# Inside Braviax/FakeRean: An analysis and history of a FakeAV family

0x3asecurity.wordpress.com/2015/11/30/134260124544/

By Yonathan November 30, 2015

Since September 2014 I've been seeing a FakeAV family pop up from time to time. This family is known under two names, Braviax and FakeRean. The family has been active for quite some years, it was first spotted by [S!Ri](https://twitter.com/siri_urz "S!Ri Twitter") back in April 2009. In this blogpost I will perform an analysis on the current version of this family making it's rounds online and a history of it starting back in 2009. A big thank you goes out to [S!Ri](https://twitter.com/siri_urz) for sharing some historical data on this group.
The reason why I'm releasing this article now on a group active back in January of this year is that, if you follow the timeline I show below, is that they should have reappeared around this time of year (although I haven't seen them yet).

The Braviax/Fakerean family has quite some similarities with the Tritrax (dubbed Namechanger FakeAV) family I analyzed and hunted down back in February 2014 (Post: [Analysis of the Tritax FakeAV family, their active campaign and the FakeAV social engineering kit](http://blog.0x3a.com/post/75474731248/analysis-of-the-tritax-fakeav-family-their-active)).
Braviax/Fakerean is also one constantly changing its name as you can see from a combination of screenshots made from samples starting in September 2014 until the start of January 2015:
![image]
(https://40.media.tumblr.com/bca28376345d856691adf3322a30394c/tumblr_nlm2bkOQtZ1qflx2go5_r1_540.png)

As said, back in September 2014 this new variant became active. After seeing it pass by multiple times I decided to look into it a bit. At some point I started noticing the name changes due to the fact that the website, website banner and the actual 'antivirus' names didn't match up at all, I tweeted about this on the 27th of September:

> #FakeAV website calls it ‘Rango Antivirus’, banner ‘Win XP Security’, sample run ‘A-Secure’ (https://t.co/EgYDdzDqFd) pic.twitter.com/i1amKQLsIy
>
> — Yonathan Klijnsma (@ydklijnsma)
> November 27, 2014

//platform.twitter.com/widgets.js

From this point on I started looking into this FakeAV threat some more, it started to hit quite often. Quite quickly I could pin this as one as part of the Fakerean/Braviax family and started to analyze it.

## Analysis: Spreading mechanism
We’ll start the analysis of this family with the method of how it was spread, simply by mail. Around the 18th of December 2014 fake FedEx emails began to appear, one of these carying methods of infecting victims with this FakeAV. The email looked like this:
![image]
(https://40.media.tumblr.com/83777a2a260029f791336b77ed05447f/tumblr_nlm9l2sz5h1qflx2go4_r1_1280.png)
In the emails’ attachment we find a JS file:
![image]
(https://41.media.tumblr.com/a29311709ac1ee9ab3148c19d90e1186/tumblr_nlm9l2sz5h1qflx2go5_r1_1280.png)
Inside of this script we find a large piece of obfuscated script:
![image]
(https://40.media.tumblr.com/681e7d4b1d06109e42d8329afd3e149d/tumblr_nlm9l2sz5h1qflx2go6_r1_1280.png)
If we clean it up we can see its just a simple downloader which tries to infect the user with 3 pieces of malware (shotgun approach much..):
![image]
(https://41.media.tumblr.com/2f198864b3493728355ab3919fe6a06a/tumblr_nlm9l2sz5h1qflx2go7_r1_1280.png)
From the three payloads only one is the interesting one for this article; its the Braviax/FakeRean sample. Would you want to perform a more detailed analysis (rather than the very short one below), the sample coming from this email and used further is:
[1d01611a1f88c7015c54efedacfcbc8fec55ad6de9a438087abff3be78c19901]
(https://www.virustotal.com/en/file/1d01611a1f88c7015c54efedacfcbc8fec55ad6de9a438087abff3be78c19901/analysis/)

## Quick analysis: a Braviax/FakeRean sample
Because this article is more about the history of this family rather than the specifics of the FakeAV this part will be a very(!) short analysis of the sample.
When ran the FakeAV shows the usual pop-up with information on your system being infected:

