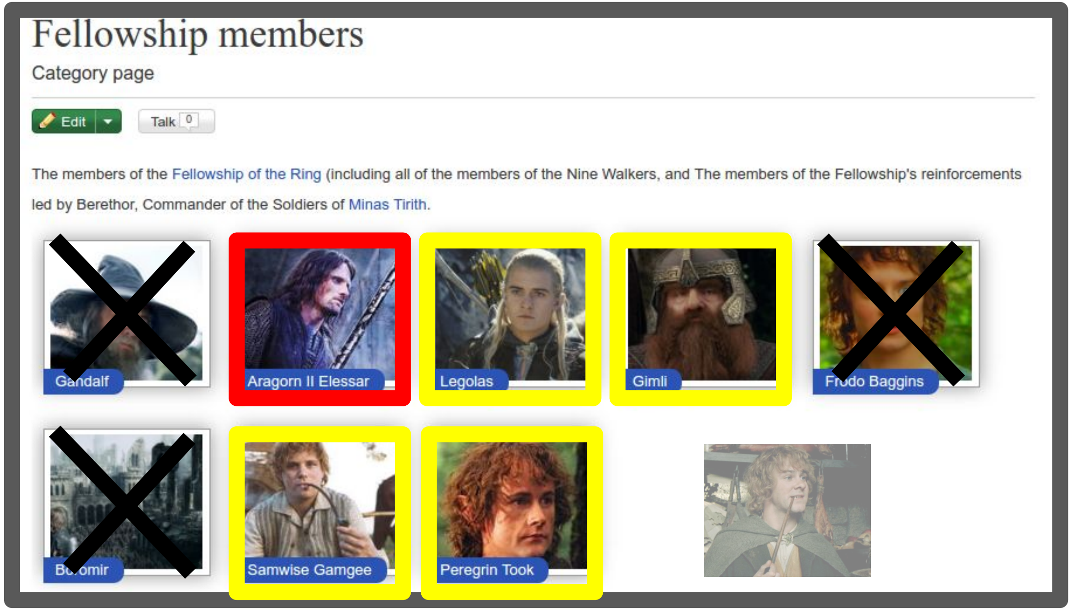
Category page

The members of the Fellowship of the Ring (including all of the members of the Nine Walkers, and The members of the Fellowship's reinforcements led by Berethor, Commander of the Soldiers of Minas Tirith.

