Killing RATs
with an Incident Response Framework

Adrien Chevalier

NSC#1

Robinson Delaugerre

Introduction

Robinson
@Rob_OEM

Adrien
@00_ach

IT Security consultants @Conix_Security

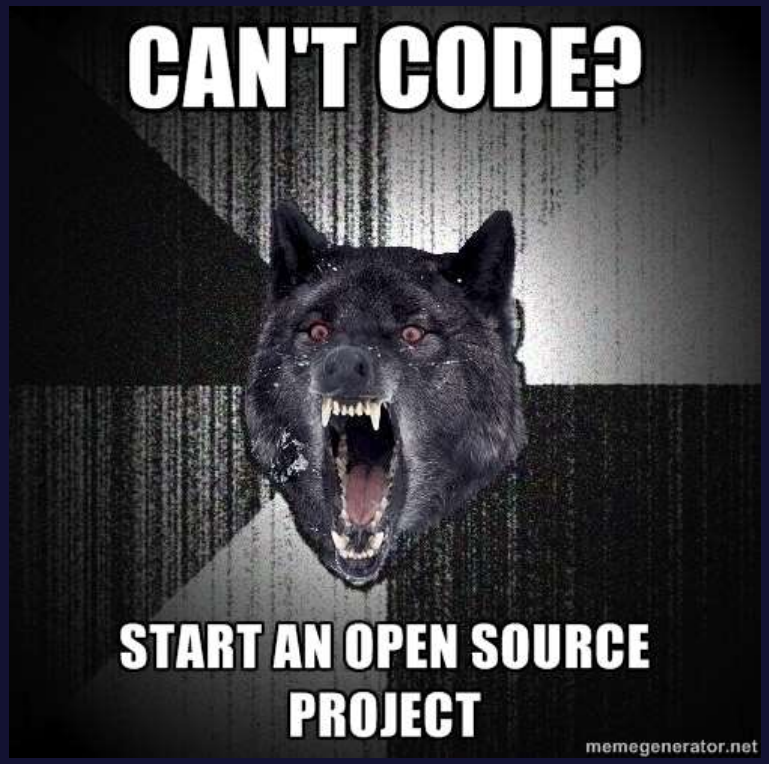
IT Forensics and Incident response
(among other things)

Pretty cool guys (according to our bio on the site…)

Introduction

Robinson

@Rob_OEM



Adrien

@00_ach

Don’t forget

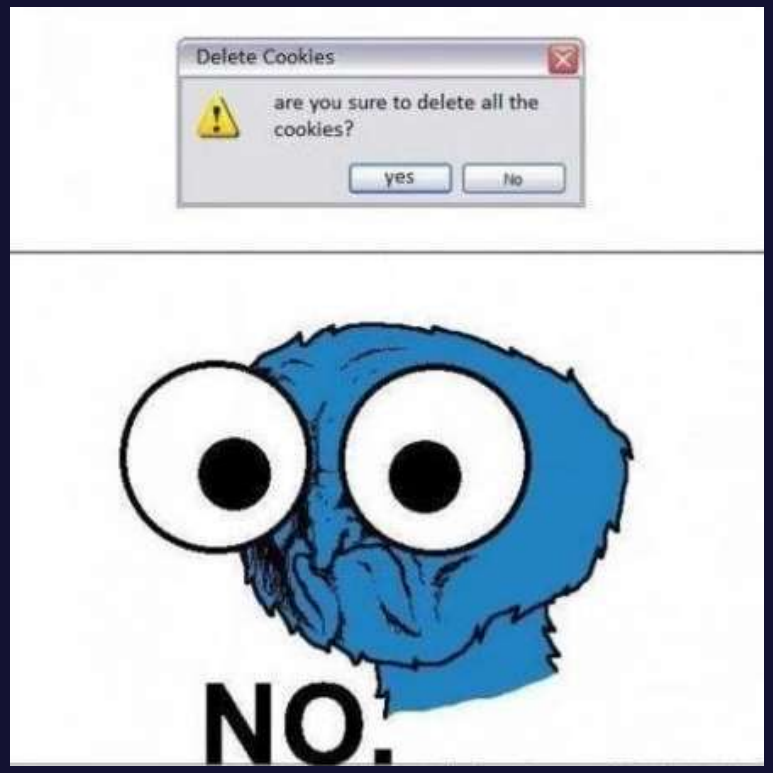
First ti[m]e speaking, please be gentle…

IT Forensics

Study of traces of activity left on computer systems and infrastructure

IT Forensics

Retrieval of traces erased by malicious users on computer systems…



Incident response

Fuck it, we'll do it live!

Incident response

Incident response

Incident response

The attackers are already there

We just got here

They might know the lay of the land better than we do

Our job is to do damage control, to buy time for the defense.

Interlude

WTF? We haven't talked about APT's yet!

APT?


Lioux
le Château
Falaise de la Madeleine
la Croisière
D943
Chât.
St-Saturnin-
-lès-Apt
les Grands Cléments
Marinier
D179
Rustrel
D22
Gignac
Bouvène
D60
les Barbiers
Res. Nat. Géologique du Luberon
D111
Villars
D214
Clavaillan
D4
Carrière d'Ocre
Carr. d'Ocre
Roussillon
D169
Carrière d'Ocre
D83
Gargas
la Doù
Blace
St-Amas
D209
Bartagnons
le Chêne
D35
Caseneuve
D190
le Coulon
Maison du Parc
Apt
le Boisset
St-Ma
-de-Cas
Casteau
N100
Pont Julien
Roquefure
Saignon
l'Abb. St-Eusèbe
27
les Tourrettes
les Agnels
D36
St-Véran
D232
Auribeau
D48
D223
Castellet
Buoux
Sivergues
Prieuré de St-Symphorien
Lacoste
Moulin Clos
Mourre Nègre
Bonnieux
le Fort
Grand Luberon
D3
D36
de la Roche
IGN
INSTITUT GÉOGRAPHIQUE NATIONAL

APT?

What happens when a large company gets pwned.

