Animals in the APT Farm

securelist.com/animals-in-the-apt-farm/69114

By GReAT

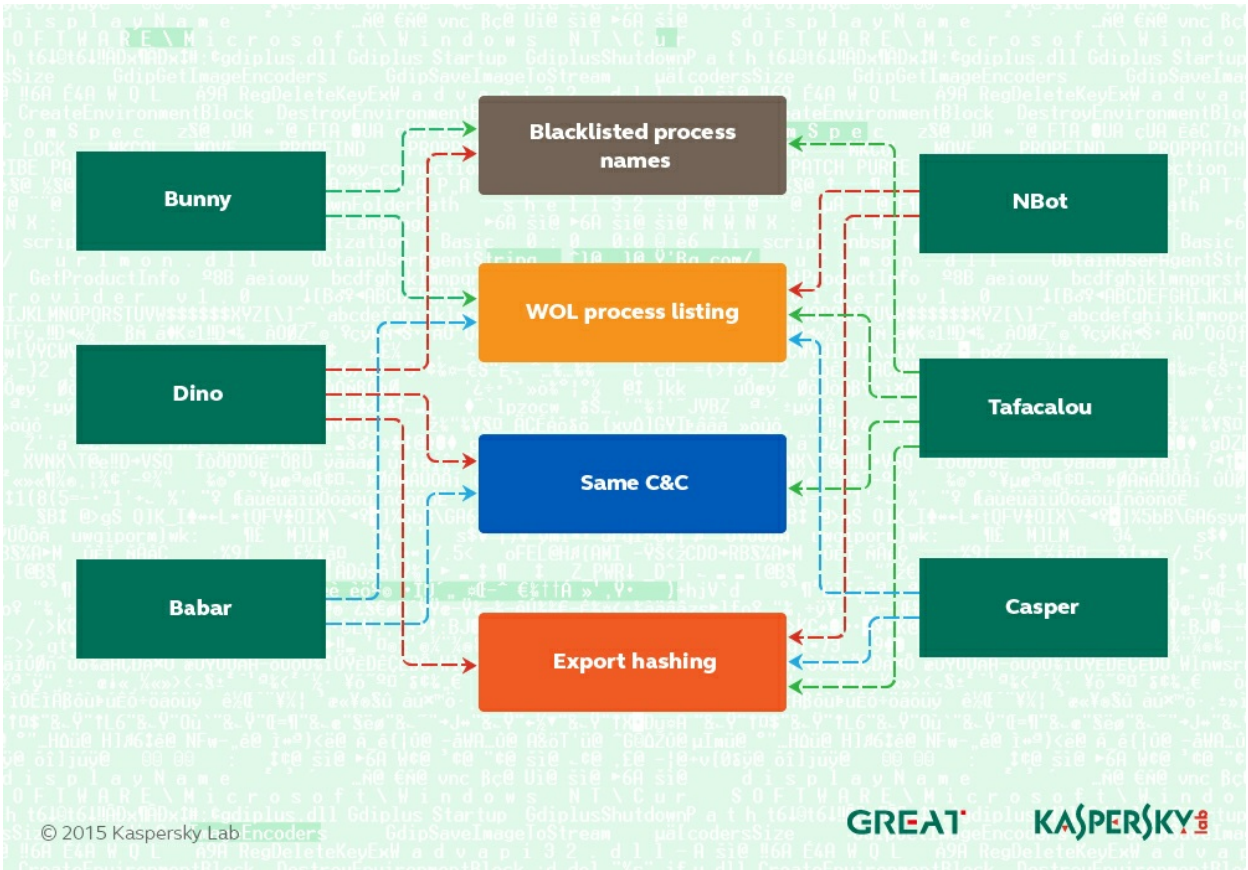
In 2014, researchers at Kaspersky Lab discovered and reported on three zero-days that were being used in cyberattacks in the wild.

Two of these zero-day vulnerabilities are associated with an advanced threat actor we call **Animal Farm**. Over the past few years, Animal Farm has targeted a wide range of global organizations. Victims include:

- Government organizations
- Military contractors
- Humanitarian aid organizations
- Private companies
- Journalists and media organizations
- Activists

Our colleagues at Cyphort, G-DATA and ESET have recently published blogs about Bunny, Casper and Babar, some of the Trojans used by the Animal Farm group.