Multiple routes to Game Over

OSINT - Open Source Intelligence Gathering

1. Google search results, public records, public pages
2. “Public” pages (behind login page/ open of Social Network)



Fellowship members

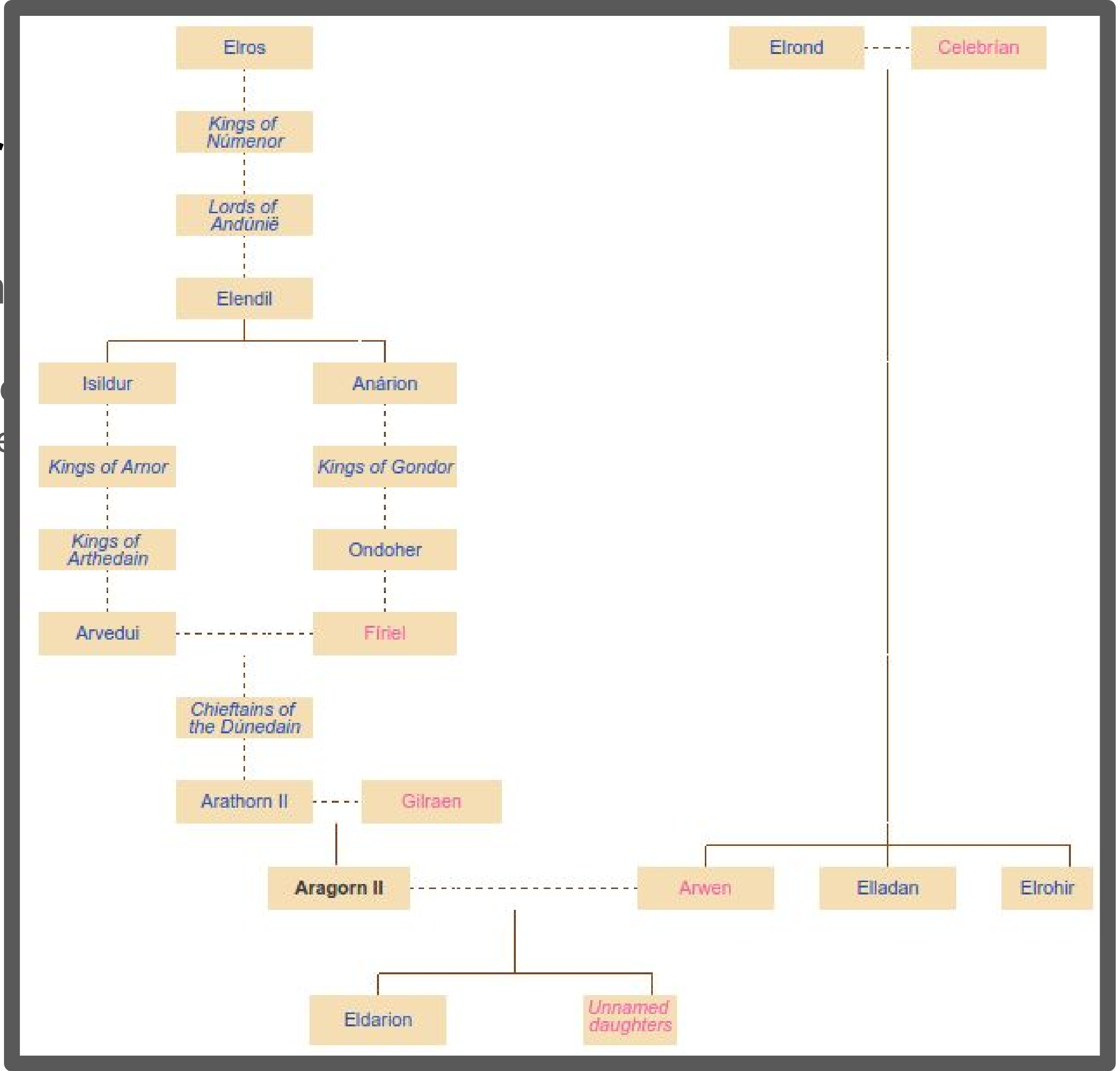
Category page

The members of the Fellowship of the Ring (including all of the members of the Nine Walkers, and The members of the Fellowship's reinforcements led by Berethor, Commander of the Soldiers of Minas Tirith.

