Animal Farm APT and the Shadow of French Intelligence

resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/

Threat Intelligence
July 8, 2015 by **Pierluigi Paganini**

Babacar and Casper

Almost every government is working to improve its cyber-capabilities. The majority of them already have in their arsenal powerful espionage malware and hacking platforms. We read about the techniques and tactics implemented by a number of APT groups from China, Russia, Iran and belonging to the Five Eyes (US, UK, Australia, New Zealand, Canada) Intelligence Agencies.

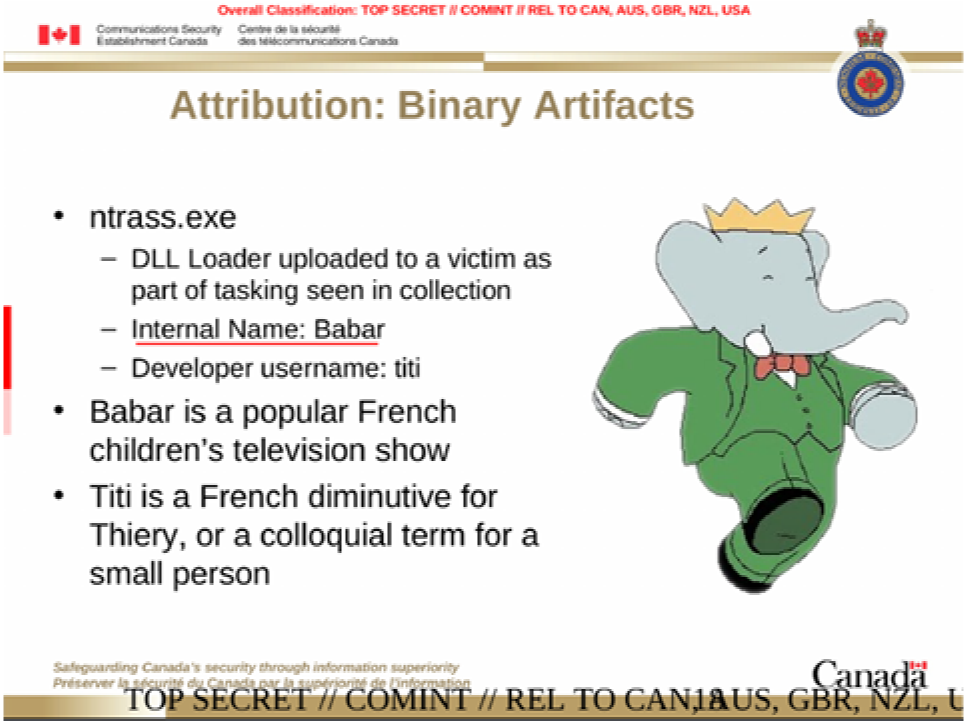
Early in 2015, security researchers detected a new strain of malware, dubbed Babar, that they consider as a malicious code developed by French intelligence. According to the experts, Babar malware was used by the General Directorate for External Security (DGSE), which is the France's external intelligence agency, for surveillance and cyber espionage purposes.

The spyware is also dubbed Snowglobe by the Canadian Intelligence agency CSEC, it was spyware designed to collect victims' e-mails.

The General Directorate for External Security is controlled by the French ministry of Defense. It is in charge of intelligence activities for the national security. The Casper malware was discovered by Canadian malware researchers that linked it to the French Intelligence.

Babar is considered by the experts powerful spyware that is capable of eavesdropping on online conversations held via popular messaging platforms, including Skype, MSN and Yahoo messenger, as well as logging keystrokes and monitoring the activity of the victim on the Internet.

Security experts have collected evidence of the use of Babar to spy on several Iranian organizations, including nuclear research institutes and universities. Babar was also used by threat actors to spy on European financial institutions. The name Babar first appeared in one of the documents leaked by the NSA whistleblower Edward Snowden, the slides were made by the Canadian intelligence agency and linked Babar to the French Government.