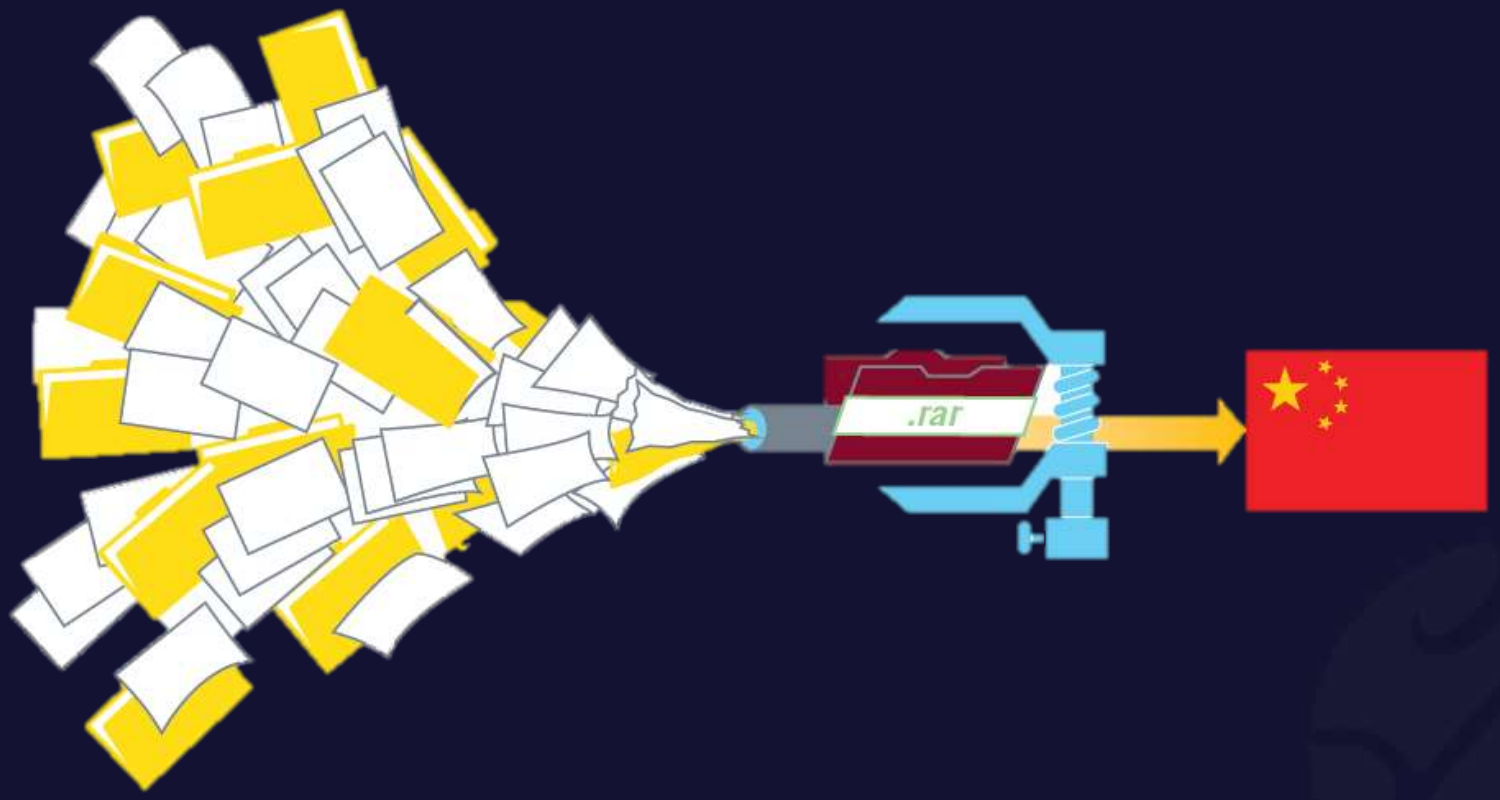
Somehow involves China

With BYOD, IPv6, and Cloud, they are the four Horsemen of the Apocalypse.

Definitely, at least somehow involves China or persons of the Chinese persuasion.

APTs

Mandiant's awesome .rar cannon!



Targeted attacks

A what, not a who

- Procedures, methods… and tools.

The end-goal is to get deep into the network, extract information, and maybe stay there for a long while.

What you get when you have a dedicated human attacker, not a bot or a virus.

Basically, a huge, infrastructure-scale and thorough, unwanted pentest.

End of the interlude

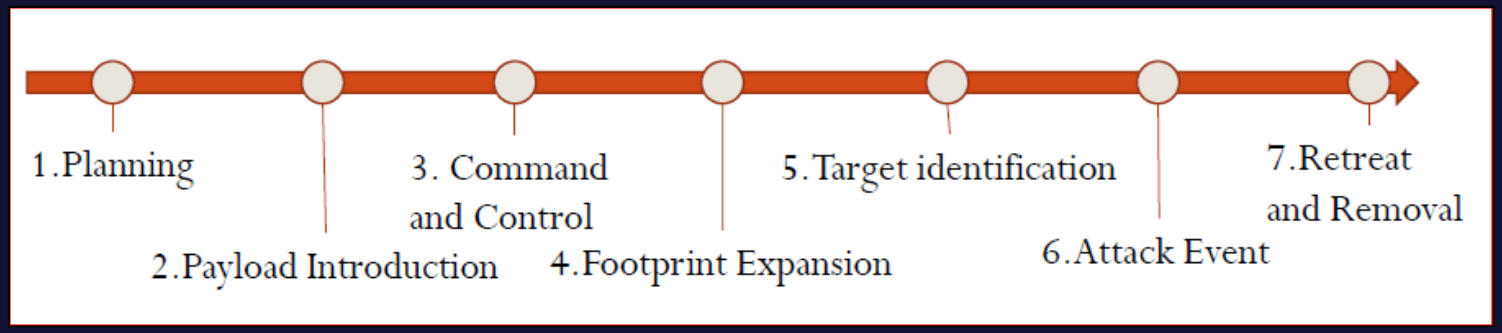
And no more talk about APTs or funny slides after this point