Multiple r

OSINT - Open

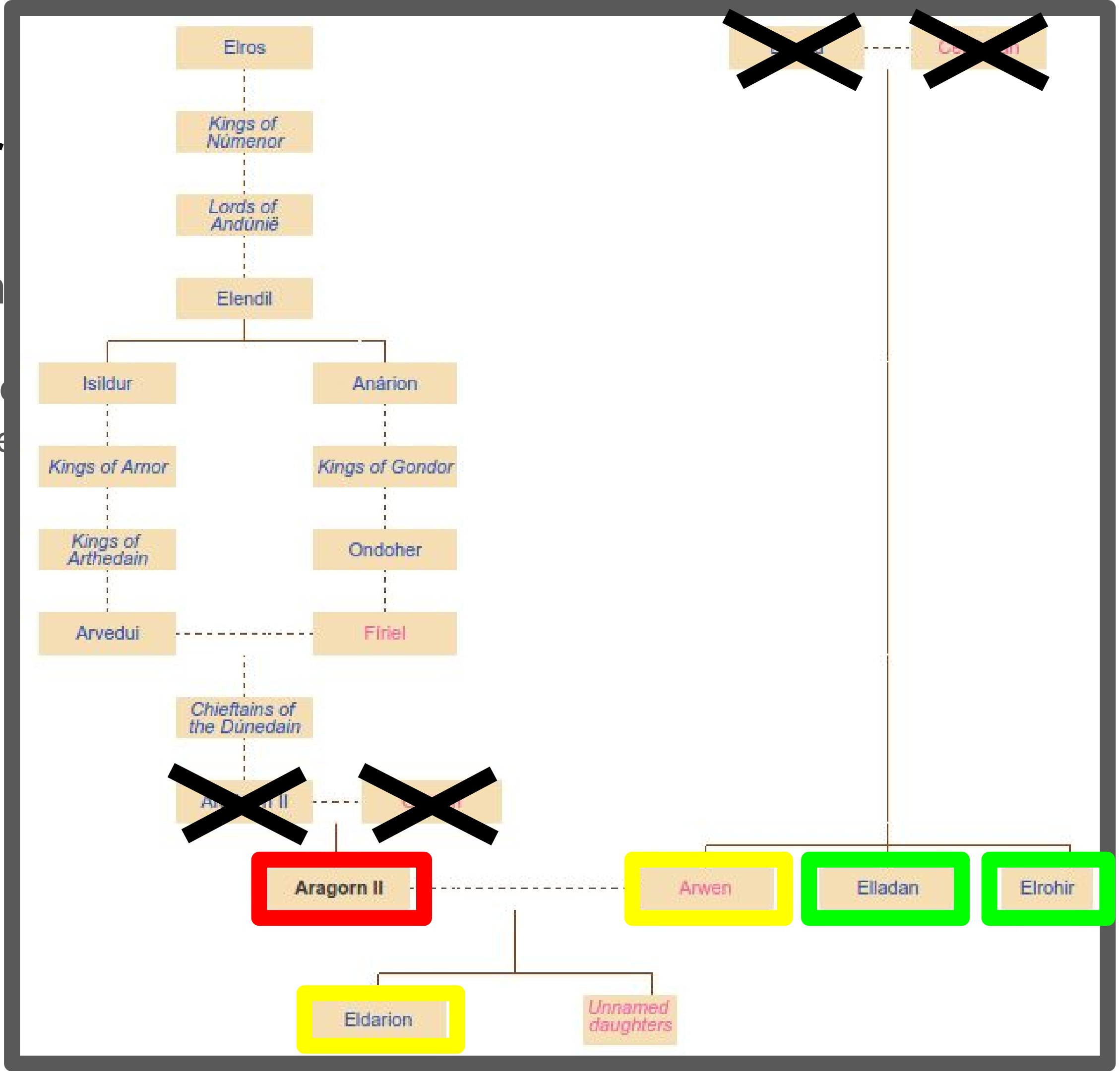
1. Google sear
2. “Public” page



Multiple r

OSINT - Open

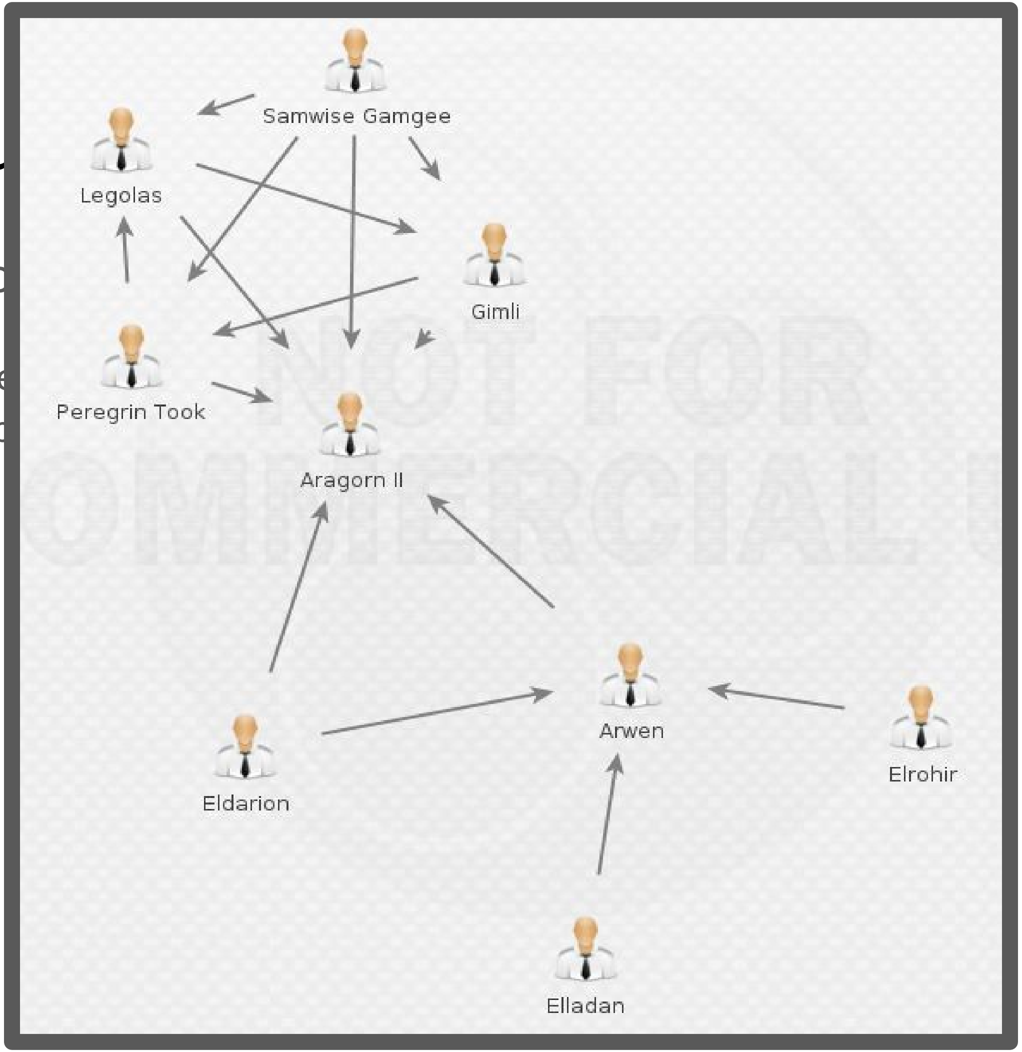
1. Google sear