Overall Classification: TOP SECRET // COMINT // REL TO CAN, AUS, GBR, NZL, USA

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

Attribution: Binary Artifacts

- ntrass.exe
  - DLL Loader uploaded to a victim as part of tasking seen in collection
  - Internal Name: Babar
  - Developer username: titi
- Babar is a popular French children's television show
- Titi is a French diminutive for Thiery, or a colloquial term for a small person

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

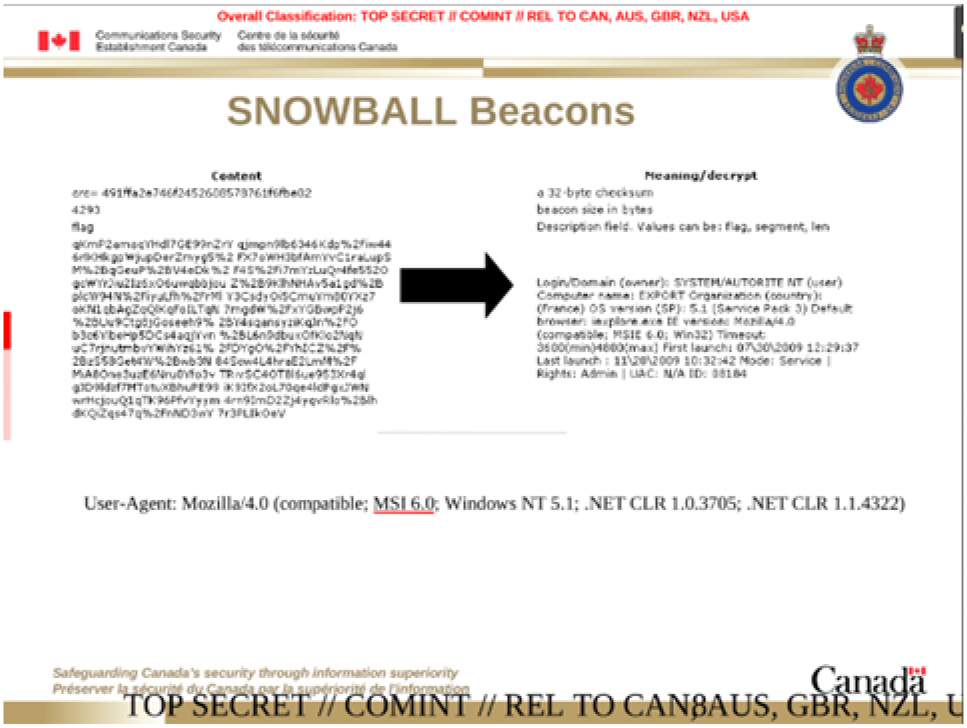
Canada

TOP SECRET // COMINT // REL TO CAN, AUS, GBR, NZL, U 18

Figure 1 – CSEC slides leaked by Snowden

The documents confirm the presence of the France's intelligence services behind an e-mail spying campaign started in November 2009 that was aimed at Iran's nuclear program. According to the French newspaper Le Monde, the hackers hit many other targets, including a Canadian media outlet.

"Canadian secret service suspect indeed their French counterparts of being behind a vast computer piracy operation, which would have begun in 2009 and still continue thanks to a spy implant," states *Le Monde.*



Overall Classification: TOP SECRET // COMINT // REL TO CAN, AUS, GBR, NZL, USA

Communications Security Establishment Canada   Centre de la sécurité des télécommunications Canada