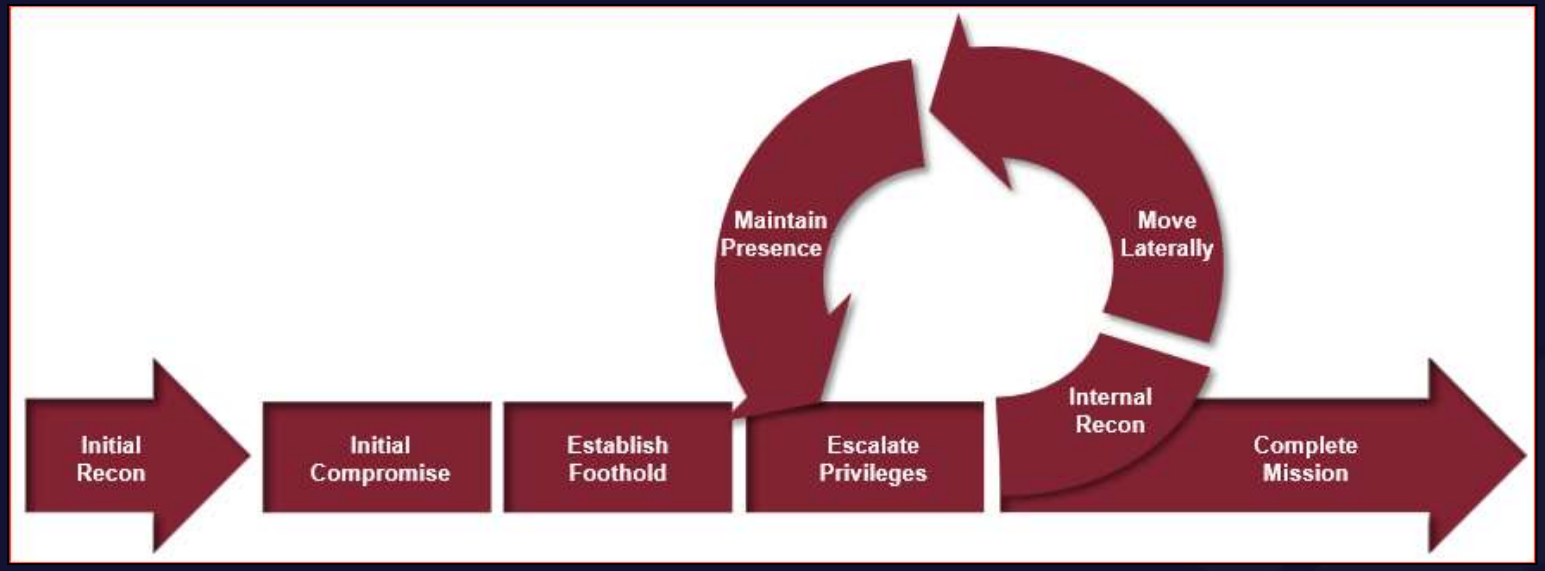
Quote

"Who are our enemies? Who are our friends? This is a question of the first importance"