2. “Public” page



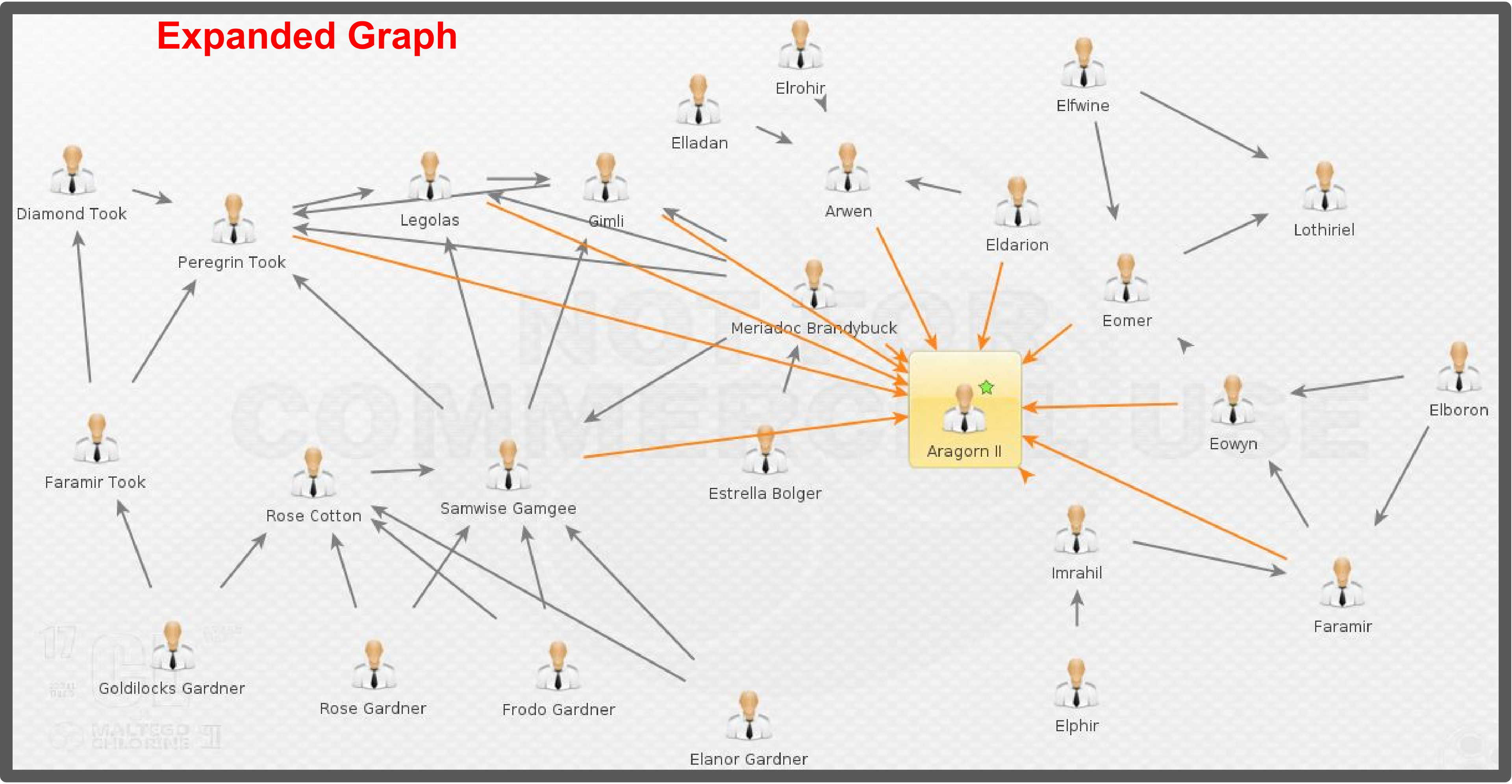
Multiple rou

OSINT - Open So

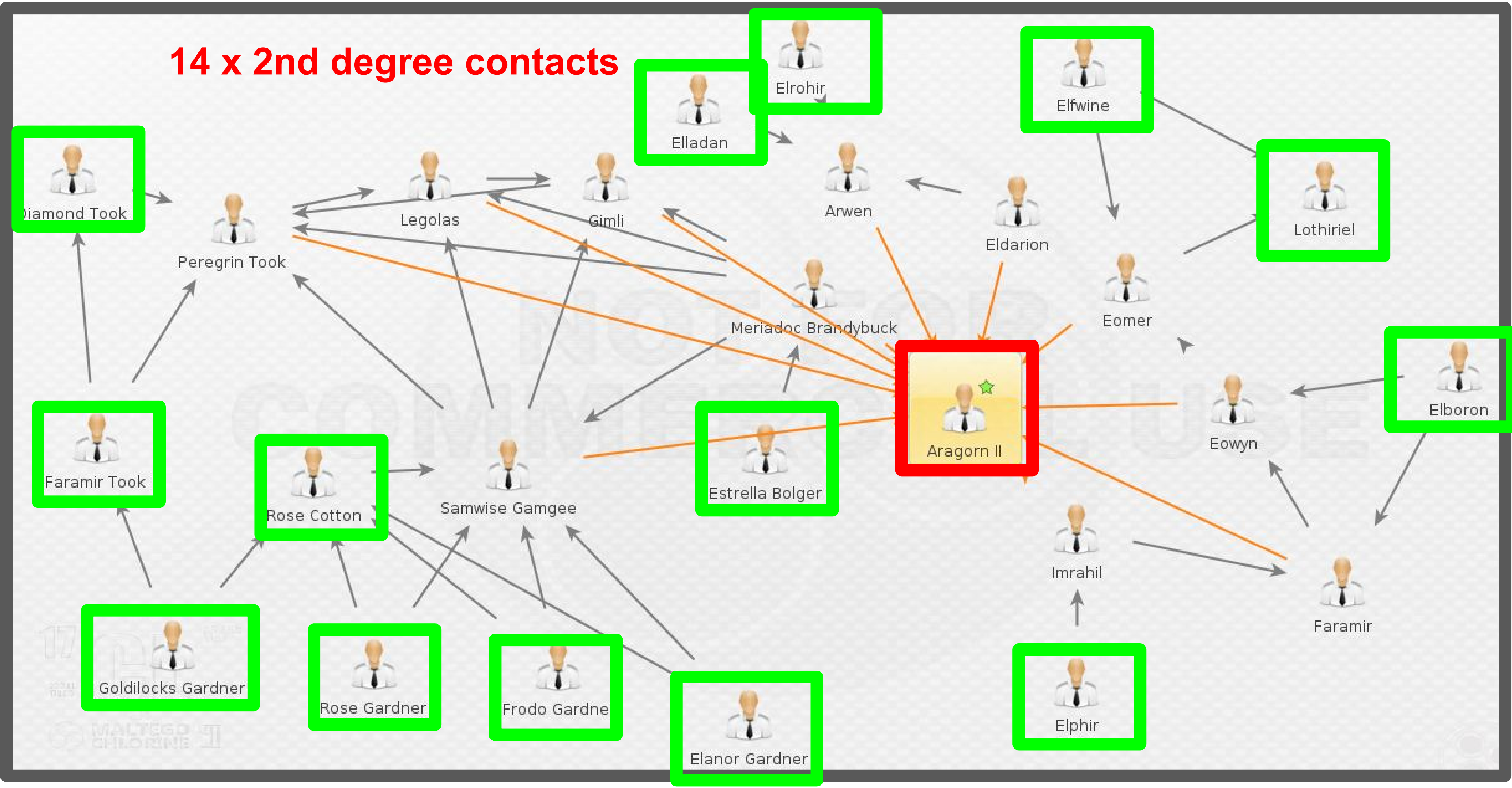
1. Google search re
2. “Public” pages (b