SNOWBALL Beacons

Content

```
crc= 491ffa2e746f245260857876lf6fbe02
4293
flag
qKmP2amaqYhdl7GE99nZrY qjmpn9Ib6346Kdp%2Fiw44
6rlKHkgp%jupDerZmyg5%2 fX7oWH3bfAmYvCiraLupS
M%2BqGeuP%2BV4eDk%2 f4S%2Fi7mYzLuQn4fe552O
gcWYJu2Iz6xO6uwqbbjou Z%2B9KhNHAv5a1pd%2B
plcW94N%2FiyuLfh%2FrMl Y3CsdyO6CmyYm80YXz7
oKN1gbAgZoQKqFo1LTgN 7mgdW%2FxYGbwpF2j6
%2BUu9CtgdjGoseeh9% 2BY4sqansyziKqJn%2FO
b3c6YlbeHp5DCs4aqjYvn %2BL6n0dbuxOfKlo2fiqN
uC7rjnutmbvYWihYz61% 2FDYgO%2FYhIC2%2F%
2Bz55BGe6W%2Bwb3N 64Sow4L4hraE2Lmf8%2F
MiA8One3uzE6Nru0Yfo3v TRvSC4OT8l6ue953Xr4gl
g3D9ldzf7MTotuXBhuPE99 iK9IfX2oL70qe4ldFgxJWN
wrHcjouQ1qTK96PfvYyym 4rn9ImD2Zj4yqvRlo%2B8h
dKQiZqs47q%2FnND3wY 7r3PLIkOeV
```

Meaning/decrypt

```
a 32-byte checksum
beacon size in bytes
Description field. Values can be: flag, segment, len

Login/Domain (owner): SYSTEM/AUTORITE NT (user)
Computer name: EXPORT Organization (country):
(France) OS version (SP): 5.1 (Service Pack 3) Default
browser: iexplore.exe IE version: Mozilla/4.0
(compatible; MSIE 6.0; Win32) Timeout:
3600(min)4800(max) First launch: 07\30\2009 12:29:37
Last launch : 11\28\2009 10:32:42 Mode: Service |
Rights: Admin | UAC: N/A ID: 38184
```

User-Agent: Mozilla/4.0 (compatible; MSI 6.0; Windows NT 5.1; .NET CLR 1.0.3705; .NET CLR 1.1.4322)

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET // COMINT // REL TO CAN, AUS, GBR, NZL, U

Figure 2 -Canadian -Intelligence – Operation Snowglobe

The presentation concludes with the revelation that CSEC agency has also detected a more sophisticated version of the Babar agent, dubbed Snowman, which is under analysis.

The slides were prepared in 2011 and shared among the Intelligence agencies belonging to the Five Eyes.

Snowglobe was detected in operation against targets in Canada, Spain, Greece, Norway, Ivory Coast and Algeria, but the main target appeared to be in Iran. The hackers were focusing on the country's foreign ministry, the Atomic Energy Organization of Iran, the Iran University of Science and Technology and two Tehran schools heavily involved in nuclear research, Malek-E-Ashtar University of Technology and Imam Hussein University.

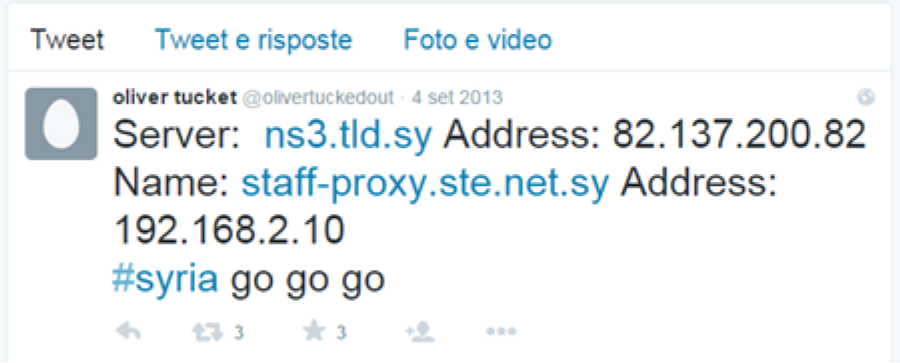
The authors of the slides speculate that the French intelligence targeted Greece because it is "possibly associated with [the] European Financial Association," and also Algeria and Ivory Coast because they are former French colonies.

"The memo outlines circumstantial evidence that led CSEC to conclude that Snowglobe was a French intelligence operation." Continues LeMonde.