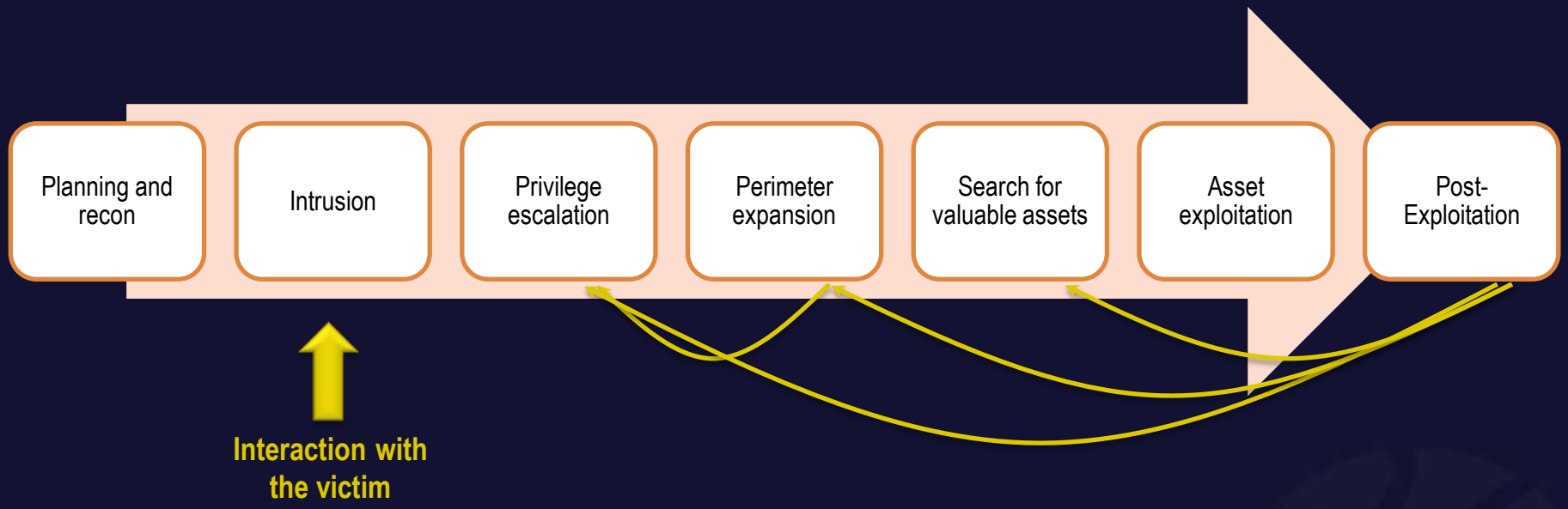
--Sun Tzu

Attacker methodology





Attacker methodology



Attacker methodology

Complex, targeted attacks

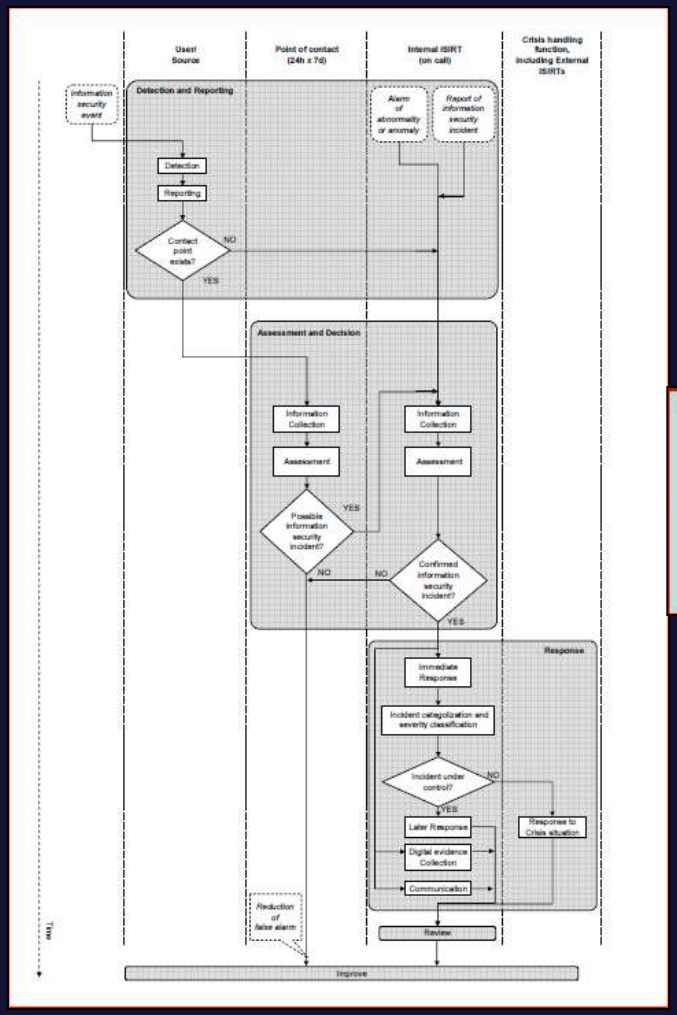
Horizontal and vertical movements

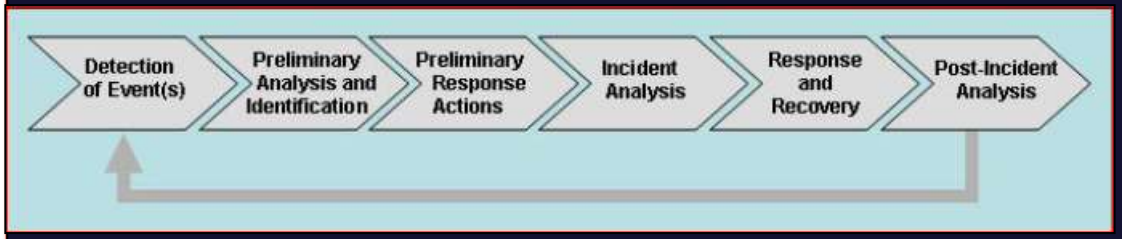
Frequent human intervention

Need for a complex and versatile tool to remotely pilot the attack

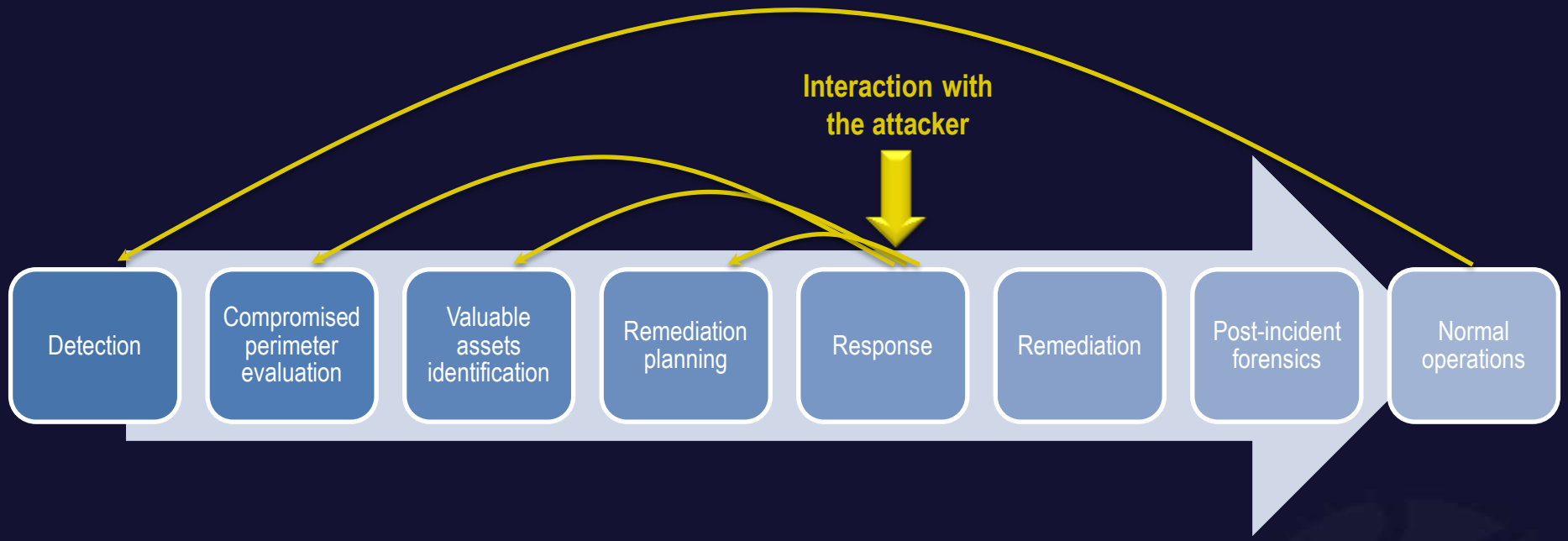
That's what RATs are for!