The Farm includes several Trojans, which we have grouped into six major families:



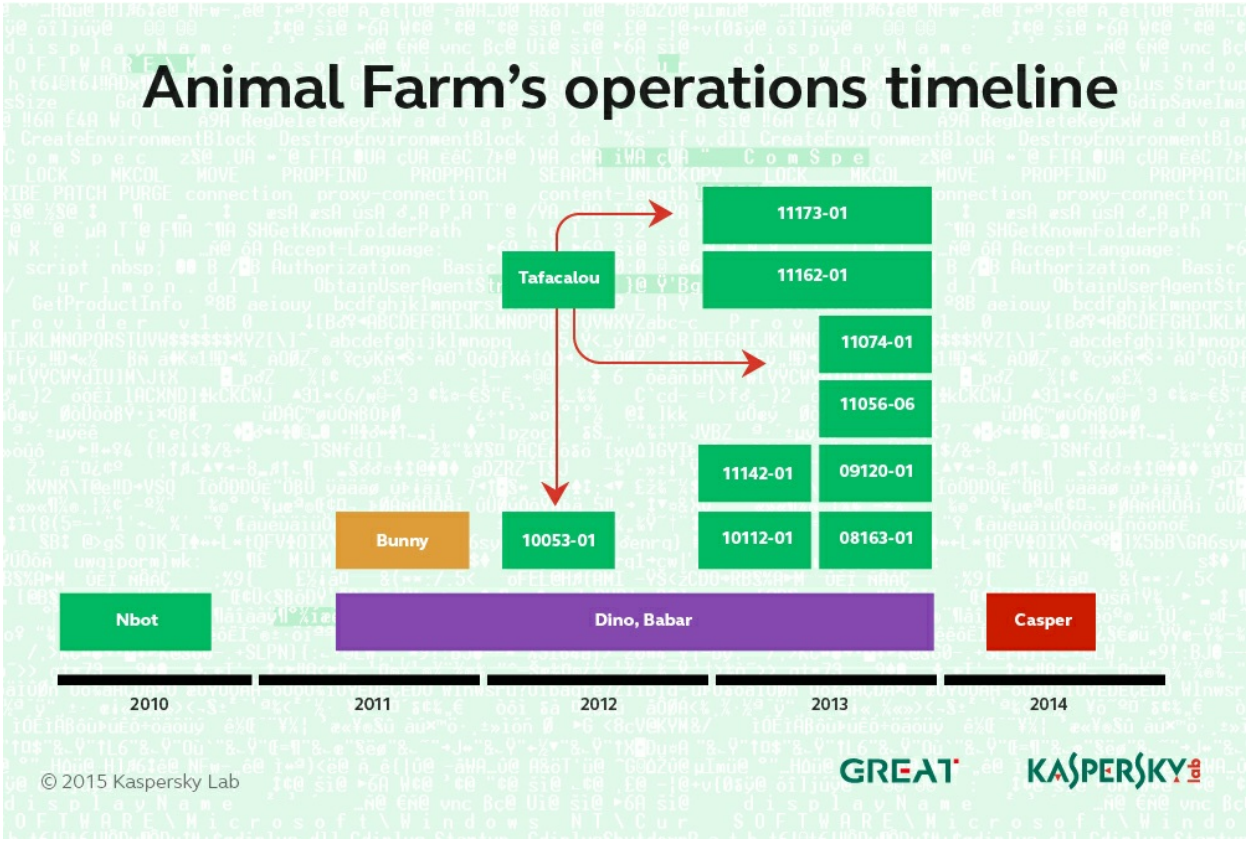
Here's a brief description of the animals in the farm:

- **Bunny** – an old "validator"-style Trojan used with a PDF zero-day attack in 2011.

- **Dino** – a full-featured espionage platform.
- **Babar** – the most sophisticated espionage platform from the Animal Farm group.
- **NBot** – malware used in a botnet-style operation by the group. It has DDoS capabilities.
- **Tafacalou** – a validator-style Trojan used by the attackers in recent years. Confirmed victims get upgraded to Dino or Babar.
- **Casper** – the most recent "validator"-style implant from the Animal Farm group.

The group has been active since at least 2009 and there are signs that earlier malware versions were developed as far back as 2007.

Over the years we have tracked multiple campaigns by the Animal Farm group. These can be identified by a specific code found either in the malware configuration or extracted from the C&C logs.