The researcher at CSEC are skeptical of possible financial motivation of the attackers, the exclude cyber-crime rings as the responsible of the campaign. Analysts noted that the malware author left his username amid the computer coding: *"Titi," a French diminutive or "colloquial term for a small person."*

On March 2015, malware researchers spotted a new strain of malware, dubbed Casper, which is spyware designed to track Internet users for surveillance purpose. The malware was hosted on a compromised website belonging to the Syrian Government (at http://jpic.gov.sy/) it was a complex agent able to exploit two zero-day flaws to infect victims.

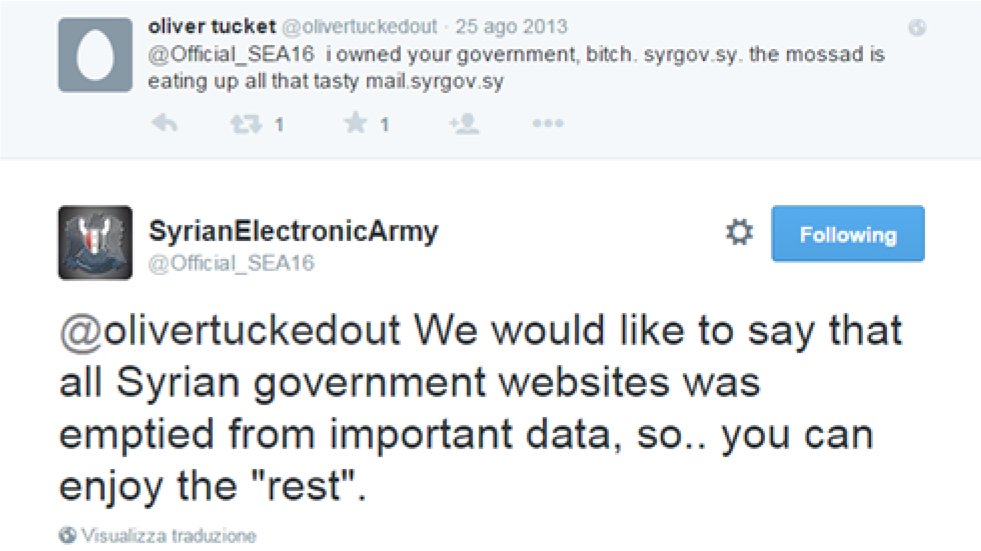
Both the exploits were hosted on a Syrian website, launched in 2011 by the Syrian Ministry of Justice that was designed as an online platform for citizens to complain about law and order violations. Experts believe it was designed to target Syrian dissidents complaining about the government. The site was hacked in September 2013 by a group using the twitter account @olivertuckedout that raised the reaction of the hacking group known as the Syrian Electronic Army.



oliver tucket @olivertuckedout · 4 set 2013

Server: ns3.tld.sy Address: 82.137.200.82
Name: staff-proxy.ste.net.sy Address: 192.168.2.10
#syria go go go

Figure 4 – olivertuckedout announced the hack of the Syrian Server


oliver tucket @olivertuckedout · 25 ago 2013

@Official_SEA16 i owned your government, bitch. syrgov.sy. the mossad is eating up all that tasty mail.syrgov.sy

SyrianElectronicArmy
@Official_SEA16

@olivertuckedout We would like to say that all Syrian government websites was emptied from important data, so.. you can enjoy the "rest".

Figure 5 – SEA replied @olivertuckedout

"In mid-April we detected two new SWF exploits. After some detailed analysis it was clear they didn't use any of the vulnerabilities that we already knew about. We sent the exploits off to Adobe and a few days later got confirmation that they did indeed use a 0-day vulnerability

that was later labeled as CVE-2014-0515. The vulnerability is located in the Pixel Bender component, designed for video and image processing." reported an analysis published by Kaspersky Lab.

The experts at Kaspersky noticed that both exploits were professionally designed, but while one of them is standard and can infect practically any vulnerable computer, the second exploit (include.swf) only works on computers where Adobe Flash Player 10 ActiveX and Cisco MeetingPlace Express Add-In are installed. The authors used the Flash Player Pixel Bender component, which Adobe no longer supports, as the attack vector and remain active for longer. This means that threat actors were running surgical espionage campaigns.