Defense methodologies

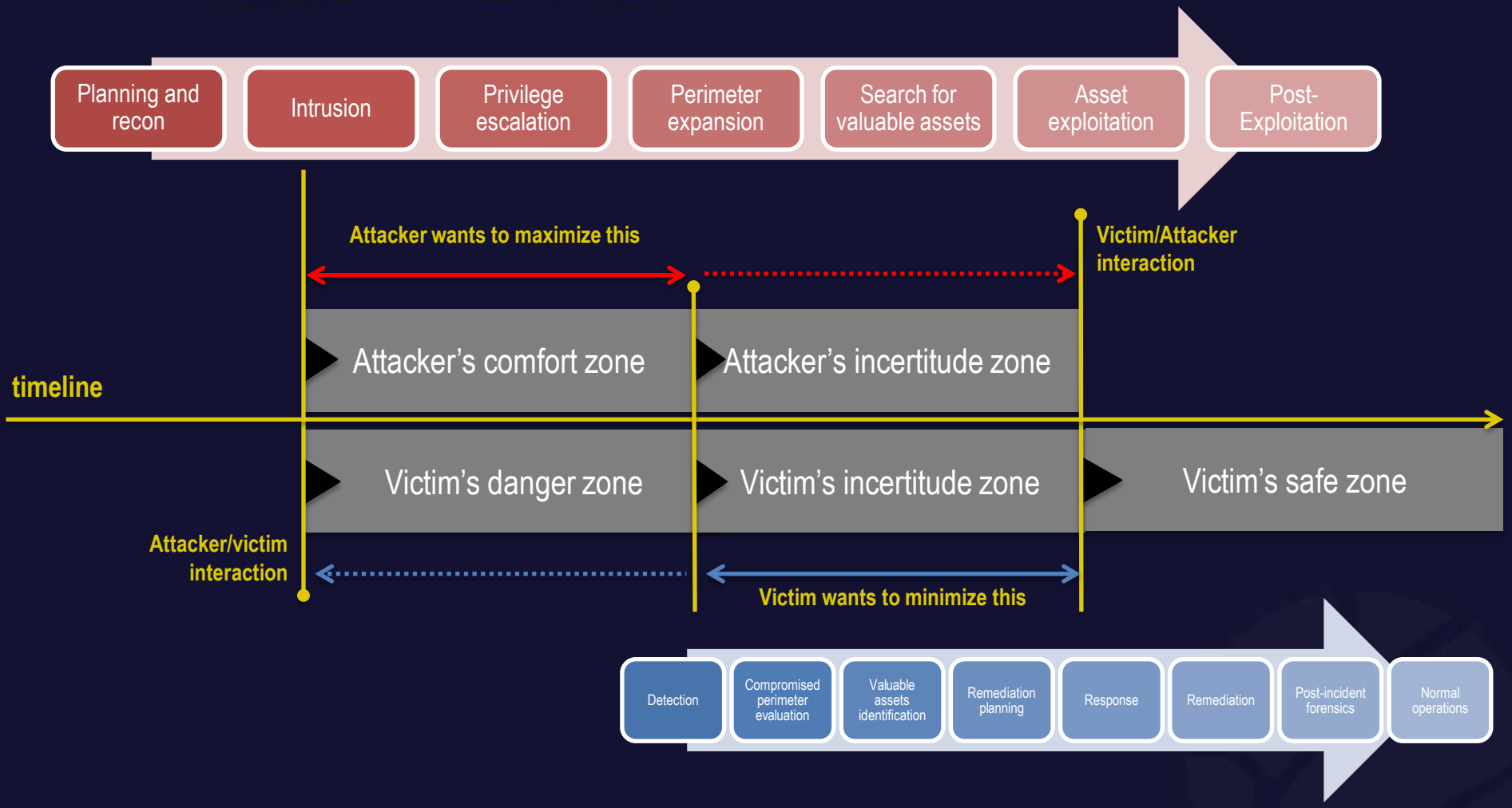




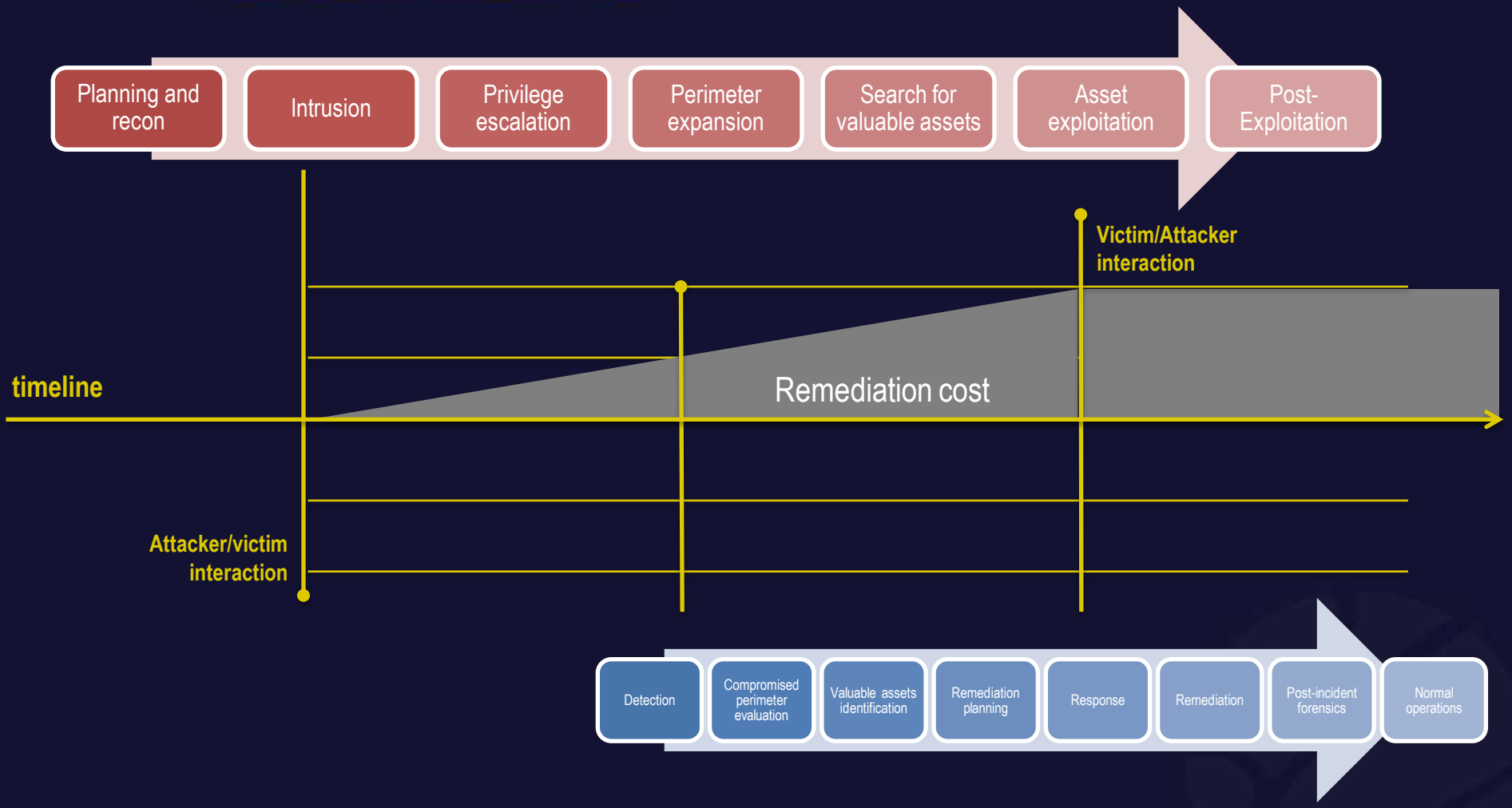
Defense methodologies



All together



All together



Incident response

Very complex process, varies from org to org, attack to attack

Surveillance across the whole perimeter

Assesment of compromized assets

Traceablity of the attacker's actions (in real time?)