Expanded Graph



14 x 2nd degree contacts



Multiple routes to Game Over

Establish Friend-of-Friend relationship (2nd degree)

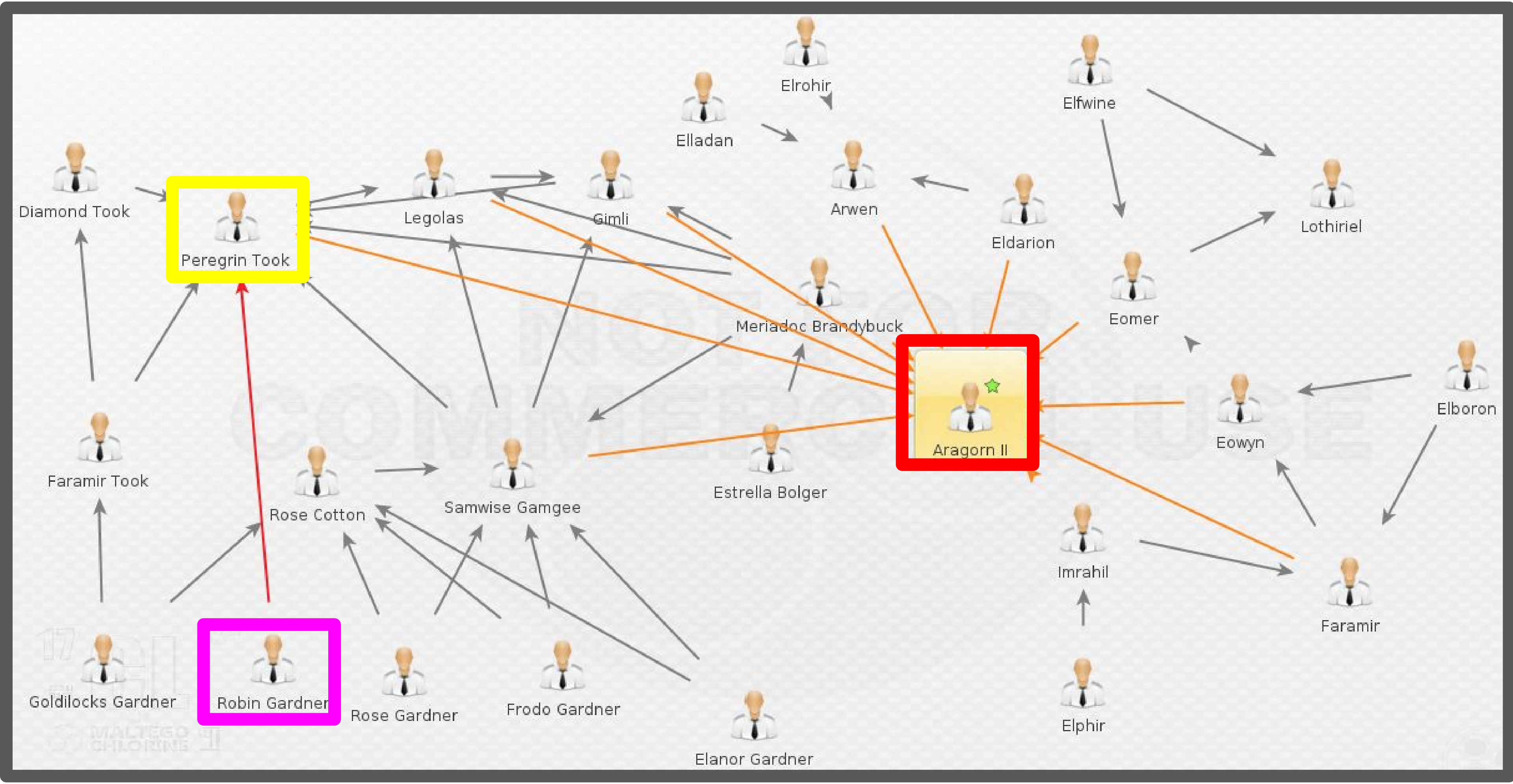
1. Create fake Facebook profile for a likely 3rd or 4th degree contact

   OR

2. Invent a new 3rd or 4th degree contact

   THEN

3. Send a friend request to the 2nd degree contact and insist legitimacy


Elrohir
Elfwine
Elladan
Diamond Took
Peregrin Took
Legolas
Gimli
Arwen
Eldarion
Lothiriel
Meriadoc Brandybuck
Eomer
Aragorn II
Elboron
Eowyn
Faramir Took
Rose Cotton
Samwise Gamgee
Estrella Bolger
Imrahil
Faramir
Goldilocks Gardner
Robin Gardner
Rose Gardner
Frodo Gardner
Elanor Gardner
Elphir
NOT FOR COMMERCIAL USE
MALTEGO CHLORINE