Casper malware was used by threat actors in the wild to target systems, spy on them, and drop other advanced persistent malware.

"According to the report, which Motherboard reviewed in advance, Casper was hosted on a hacked Syrian government website in April of last year. The incident caught the attention of some security researchers because the attackers used two zero-day vulnerabilities to infect victims" states a blog post published by the Motherboard news portal.

The report published by Motherboard confirms that the Casper malware was designed by a French APT group, likely a state-sponsored hacking crew.

Casper was used to run several espionage campaigns over the last few years and its authors had access to two zero-day exploits that were used in a sample detected by malware researchers in April 2014.

Casper is not common malware; security researchers speculate it requested a significant effort for its development in term of resource and financial investment, a prerogative of Government-built malware.

Babar, Casper, and Evil Bunny have the same root

Malware specialists have discovered several similarities between the source code of Casper and Babar, the researchers speculate that they were "likely" developed by the same team of coders. The experts discovered much more, both agents appear as the product of a common hacking platform developed by French Intelligence that was used to distribute other malicious code, including the Evil Bunny. In December 2014, the security firm Cyphort Labs firm detected another sophisticated malware dubbed EvilBunny that implements a very complex evasion technique.

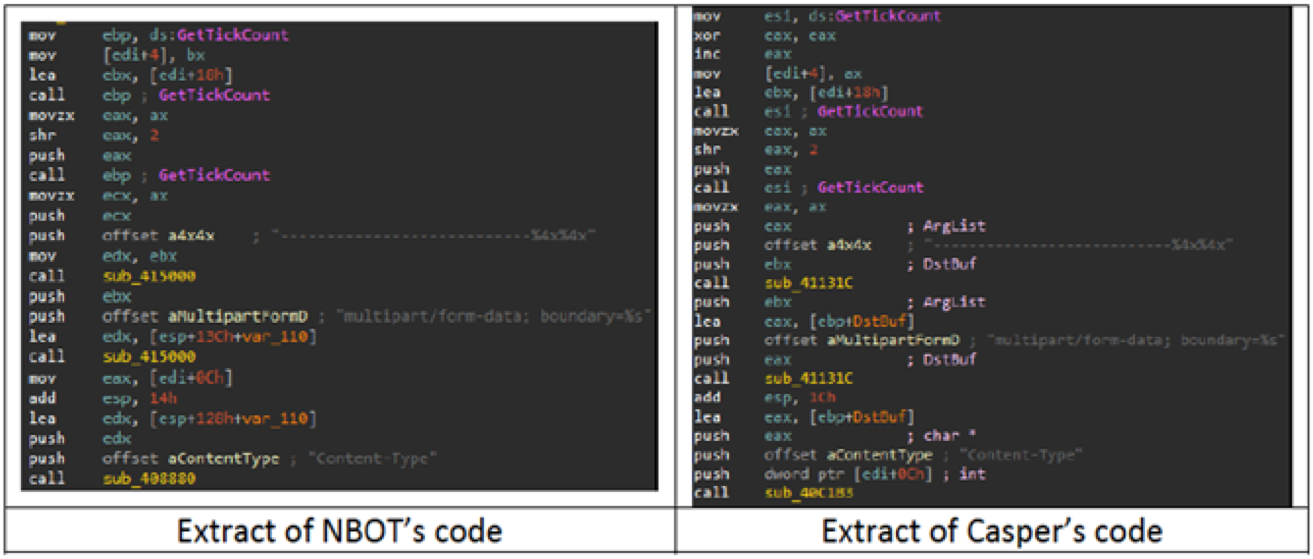
To establish that the same development team has worked on Bunny, Babar, and Casper the experts focused the analysis on the identification of unusual stubs of code or algorithms implemented by all the malware in the arsenal of the Animal Farm APT.

EvilBunny is written in C++ and is able to detect installed antivirus and other defensive solutions. It includes a Lua 5.1 interpreter, which allows the spyware to execute Lua scripts and change its behavior at runtime.

