
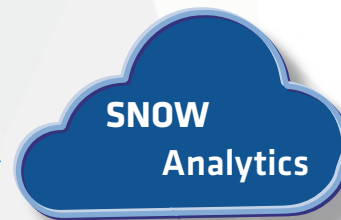


# Feedback\_loop\_step1

## STAGE 0 BACKDOOR



	<b>STRANGE DOMAIN NAMES IP ADDRESSES</b>
	198.48.2.9 198.48.2.6 f152.no-ip.biz f1fw.no-ip.com
<b>ACROREEL.EXE</b>	



1. During the baselining phase at a new client, Arc4dia analysts observed odd behaviour from what looked like an Acrobat Reader component.
2. The executable in question, located within the directory of a legitimate install, was named extremely closely to other various components in the directory. But when observed being launched sometimes contained IP addresses or Domains.
3. No other copy of this executable was anywhere else on the network, or documented on the Internet.
4. An analyst fetched the file and began reverse engineering it. It was clearly a very simple Stage 0 implant without any functionality other than very basic recon and the ability to download additional components from its command and control.



## Feedback\_loop\_step2

1. Having difficulty believing this presence was alone on the network, the analyst began digging deeper, eventually finding multiple other versions of the implant, adapted to other legitimate software throughout the network.
2. The implants had been present for over a year, but were never actually activated to download additional packages, or to execute additional recon. They were still able to communicate to their command and control.

ACROREEL.EXE



**SNOW Analytics**  
with time zone analysis

## Feedback\_loop\_step3

1. A handful of interactive sessions were detected over time, eventually providing enough data to do an analysis mapping the activity onto a time zone, days of the week and holidays of a specific country.
2. In discussion with the client, we eventually cleaned up the presence onto the network.
3. The final analysis lead us to determine that the only logical purpose for the implants were “prepositioning”, meaning waiting for the day they could be of some use, by delivering a payload yet unknown with goals unknown.

**Security problems can be hidden even in files which other solutions are not able to find as malicious, Arc4dia is able to track them.**