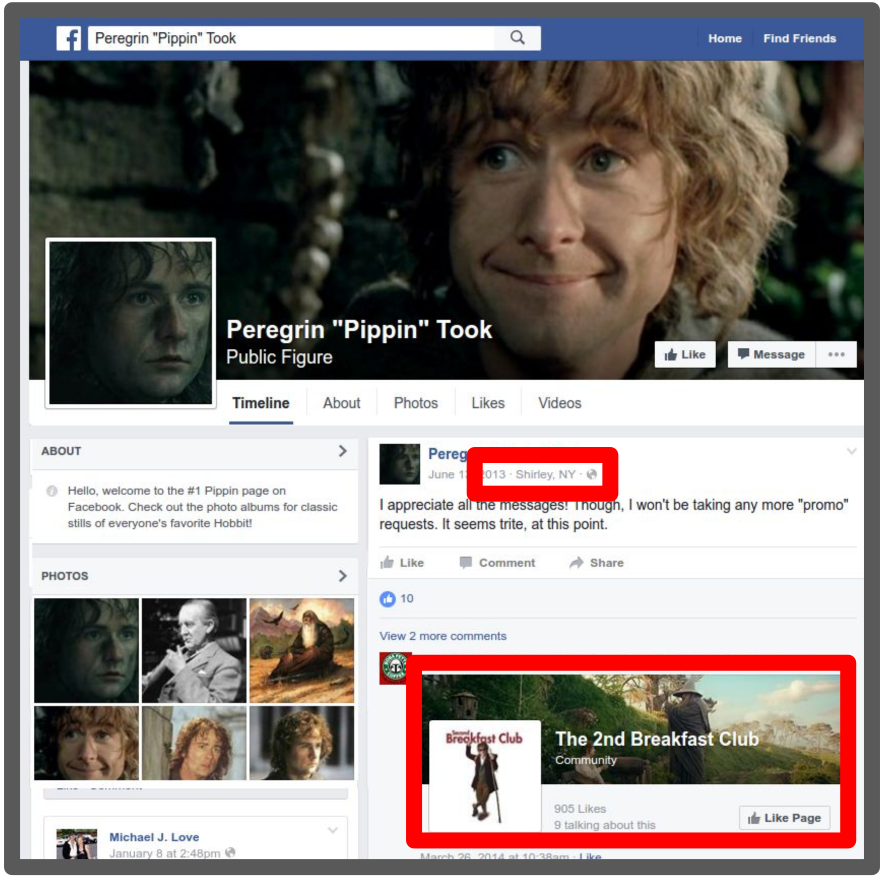
Multiple routes to Game Over

Compromise Friend (1st degree)

1. Explore Interests, Likes, Location

   THEN

2. Craft phish to compromise credentials



Hello, welcome to the #1 Pippin page on Facebook. Check out the photo albums for classic stills of everyone's favorite Hobbit!

Pereg

June 1 013 · Shirley, NY ·

I appreciate all the messages! Though, I won't be taking any more "promo" requests. It seems trite, at this point.

View 2 more comments

The 2nd Breakfast Club

Community

905 Likes

9 talking about this

March 26, 2014 at 10:38am · Like

Michael J. Love

January 8 at 2:48pm

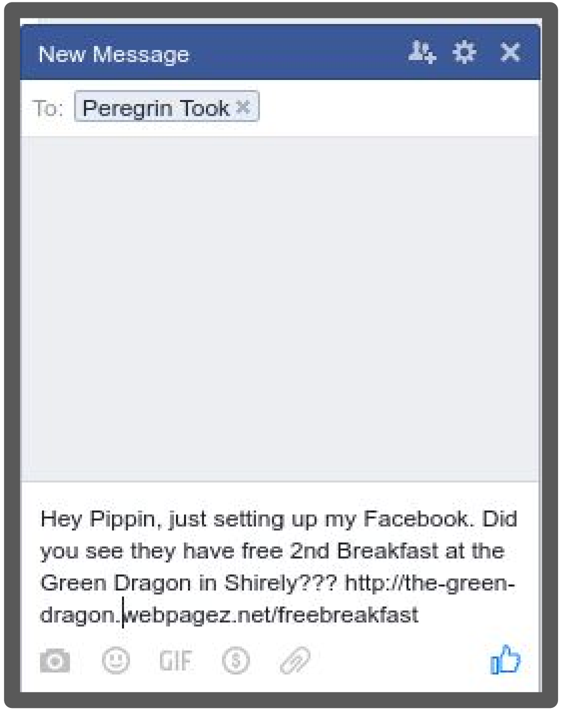
Multiple routes to Game Over

Compromise Friend (1st degree)

1. Explore Interests, Likes, Location

   THEN

2. Craft phish to compromise credentials



To: Peregrin Took

Hey Pippin, just setting up my Facebook. Did you see they have free 2nd Breakfast at the Green Dragon in Shirely??? http://the-green-dragon.webpagez.net/freebreakfast