The experts discovered that EvilBunny is able to receive commands from the C&C server at least in three different ways, via HTTP, through a downloaded database file or as a scheduled task.

The EvilBunny malware was initially delivered through a malicious PDF document, exploiting CVE-2011-4369. Once compromised the target the malware is loaded onto the system and infects the PC with EvilBunny malware.

"The malware is dubbed 'EvilBunny' and is designed to be an execution platform for Lua scripts injected by the attacker." According to the new report written by Joan Calvet, a malware researcher at anti-virus maker ESET, the EvilBunny together with other hacking tools, like the NBOT tool, suggested ties to the French Intelligence.



```
mov     ebp, ds:GetTickCount
mov     [edi+4], bx
lea     ebx, [edi+18h]
call    ebp ; GetTickCount
movzx   eax, ax
shr     eax, 2
push    eax
call    ebp ; GetTickCount
movzx   ecx, ax
push    ecx
push    offset a4x4x    ; "--------------------------%4x%4x"
mov     edx, ebx
call    sub_415000
push    ebx
push    offset aMultipartFormD ; "multipart/form-data; boundary=%s"
lea     edx, [esp+13Ch+var_110]
call    sub_415000
mov     eax, [edi+0Ch]
add     esp, 14h
lea     edx, [esp+128h+var_110]
push    edx
push    offset aContentType ; "Content-Type"
call    sub_408880
```

Extract of NBOT's code

```
mov     esi, ds:GetTickCount
xor     eax, eax
inc     eax
mov     [edi+4], ax
lea     ebx, [edi+18h]
call    esi ; GetTickCount
movzx   eax, ax
shr     eax, 2
push    eax
call    esi ; GetTickCount
movzx   eax, ax
push    eax             ; ArgList
push    offset a4x4x    ; "--------------------------%4x%4x"
push    ebx             ; DstBuf
call    sub_41131C
push    ebx             ; ArgList
lea     eax, [ebp+DstBuf]
push    offset aMultipartFormD ; "multipart/form-data; boundary=%s"
push    eax             ; DstBuf
call    sub_41131C
add     esp, 1Ch
lea     eax, [ebp+DstBuf]
push    eax             ; char *
push    offset aContentType ; "Content-Type"
push    dword ptr [edi+0Ch] ; int
call    sub_40C183
```

Extract of Casper's code

Figure 6 – Comparison between NBOT code and Caper code

"We have reasons to believe that French intelligence has been using—or is even still using—at least four different malware families," Marion Marschalek, another researcher who worked with Calvet and Paul Rascagneres in investigating the malware, told Motherboard.

The Animal Farm is a very prolific malware factory; Casper is just the latest tool in order of time belonging to the arsenal of the Animal Farm group. Security researchers believe Casper has been active since at least 2009 or 2010.

"Other security researchers agree that Casper, perhaps named after the famous cartoon "friendly ghost," was likely created by the French government and its spying agency the General Directorate for External Security (DGSE). They refer to the hacking group as the

"Animal Farm" because of each malware's animal-like and cartoon-inspired names." continues the Motherboard.

Experts at ESET firm collected the following evidence that suggests the involvement of the same development team for the malware used by the Animal Farm group:

- Casper hides its calls to API functions by using a hash calculated from the functions' names, rather than the names themselves, a technique implemented by other malware on the Animal Farm, including NBOT and Babar.
- Casper, Bunny, Babar, and NBOT gather information about the running antivirus solution in a similar way. The computer the SHA-256 hash of the first word of the antivirus name.
- *Casper generates delimiters for its HTTP requests by filling a specific format string with the results of calls to the GetTickCount API function. The same code is present in some NBOT samples.*

Costin Raiu, the director of the Global Research and Analysis Team at Kaspersky Labs, confirmed that his company has been tracking the Animal Farm since 2013, the popular expert has no doubts about the involvement of a government for the development of the malicious code used by the APT group.

"When you have such a large-scale operation going on for several years using multiple zero-days without any kind of financial outcome,"Raiu told Motherboard, "it's obvious that it's a nation-state sponsored—it has to be."