That's what Arsenic is for!

Incident response

The Arsenic Framework

Quote

"In this world, things are complicated and are decided by many factors. We should look at problems from different aspects, not from just one."

--Sun Tzu

3 pillars of incident response

Network Analysis

Host Forensics

Reverse Engineering

The Arsenic Framework

Aims to bring together all three pillars

Shared, modular workspace, where each discipline can express its skills

A central place for all the tools needed

An open-source sharing place

The Arsenic Framework

Network traffic signatures → Compromised host analysis → Network traffic dissection

Network traffic signatures

Network traffic reconstruction and dissection

Known protocols (HTTP, DNS) out of the box

- httprequest[:requesturi]
- httpresponse[:headers][:content-type]
- dnsresponse[:ttl]

« session-state » to build protocol-based signatures

Network traffic signatures

Packet or frame-based signatures

- Straight-out Snort signatures
- 60% of the time, it works all the time

Behavioral or protocol based signatures

- Access to a full state machine
- Harder to write
- Harder to evade

Compromised host analysis

The framework generates an executable

Runs on the infected host and gathers information

Embedded signatures are provided by modules

Extracts relevant information

Modules process this information

Compromised host analysis

Tries to identify the module-supplied signatures

In files for patterns

In running processes memory regions for patterns

In the registry for regex in key names, values, etc.

Compromised host analysis

Sandbox mode to analyze packed RATs

Starts the executable and injects code

Blocks specified APIs to avoid propagation

Starts a scan when a specific API is called

Still must be ran on isolated machines

Network traffic dissection

Built with reverse engineering of the malware

Decrypts and decodes all the network traffic

Gives the defense a full visibility of the attacker's actions

This is where module writers do most of the work

Quote

"It is not enough to set tasks; we must also solve the problem of the methods for carrying them out. If our task is to cross a river, we cannot cross it without a bridge or a boat. Unless the bridge or boat problem is solved, it is idle to speak of crossing the river. Unless the problem of method is solved, talk about the task is useless.

--Sun Tzu

Demo!

Arsenic Framework vs. Poison Ivy

The Poison Ivy RAT

10 years old, development discontinued

Free to download and play with (in throwaway VM's)

Not fully detected by AVs until a few months ago

Hard to detect on the network

Still used today to pwn Big Companies

Poison Ivy - [Listening on Port: 3460 (Connections: 1)]

File Preferences Window Help

Connection

WAN

92.168.158.

Version 2.3

rat01 [192.168.158.131] - Poison Ivy

- Information
- Managers
  - Files
    - Search
  - Regedit
    - Search
  - Processes
  - Services
  - Devices
  - Installed Applications
  - Windows
- Tools
  - Relay
  - Active Ports
  - Remote Shell
  - Password Audit
    - Cached
    - NT/NTLM Hashes
    - Wireless
- Surveillance
  - Key Logger
  - Audio Capture
  - Screen Capture
  - Webcam Capture
- Plugins
- Administration
  - Edit ID
  - Share
  - Update
  - Restart
  - Uninstall

File Manager

- A:\ (Removable)
- C:\ (Fixed, free: 38.07/39.99 GiB)
  - abcd
  - Documents and Settings
    - Administrateur
      - Application Data
      - Bureau
      - Cookies
      - Favoris
      - Local Settings
      - Menu Démarrer
      - Mes documents
        - Ma musique
        - Mes images
      - Modèles
      - Recent
      - SendTo
      - Voisinage d'impression
      - Voisinage réseau
    - All Users
    - Default User
    - LocalService
    - NetworkService
  - Program Files
  - RECYCLER
    - S-1-5-21-1482476501-2111687655-1801674531-500
      - Dc3
  - test
    - test1
  - System Volume Information
  - testfolder3
  - WINDOWS
    - addins
    - AppPatch
    - Config

Name	Size	Type	Attrib.
desktop.ini	86.00 B	INI	AHS

C:\Documents and Settings\Administrateur\Mes documents\ 5 objects 86.00 B

Download: 0.00 B/s Upload: 0.00 B/s

Poison Ivy - [Listening on Port: 3460 (Connections: 1)]

File Preferences Window Help

Connections | Statistics | Settings

rat01 [192.168.158.131] - Poison Ivy

- Information
- Managers
  - Files
    - Search
  - Regedit
    - Search
  - Processes
  - Services
  - Devices
  - Installed Applications
  - Windows
- Tools
  - Relay
  - Active Ports
  - Remote Shell*
  - Password Audit
    - Cached
    - NT/NTLM Hashes
    - Wireless
- Surveillance
  - Key Logger
  - Audio Capture
  - Screen Capture
  - Webcam Capture
- Plugins
- Administration
  - Edit ID
  - Share
  - Update
  - Restart
  - Uninstall

Remote Shell

```
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>net use
net use
Les nouvelles connexions seront mémorisées.

La liste est vide.

C:\>
```

Poison Ivy - [Listening on Port: 3460 (Connections: 1)]

File Preferences Window Help

Connection

WAN

92.168.158.

Version 2.3

rat01 [192.168.158.131] - Poison Ivy

- Information
- Managers
  - Files
    - Search
  - Regedit
    - Search
  - Processes
  - Services
  - Devices
  - Installed Applications
  - Windows
- Tools
  - Relay
  - Active Ports
  - Remote Shell
  - Password Audit
    - Cached
    - NT/NTLM Hashes
    - Wireless
- Surveillance
  - Key Logger
  - Audio Capture
  - Screen Capture
  - Webcam Capture
- Plugins
- Administration
  - Edit ID
  - Share
  - Update
  - Restart
  - Uninstall

LM/NTLM Hashes

User Name	LM Hash	NT Hash
Administrateur	AAD3B435B51404EEAAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
HelpAssistant	75CBF8D08D7E9DAE3934B67CC92...	3AD4AA84BE2DA132A0C5EA85C6F234F6
Invité	AAD3B435B51404EEAAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0
SUPPORT_3889...	AAD3B435B51404EEAAD3B435B51...	7A8DE945915F1F9604C5233335187ABF

Download: 0.00 B/s Upload: 0.00 B/s

Process overview

Poison Ivy: Network detection

Some Emerging Threats signatures

- Handshake packet size (matches on any 256b packet)
- Keep-alive (key-based)
  - Nice to know, when you know it

Some protocol-based signatures

- Keepalive (class signature – key agnostic)
- Handshake (instance signature – known key)

Poison Ivy: Network detection

What if the we don't know the key, or it is changed?