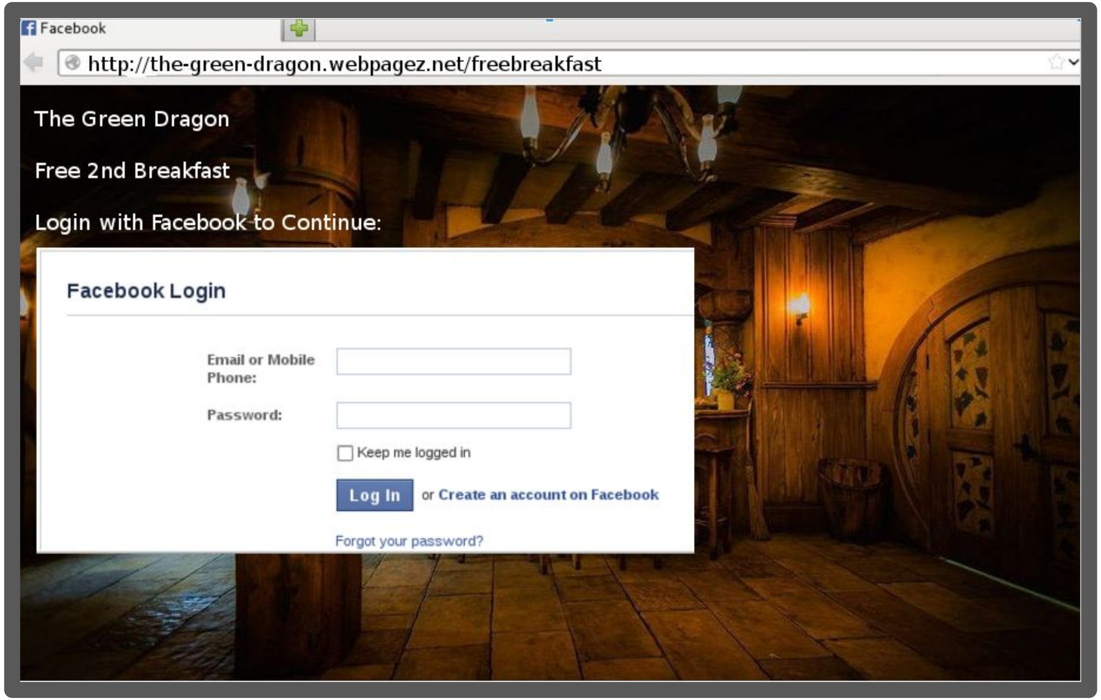
Multiple routes to Game Over

Compromise Friend (1st degree)

1. Explore Interests, Likes, Location

   THEN

2. Craft phish to compromise credentials



Facebook

http://the-green-dragon.webpagez.net/freebreakfast

The Green Dragon

Free 2nd Breakfast

Login with Facebook to Continue:

Facebook Login

Email or Mobile Phone:

Password:

□ Keep me logged in

Log In or Create an account on Facebook

Forgot your password?

Multiple routes to Game Over

Compromise Primary Target

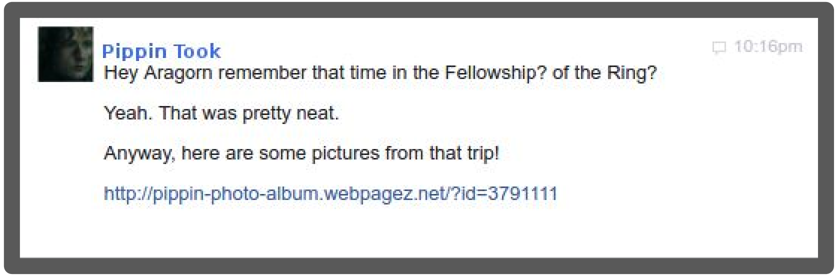
1. Review Primary Target information (friendship history)

   THEN

2. Review Compromised 1st Degree private information

   THEN

3. Craft spear phish to compromise Primary Target



Pippin Took

10:16pm

Hey Aragorn remember that time in the Fellowship? of the Ring?

Yeah. That was pretty neat.

Anyway, here are some pictures from that trip!

http://pippin-photo-album.webpagez.net/?id=3791111

Multiple routes to Game Over

Compromise Primary Target

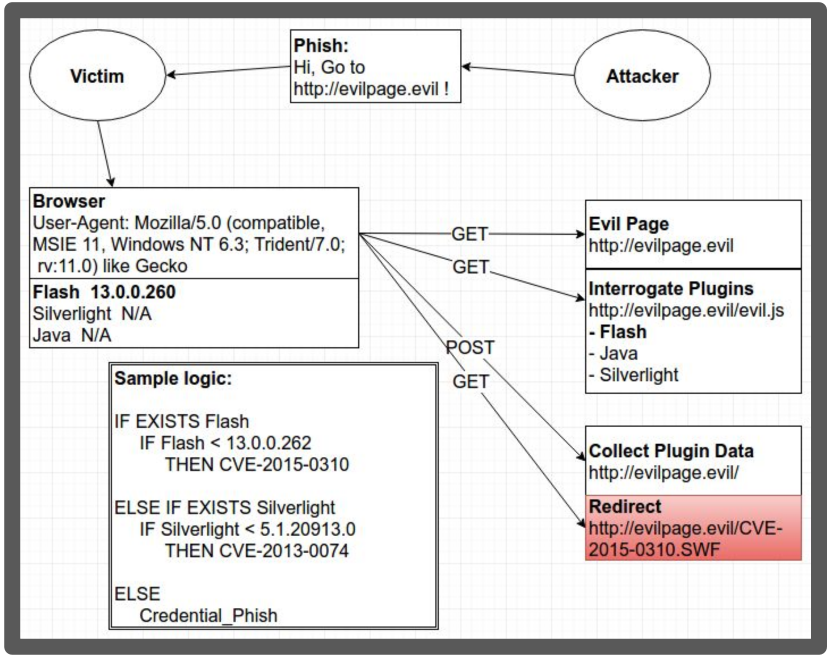
1. Review Primary Target information (friendship history)

   THEN

2. Review Compromised 1st Degree private information

   THEN

3. Craft spear phish to compromise Primary Target



Victim

Phish:
Hi, Go to
http://evilpage.evil !

Attacker

Browser
User-Agent: Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko

Flash 13.0.0.260
Silverlight N/A
Java N/A

GET

GET

POST

GET

Evil Page
http://evilpage.evil

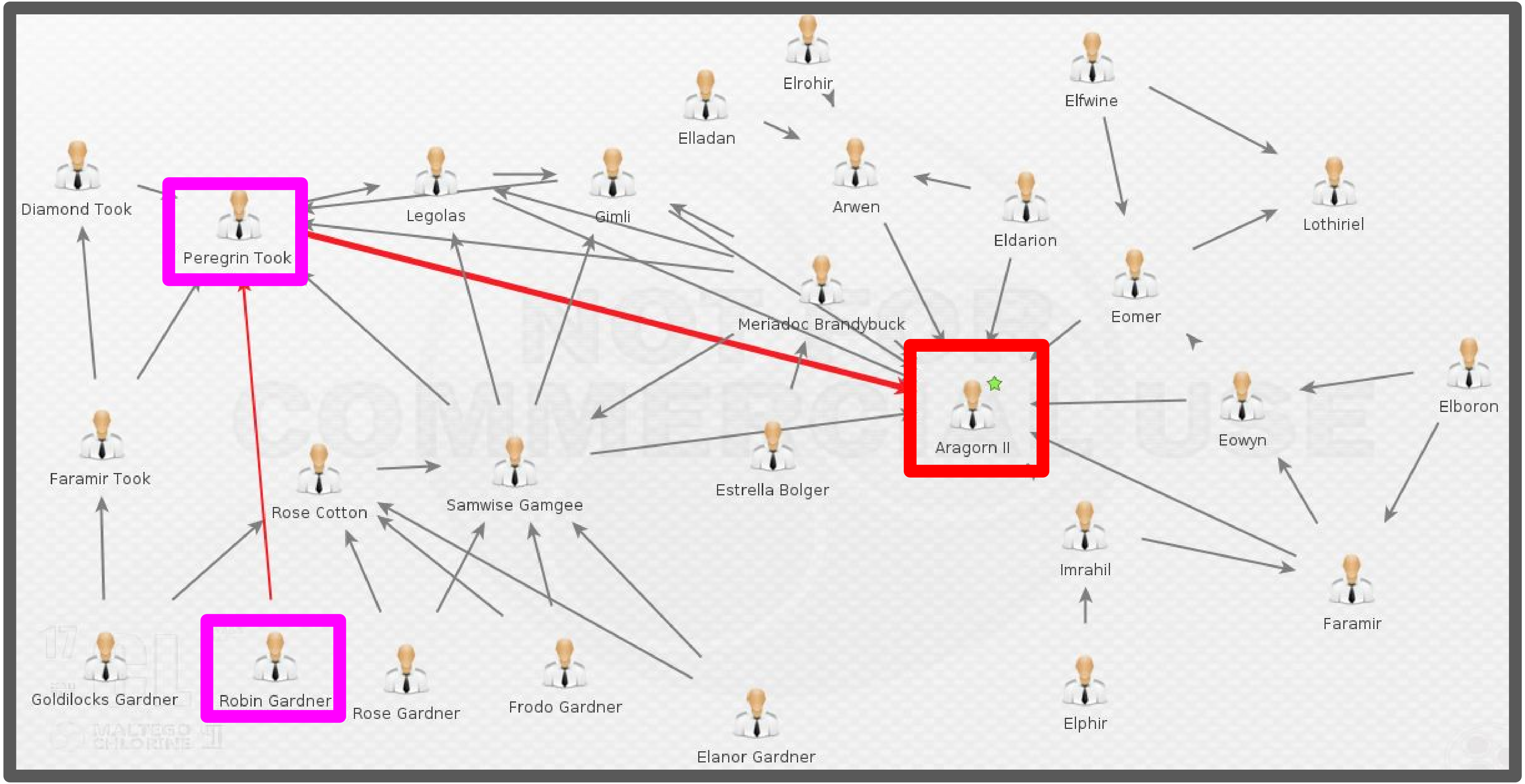
Interrogate Plugins
http://evilpage.evil/evil.js
- **Flash**
- Java
- Silverlight

Collect Plugin Data
http://evilpage.evil/

Redirect
http://evilpage.evil/CVE-2015-0310.SWF

Sample logic:

```
IF EXISTS Flash
    IF Flash < 13.0.0.262
        THEN CVE-2015-0310

ELSE IF EXISTS Silverlight
    IF Silverlight < 5.1.20913.0
        THEN CVE-2013-0074

ELSE
    Credential_Phish
```


Elrohir
Elfwine
Elladan
Diamond Took
Peregrin Took
Legolas
Gimli
Arwen
Eldarion
Lothiriel
Eomer
Meriadoc Brandybuck
Aragorn II
Elboron
Eowyn
Faramir Took
Rose Cotton
Samwise Gamgee
Estrella Bolger
Imrahil
Faramir
Goldilocks Gardner
Robin Gardner
Rose Gardner
Frodo Gardner
Elanor Gardner
Elphir

Game Over

The Lord of The Rings is property of The Tolkien Estate, images New Line Cinema, etc.

Questions

Social Network Phishing

BSidesSATX 21 May 2016

Will Woodson, @wjwoodson, sec@williamwoodson.com