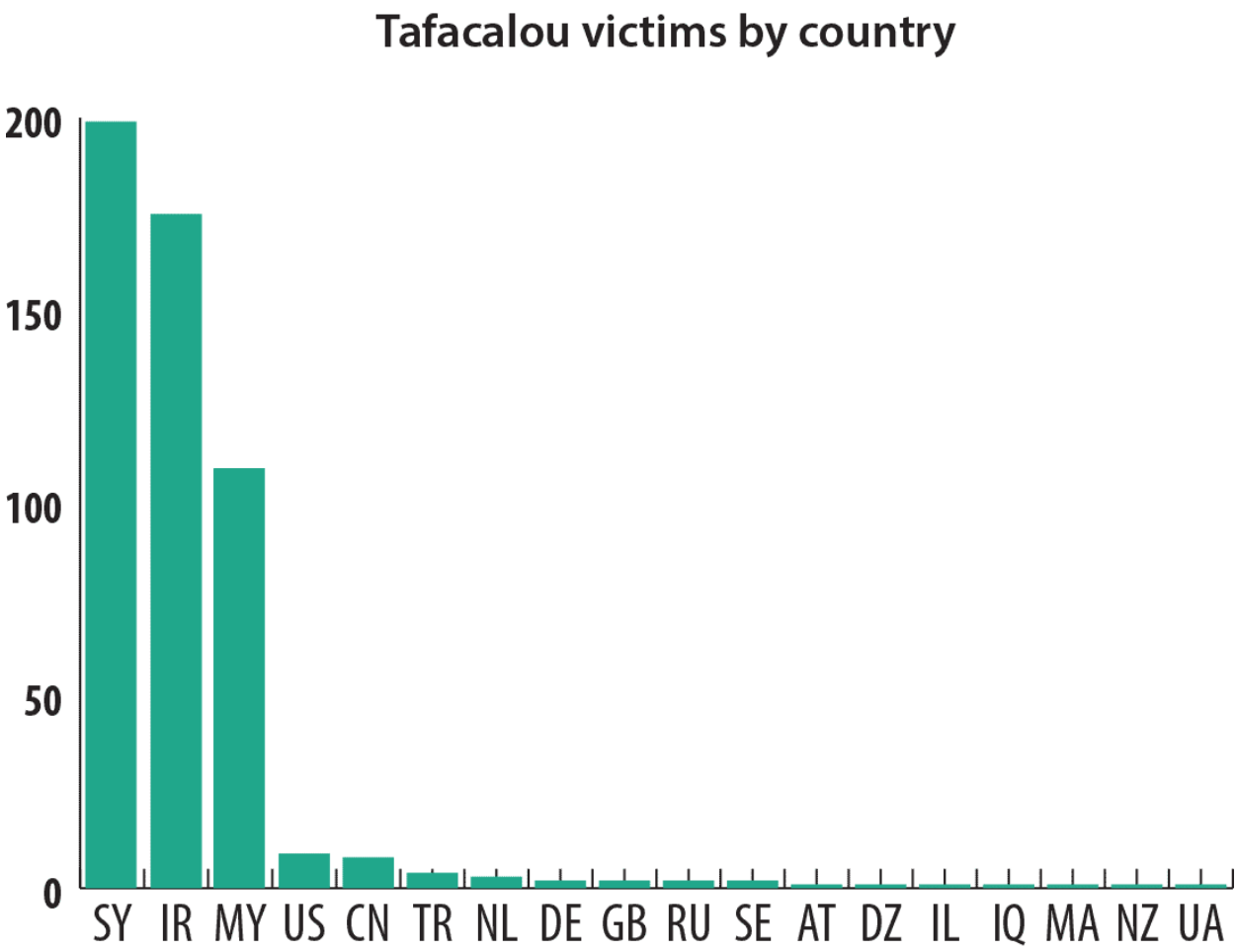
Most recently, the group deployed the Casper Trojan via a watering-hole attack in Syria. A full description of this zero-day attack can be found in this blog post by Kaspersky Lab's Vyacheslav Zakorzhevsky.

In addition to these, the Animal Farm attackers used at least one unknown, mysterious malware during an operation targeting computer users in Burkina Faso.

KSN & Sinkholing statistics

During the investigation we sinkholed a large number of C&C servers used by the Animal Farm group. This allowed us to compile a comprehensive picture of both targets and victims.

The malware known as Tafacalou (aka “TFC”, “Transporter”) is perhaps of greatest interest here, because it acts as an entry point for the more sophisticated spy platforms Babar and Dino. Based on the Tafacalou infection logs, we observed that most of the victims are in the following countries: Syria, Iran, Malaysia, USA, China, Turkey, Netherlands, Germany, Great Britain, Russia, Sweden, Austria, Algeria, Israel, Iraq, Morocco, New Zealand, Ukraine.



What does “Tafacalou” mean?

“Tafacalou” is the attacker’s internal name for one of the validator (1st stage) Trojans. We tried various spellings of this word to see if it means anything in a specific language, and the most interesting option is one with its origins in the Occitan language: “Ta Fa Calou.”

The expression “Fa Calou” is the French interpretation of the Occitane “Fa Calor” which means “it’s getting hot” (see http://ejournaux.blogspot.com/2008/07/la-langue-occitane-et-ses-quelques.html). ‘Ta Fa Calou” could therefore be taken to mean “so it’s getting hot” based on the Occitan language.

According to Wikipedia: ‘*Occitan is a Romance language spoken in southern France, Italy’s Occitan Valleys, Monaco, and Spain’s Val d’Aran; collectively, these regions are sometimes referred to unofficially as “Occitania”.*

Note: A detailed technical report on Animal Farm is available to customers of Kaspersky Intelligent Services. For more information, contact intelreports@kaspersky.com