- We still have one reliable class signature
- We are able to pinpoint infected hosts

Poison Ivy: Network detection

```
root@cnxcpy-laptop:/home/conix/arsenic#  ./ArsenicFramework.rb

 Do you think what I'm        ,.   '\'\    ,---.    Err ... right,
   thinking, Pinky?           | \\  l\\l_ //    |   Brain! But how
   _    \          _          |  \\/ '/  .|     |   do we go to
  /~\\   \        //~\        | Y |   |   ||  Y |   China by foot?
  |  \\   \      //  |        |  \|   |   |\ /  |   /
  [   ||        ||   ]        \   |  o|o  | >  /   /
  ] Y  ||        ||  Y [        \___\_--_ /_/__/
  |  \_|l,-------.l|_/  |       /.-\(____) /--.\
  |   >'            `<   |      `--(_____)----'
  \  (/~`--____--'~\)  /           U// U / \
   `-_>-_________-<_-'              / \  / /|
      /(_#(__)#_)\                 ( .) / / ]
      \___/__\___/                   `.'`/   [
       /__`--'__\                     |`.`    |
    /\(__,>--- __)                    |       |__
  /\//\\(   `---- )                   _l      |--:.
  '\/  <^\      /^>                  |  `    (  <   \\
      _\ >-__-< /_                  ,-\  ,----->. \    `:___,/
     (___\    /___)                (____/   (____)     `---'

Arsenic Framework - v.1.0 - NoSuchFramework
type options to get contextual help

Arsenic> capture
Arsenic::Capture> capture 'vmnet1'
[+] Begin capture on vmnet1
[+] Capture filter :
[d] Found possible Poison Ivy keepalive
[d] Found possible Poison Ivy keepalive response
##############################################################################
#                    Poison Ivy keepalive signature matched                  #
##############################################################################
        [+] Infected Host : 192.168.158.131
        [+] C2 server : 192.168.158.129
```

WXP - C2 - VMware Player (Non-commercial use only)

File Virtual Machine Help

Poison Ivy - [Listening on Port: 3460 (Connections: 1)]

File Preferences Window Help

Connections Statistics Settings

WAN	LAN	Con. Type	Computer	User Name	Acc. Type	OS	CPU	RAM	Version
192.168.158.131	192.168.158.131	Direct	USER	Administrateur	Admin	WinXP	2891 MHz	511.48 MiB	2.3.1

Version 2.3.2 Nr. of Ports: 1 Nr. of Plugins: 0 Nr. of Connections: 1

démarrer

To grab input, press Ctrl+G

Process overview

Network traffic signatures → Compromised host analysis → Network traffic dissection

Poison Ivy: Host Analysis

Various Poison Ivy signatures

Binary : machine code pattern

Registry : startup keys pointing to ADS

In memory : machine code / configuration structs

Sandbox : blocks infection & connection to C2 server

Poison Ivy: Host Analysis

```
root@cnxcpy-laptop:/home/conix/arsenic# sudo ./ArsenicFramework.r

 Do you think what I'm thinking, Pinky?

 Err ... right, Brain! But how do we go to China by foot?

Arsenic Framework - v.1.0 - NoSuchFramework
type options to get contextual help

Arsenic> modules
Arsenic::Modules> poisonIvy
Arsenic::Modules::PoisonIvy> generate
Generating scan binary for module Arsenic::PoisonIvy
Done. Output is at /tmp/arsenicframework/scanner.exe
Arsenic::Modules::PoisonIvy>
```

WXP - user - VMware Player (Non-commercial use only)

File Virtual Machine Help

```
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrateur>cd Bureau

C:\Documents and Settings\Administrateur\Bureau>scanner.exe
> Loading configuration...
        [-] Loading memory pattern... OK!
        [-] Loading memory pattern... OK!
        [-] Loading memory pattern... OK!
        [-] Loading memory pattern... OK!
        [-] Loading file pattern... OK!
        [-] Loading registry pattern... OK!
        [-] Loading registry pattern... OK!
        [-] Loading debug data... OK!

> Starting registry scan!

> Starting memory scan!
        [-] Scan System... CLEAN.
        [-] Scan smss.exe... CLEAN.
        [-] Scan csrss.exe... CLEAN.
        [-] Scan winlogon.exe... CLEAN.
        [-] Scan services.exe... CLEAN.
        [-] Scan lsass.exe... CLEAN.
        [-] Scan svchost.exe... CLEAN.
        [-] Scan svchost.exe... CLEAN.
        [-] Scan svchost.exe... CLEAN.
        [-] Scan svchost.exe... CLEAN.
        [-] Scan svchost.exe... CLEAN.
        [-] Scan spoolsv.exe... CLEAN.
        [-] Scan explorer.exe... PATTERN MATCHED.
        [-] Scan alg.exe... CLEAN.
        [-] Scan wscntfy.exe... CLEAN.
        [-] Scan wpabaln.exe... CLEAN.
        [-] Scan cmd.exe... CLEAN.
        [-] Scan IEXPLORE.EXE... PATTERN MATCHED.
        [-] Scan cmd.exe... CLEAN.
        [-] Scan scanner.exe... CLEAN.

> Output saved in scan_report.bin file.

C:\Documents and Settings\Administrateur\Bureau>_
```

Process overview

Network traffic signatures → Compromised host analysis → Network traffic dissection

Poison Ivy: Network Dissection

"It is well known that when you do anything, unless you understand its actual circumstances, its nature and its relations to other things, you will not know the laws governing it, or know how to do it, or be able to do it well."