France's Defense Ministry did not respond to Motherboard's requests for comment.

Another character from the cartoons … this time it's Dino Malware

Security experts at ESET have recently discovered a new sophisticated malware dubbed Dino that experts believe linked to the arsenal of the Animal Farm ATP group.

The researcher that discovered and analyzed Dino, the new strain of malware used by the so-called "Animal Farm", explained that it was detected for the first time in March 2014 when French media released a new collection of Snowden's slides describing a campaign dubbed "Operation Snowglobe."

Several security firms, including ESET, Cyphort and G DATA, have analyzed in details the malware belonging the Animal Farm APT. Below a list of the reports they published:

- Casper, a stealthy first-stage implant, documented by ESET in last March
- Bunny, a Lua-based backdoor, documented by Marion Marschalek (Cyphort)
- Babar, an espionage platform, also analyzed by Marion Marschalek

The arsenal of the Animal Farm includes Babar, EvilBunny, and Casper, but the list is long and NBot, Tafacalou (TFC / Transporter) and Dino are other malicious code used by the APT.

ESET published a detailed analysis of the Dino malware, the ESET researcher Joan Calvet has detected a single sample of Dino in the wild that was used in an attempt to infect a target in Iran in 2013.

“Dino is so hard to find because the group behind the Animal Farm is really good at targeting people precisely, and we basically miss a lot of their samples,” Calvet told

Dino is a modular malware, a number of components allow it to carry out several tasks, the agent is able to execute commands sent by C2C servers and Windows batch commands.

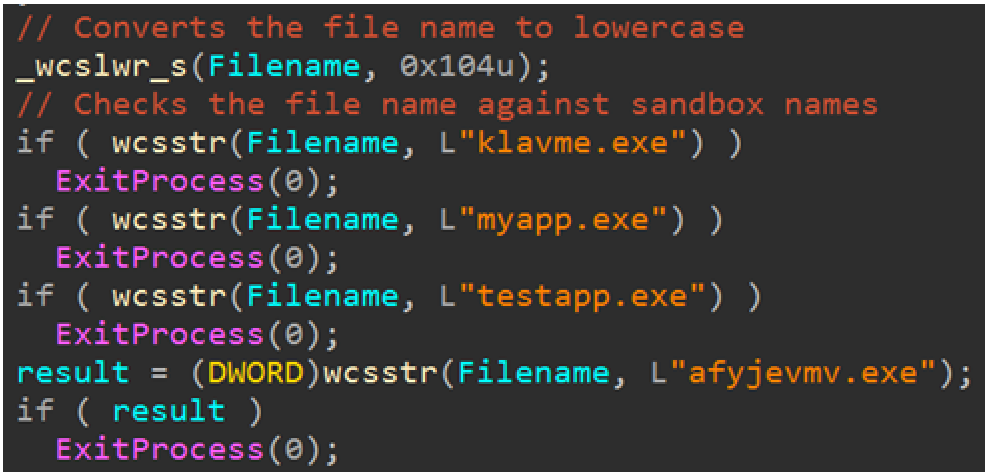
The malware is also able to search for specific files, upload files to the command and control (C&C) server, and download further files from the control architecture. The experts noticed that Dino can also schedule commands to be executed at a specified time, it is also able to kill processes and uninstall the malicious code from the infected system to avoid leave traces of its presence.

Experts at Kaspersky explained that the Tafacalou malware is used by the Animal Farm APT to serve further sophisticated spyware like Babar and Dino.

The researchers discovered several similarities between the code of the Dino malware and other threats from the Animal Farm malware families. The experts highlighted that the developers of these malware families are French speakers.

