Killing RATs with an Incident Response Framework

Adrien Chevalier

Robinson Delaugerre
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…)

May 17th 2013

NoSuchCon
Robinson
@Rob_OEM

Adrien
@00_ach

May 17th 2013
NoSuchCon

Introduction
First time speaking, please be gentle...
Study of traces of activity left on computer systems and infrastructure
Retrieval of traces erased by malicious users on computer systems...
Incident response

Fuck it, we’ll do it live!
Incident response

Ninjas

When u see them comin', it's already too late
Incident response

May 17th 2013

NoSuchCon

Cats: All your base are belong to us.
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!
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.
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
“Who are our enemies? Who are our friends? This is a question of the first importance”

--Sun Tzu
Attacker methodology

1. Planning
2. Payload Introduction
3. Command and Control
4. Footprint Expansion
5. Target identification
6. Attack Event
7. Retreat and Removal

Initial Recon
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Recon
Maintain Presence
Move Laterally
Complete Mission
Attacker methodology

Planning and recon
Intrusion
Privilege escalation
Perimeter expansion
Search for valuable assets
Asset exploitation
Post-Exploitation

Interaction with the victim
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

Detection
Compromised perimeter evaluation
Valuable assets identification
Remediation planning
Response
Remediation
Post-incident forensics
Normal operations

Interaction with the attacker
All together

Planning and recon | Intrusion | Privilege escalation | Perimeter expansion | Search for valuable assets | Asset exploitation | Post-Exploitation

Victim’s danger zone | Victim’s incertitude zone | Attacker’s comfort zone | Attacker’s incertitude zone

Attacker wants to maximize this | Victim/Attacker interaction | Victim wants to minimize this

Detection | Compromised perimeter evaluation | Valuable assets identification | Remediation planning | Response | Remediation | Post-incident forensics | Normal operations

May 17th 2013
NoSuchCon
Planning and recon | Intrusion | Privilege escalation | Perimeter expansion | Search for valuable assets | Asset exploitation | Post-Exploitation

Attacker/victim interaction | Victim/Attacker interaction

timeline

Remediation cost

Detection | Compromised perimeter evaluation | Valuable assets identification | Remediation planning | Response | Remediation | Post-incident forensics | Normal operations

May 17th 2013  NoSuchCon  24
Incident response

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

Surveillance across the whole perimeter

Assessment of compromised assets

Traceability of the attacker’s actions (in real time?)

That’s what Arsenic is for!
Incident response

The Arsenic Framework
“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

May 17th 2013 NoSuchCon
The Arsenic Framework

Network traffic signatures → Compromised host analysis → Network traffic dissection
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
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.
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
“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
La liste est vide.
Process overview

Network traffic signatures → Compromised host analysis → Network traffic dissection
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)
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

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> capture
Arsenic> 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
Process overview

Network traffic signatures → Compromised host analysis → Network traffic dissection
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

May 17th 2013

NoSuchCon
Process overview

Network traffic signatures → Compromised host analysis → Network traffic 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
Wrapping up
“Be resolute, fear no sacrifice and surmount every difficulty to win victory.”

--Sun Tzu
In the Framework, every attacker action is journalized.

You can query the timeline database.

Export data.

Traceability out of the box!
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…)

May 17th 2013

NoSuchCon
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.

May 17th 2013
NoSuchCon