--Sun Tzu

Poison Ivy: Network Dissection

Parsing of the dump from earlier

Decryption and decompression of the traffic

Interpretation

The bulk of what we want, and most of the work

Let's see how this works

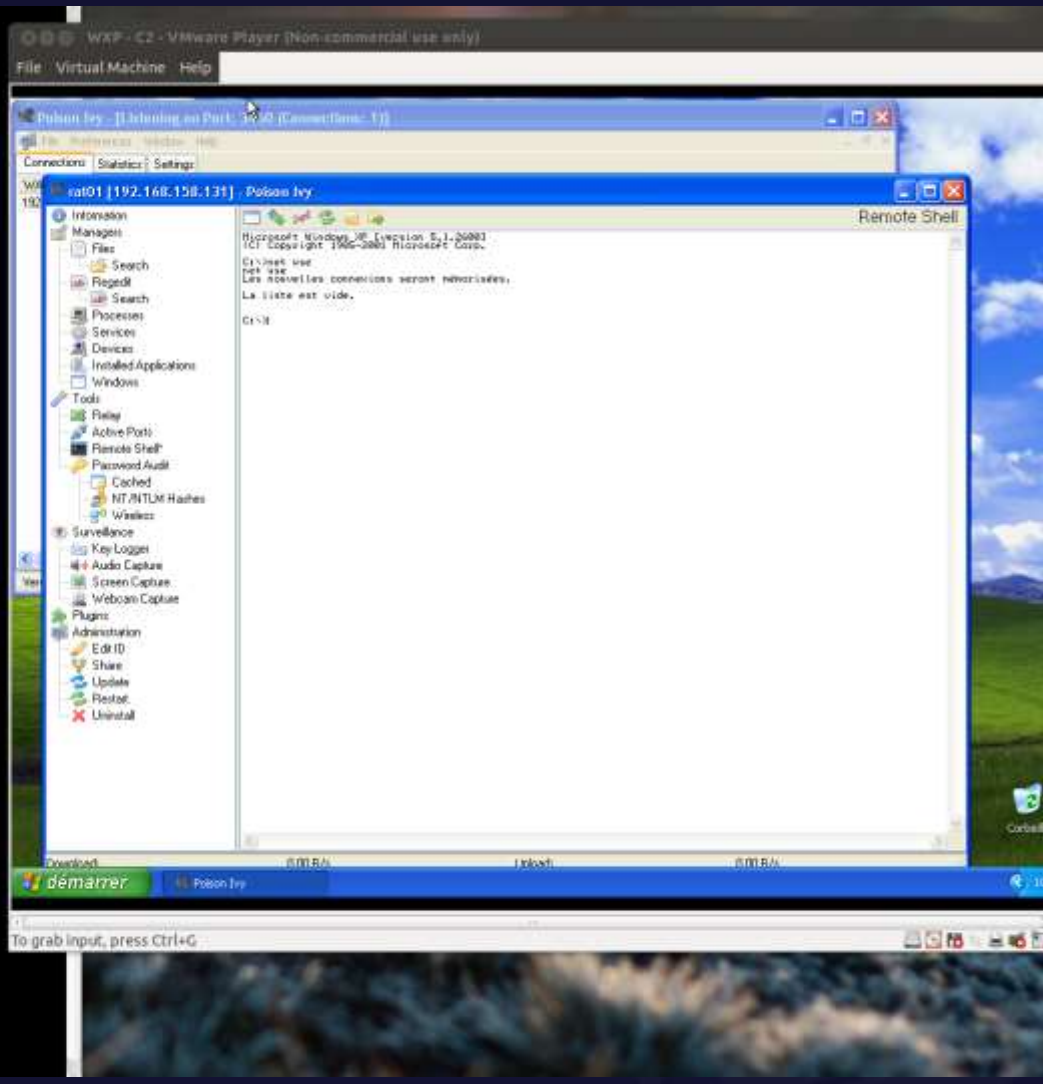
Poison Ivy: Network Dissection

```
Arsenic::Capture> capture 'vmnet1'
[+] Begin capture on vmnet1
[+] Capture filter :
[d] Found Poison Ivy keepalive matching instance key
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Keepalive
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Keepalive
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Query system information
        - Information sent by the RAT :
            + Machine's name : 76413-028-4653287-22384
            + Domain : WORKGROUP
            + CPU :        Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
            + Proxy server : c2.nosuchcon.local:3460
            + Proxy server : 192.168.158.129:3460
            + Persistance registry key : SOFTWARE\Microsoft\Windows\CurrentVersion\Run
            + Key value name : msupdate
            + Malware executable filename : msupdate.exe
            + Malware actually running : C:\WINDOWS\system32\msupdate.exe
            + Malware's mutex : mut3x!
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Keepalive
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Dump NT/NTLM hashs
        - Administrateur hashs :
          + LM : aad3b435b5144eeaad3b435b5144ee
          + NT : 31d6cfe0d16ae931b73c59d7e0c089c0
        - HelpAssistant hashs :
          + LM : 75cbf8d08d7e9dae3934b67cc9206191
          + NT : 3ad4aa84be2da132a0c5ea85c6f234f6
        - Invit? hashs :
          + LM : aad3b435b5144eeaad3b435b5144ee
          + NT : 31d6cfe0d16ae931b73c59d7e0c089c0
        - SUPPORT_388945a0????\PIPE\lsarpc hashs :
          + LM : aad3b435b5144eeaad3b435b5144ee
          + NT : 7a8de945915f1f964c5233335187abf
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Start command-line feature
        - output :
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Keepalive
[-] Poison Ivy command from 192.168.158.129:3460 to 192.168.158.131:1177
        Remote shell command execution
        - command : net use
        - output :
net use
Les nouvelles connexions seront memorisees.

La liste est vide.


C:\>
```



Wrapping up

Arsenic Framework

"Be resolute, fear no sacrifice and surmount every difficulty to win victory."

--Sun Tzu

Forensics and Incident Response

In the Framework, every attacker action is journalized

You can query the timeline database

Export data

Traceability out of the box!

TODO list

Code cleaning/Test writing

A better API for module writers

Performance issues (multithreading)

Add features to the host analysis

MOAR modules!

IPv6 and x64 compatibility (we'll get to it…)

What's next?

Release of the source code in less than a month

Everything will be announced on Twitter
@ArsenicRats

We hope you will enjoy it, or at least play with it

Questions?

Thanks for your attention

Killing RATs, the Arsenic Framework

Robinson Delaugerre
@Rob_OEM

robinson.delaugerre@conix.fr

Adrien Chevalier
@00_ach

adrien.chevalier@conix.fr

Don’t hesitate to contact us on twitter or by email.