The amount of shared code between Dino and the other Animal Farm malware is significant and leaves no doubt that Dino belongs to Animal Farm’s arsenal. Below the list of shared features provided by the experts at ESET:

> *At the very beginning of Dino execution, the current process name is checked against process names used by some sandboxes, the feature allows it to avoid the execution in testing environments.*



```
// Converts the file name to lowercase
_wcslwr_s(Filename, 0x104u);
// Checks the file name against sandbox names
if ( wcsstr(Filename, L"klavme.exe") )
  ExitProcess(0);
if ( wcsstr(Filename, L"myapp.exe") )
  ExitProcess(0);
if ( wcsstr(Filename, L"testapp.exe") )
  ExitProcess(0);
result = (DWORD)wcsstr(Filename, L"afyjevmv.exe");
if ( result )
  ExitProcess(0);
```

Figure 7 – Dino checks to avoid execution in virtualized environments.

- *The call to API functions is hidden with the same hashing mechanisms implemented by other malware on the Animal Farm APT. The hash is calculated from the function's name and used to look for the address of the API function.*
- *The Dino's custom file system – the so-called ramFS – is present in several droppers used by Animal Farm.*
- *The output of Dino's sysinfo command looks like an updated version of the "beacon" from the SNOWBALL implant described in the leaked CSE slides – part of operation SNOWGLOBE, which led to the discovery of Babar:*

"Dino's binary contains a resource whose language code value is 1036. The original purpose of this language code is to allow developers to provide resources (menus, icons, version information…) for*different locations in the world in the corresponding language. Interestingly, when a developer does not manually specify the language code, the compiler sets it to the language of the developer's machine. So, which language corresponds to the value 1036, or 0x40c in hexadecimal? French (France)." states the report published by the ESET.*

Another anomaly discovered by researchers is the presence in the file path of the word "arithmetique," which is French for "arithmetic."arithmetique," which is French for "arithmetic."

Experts at ESET explained that the Dino malware, differently for other codes used by the Animal Farm APT, doesn't implement sophisticated anti-analysis techniques.

Conclusion

The information presented in this post reviews the findings of the reports prepared by the principal security firms that confirm the existence of a state-sponsored hacking group behind the Animal Farm APT.

All the malicious codes share a large amount of code and appear developed by the same pool of experts. The malware is very sophisticated and their development requested for sure a significant effort. The analysis of Babar in the documents prepared by the Canadian CSEC indicates that the group is active at least since 2009, and the availability of zero-day exploits is another element that led the experts to consider the Anima Farm a Government-backed actor.

In the following table explains the principal malware that security experts linked to the group of Animal Farm.

Malware	Function	Further info

Casper	Stealthy first-stage implant	Casper was used against Syrian targets in April 2014, which makes it the most recent malware from this group publicly known at this time. Casper has been active since at least 2009 or 2010.
Evil Bunny	Backdoor	The malware is written in C++, multi-threaded, aims to detect installed anti-virus- and firewall solutions and accepts a vast number of different control commands.
Babar	Spyware that infects Windows desktop machines and exfiltrates data, including instant messenger conversations, browsers, and office application data.	The security firm Cyphort Labs firm detected it in December 2014. It implements a very complex evasion technique.
NBot	Backdoor	
Dino	Spyware	Dino is a modular malware, researchers discovered a number of components that allows it to carry out several tasks.
Tafacalou	Backdoor	Malware used in a first stage of attack that was used to load further malware including the Evil Bunny.

Is the France intelligence behind Animal Farm?

It’s difficult to confirm it, despite the malware share the same features, the attribution is not simple, despite many experts speculate in the involvement of the France Intelligence.

References

http://securityaffairs.co/wordpress/34462/intelligence/babar-casper-french-intelligence.html

http://securityaffairs.co/wordpress/38204/cyber-crime/dino-malware-animal-farm.html

http://motherboard.vice.com/read/meet-casper-yet-another-malware-likely-created-by-france-for-surveillance

http://www.cyphort.com/evilbunny-malware-instrumented-lua/

http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/

http://www.theglobeandmail.com/news/national/french-spy-software-targeted-canada-report/article17608109/

http://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/

http://www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html

http://www.welivesecurity.com/2015/06/30/dino-spying-malware-analyzed/

http://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/

Posted: July 8, 2015

Author

Pierluigi Paganini

VIEW PROFILE

Pierluigi is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Professor and Director of the Master in Cyber Security at the Link Campus University. He is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines.