

Bedep has raised its game vs Bot Zombies

 malware.dontneedcoffee.com/2016/04/bedepantiVM.html

2016-04-14 - Deception



Simulacra & Simulation - Jean Baudrillard

Featured in Matrix

Bedep could be described as a fileless loader with a resident module that can optionally perform AdFraud. It's intimate to Angler EK and appeared around August 2014.

On the 2016-03-24 I noticed several move in Bedep.



Angler infecting a VM and integrating it into an instance of Bedep botnet
2016-03-24

No more variable in the URI (as several month before), the protocol Key changed and in most of my manual checks, all threads were sending a strange payload in the first stream.

2ko size for Win7 64bits :

80eb8a6aba5e6e70fb6c4032242e9ae82ce305d656b4ed8b629b24e1df0aef9a



Popup shown by the first payload from Bedep Stream - Win7
(in the background Angler Landing)

48ko size for WinXP 32bits:

[a0fe4139133ddb62e6db8608696ecdaf5ea6ca79b5e049371a93a83cbcc8e780](#)



Popup shown by the first payload from Bedep Stream - WinXP

Looking at my traffic I thought for some time that one of the Bedep instances was split in two.

Then I understood that I got different result on my "manually" driven VM (on VMWare ESXi) and my automated Cuckoo driven one (on VirtualBox). I suspected it was related to hardening, as this is one of the main difference between those two systems.

And I got confirmation. Here is an example on a GooNky ([1] [2] [3]) malvertising traffic in Australia :



A VM not hardened enough against Bedep got redirected to a "decoy" instance of Bedep
that i will refer as :
Bedep "Robot Town" - 2016-04-12

Now look what i get instead with a VM that is not spotted as is:



Same Angler thread - VM not detected. 1st Stream get Vawtrak
2016-04-12

(*Vawtrak in that stream*

[d24674f2f9879ee9cec3eeb49185d4ea6bf555d150b4e840407051192eda1d61](#))

I am not skilled enough to give you the list of checks Bedep is doing. But here is one of them spotted by Cuckoo :



Bedep doing some ACPI checks

I think there are multiple level of checks. Some resulting in Bedep not trying to contact the C&C, some where the positive check end up with a different seed for the Bedep DGA redirecting spotted machines in a dedicated instance.

This is quite powerful :

- the checks are made without dropping an executable.
- if you don't know what to expect it's quite difficult to figure out that you have been trapped

- there is a lot of things that operators can do with this list of known bots and initial Bedep thread ID.

One of them is for instance knowing which of the infection path are researcher/bots "highway" :



Illustration for Bedep "Robot Town" from an "infection path" focused point of view

This could be just a move to perform different tasks (AdFraud only (?)) on VMs, but my guess is that this Bedep evolution on 2016-03-24 is a fast reaction to this [Proofpoint Blog](#) from 2016-03-18 which show how Bedep threads are additional connectable dots.

Sharing publicly is often a difficult decision. The question is which side will benefit the most from it, in the long time.

For researchers:

In the last 3 weeks, if your VM have communicated with :

95.211.205.228 (*which is a Bedep ip from end of 2015 reused*) || (85.25.41.95 && http.uri.path "ads.php?sid=**1901**") and you are interested by the "real payload" then you might want to give [PAfish](#) a run.

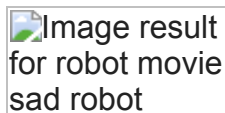


Image result
for robot movie
sad robot

Marvin - Paranoid Android

On the other hand, any of your VM which has communicated with 104.193.252.245 (Bedep "standard" 18xx 19xx instance) since the 24 of March is hardened enough to grab the real payload.

[Edits]

- Removed the AU focused mention on the Vawtrak. I have been told (Thanks !) it's US focused. Got geo

Glitched. Maybe more about that a day or the other.

- Refine the check conditions for Researcher. IP 85.25.41.95 and sid=1901...otherwise...ok :)

[/Edits]

Acknowledgements :

Thanks [Will Metcalf](#) and [Malc0de](#) for the discussions and help on this topic

--

I'm sorry, but I must do it...Greetings to Angler and Bedep guys. ;) You are keeping us busy...and awake !

Reading :

Video Malvertising Bringing New Risks to High-Profile Sites - 2016-03-18 - Proofpoint
Bedep's DGA: Trading Foreign Exchange for Malware Domains - 2015-04-21 - Dennis Schwarz - ArborSert
Angler EK : now capable of "fileless" infection (memory malware) - 2014-08-30
Modifying VirtualBox settings for malware analysis - 2012-08-23 - Mikael Keri