![image]
(https://36.media.tumblr.com/628a1e91dbebef773867c074d0c7c9b4/tumblr_nlm9l2sz5h1qflx2go8_r2_1280.jpg)
Additionally when you close the window (or try to close the FakeAV program in any way) a fake Windows security center window will pop-up:
![image]
(https://36.media.tumblr.com/7fc154b56dbc552afa70b143064d9097/tumblr_nlm9l2sz5h1qflx2go9_r1_1280.jpg)
In the process of scaring the user the FakeAV copies itself to a new location and installs a registry startup key, the normal persistence method seen. The FakeAV also monitors processes that are running and kills the ones it doesn't like which includes system utilities like taskmgr but also tools like wireshark and alike. All of this to convince the user into buying the 'product' to clean up the 'infection' that stops them from starting these processes.
The FakeAV also performs some C2 communication which includes information on the payment C2 service:
![image]
(https://41.media.tumblr.com/246f33ced9f8215f3b3857e4302028e7/tumblr_nlm9l2sz5h1qflx2go10_r1_1280.png)
The client performs a request to the C2 server located at gelun-posak[.]com, the path is an encoded and base64'd unique system ID. The response contains a small config, the partially readable text string 'eo-moquales[.]Nom' is in fact the payment wall which (after decoding) is golen-mortales[.]com.
Overal this FakeAV is just alike any other I've written on in the past. Payment service runs on a seperate C2 server while the main C2 server is just for infection registration / statistics.
Enough on the malware, lets move on to have a look at this family's history.

## The Family

The Braviax/Fakerean FakeAV family has been around for quite some time, [@S!Ri] (https://twitter.com/siri_urz) first spotted them 6 years ago.
Back in around April 2009 samples started to appear for a FakeAV naming itself "Home Antivirus 2009″ and was the first of more to come:

![image]
(https://41.media.tumblr.com/775bb9ebf3302ed8302f9c2c58c3d2d8/tumblr_nlm29udmth1qflx2go6_r2_540.png)

Around the start of July it was followed by a 2nd version called "PC Security 2009″:

![image]
(https://40.media.tumblr.com/bba567b5e3a3b0f59160f30908cf41d4/tumblr_nlm2bkOQtZ1qflx2go7_r1_540.png)

A 3rd version appeared at the end of July already, this time called “Home Antivirus 2010″ (even though still being 2009… they were ahead of time it seems):
![image]
(https://40.media.tumblr.com/ac521b48dd614859c8893b1653685bab/tumblr_nlm29udmth1qflx2go7_r2_540.png)

Near the end of August the 4th installment of the family appeared, this time it was called “PC Antispyware 2010”. This one actually loaded an AV database, stolen from ClamAV (in fact an old one from 2007):
![image]
(https://40.media.tumblr.com/36579be2d29cb960d6eec7ca7ca02ac9/tumblr_nlm2bkOQtZ1qflx2go6_r1_540.png)

Then in September the 5th version appeared, “Antivirus Pro 2010”:
![image]
(https://41.media.tumblr.com/0a7132ca437d2c5ca2b920dc304be799/tumblr_nlm29udmth1qflx2go2_r2_540.png)

In 2009 5 versions of the Braviax/Fakerean family hit, from September until the end of January 2010 it was quiet; nothing new appeared. At the end of January a completely changed version appeared, this one changed it appearances depending on whether it ran on Windows XP, Vista or 7. Even under these platforms it had multiple names.
Under Windows XP it called itself one of the following names:

Antivirus XP 2010
![image]
(https://40.media.tumblr.com/983284bcde5b875ee1f6a4c62157fcb6/tumblr_nlm29udmth1qflx2go3_r2_540.png)

XP Guardian
![image]
(https://41.media.tumblr.com/9276ab359f5ca9eff16226ffb4b21989/tumblr_nlm9jpDqdC1qflx2go4_540.png)

XP Internet Security
![image]
(https://41.media.tumblr.com/ef2125059523522a6f250817874b9289/tumblr_nlm9jpDqdC1qflx2go9_540.png)

Under Windows Vista it called itself one of the following names:

Vista Antivirus Pro 2010
![image]
(https://36.media.tumblr.com/53ca86e9e1c6aab06dc107bb33b2bc04/tumblr_nlm2bkOQtZ1qflx2go8_r1_540.png)

Vista Internet Security 2010
![image]
(https://36.media.tumblr.com/6c7771d5489358eb8d7cfd18b86a3405/tumblr_nlm2bkOQtZ1qflx2go9_r1_540.png)

Finally, under Windows 7 it called itself one of the following names:

Win 7 Antispyware 2010
![image]
(https://40.media.tumblr.com/dd37d7d81d320526c5ec7986150a08eb/tumblr_nlm2bkOQtZ1qflx2go10_r1_540.png)

Win 7 Internet Security 2010
![image]
(https://41.media.tumblr.com/168028a0bbb1bf7de5febadf103054ad/tumblr_nlm9jpDqdC1qflx2go1_540.png)

An interesting move to have some name mangling dependent on the platform. After they pushed these it stayed quiet until November. In November they released a new version with similar names, only the year was bumped from 2010 to 2011. The Windows XP variants for example:

XP Security 2011
![image]
(https://41.media.tumblr.com/39e8aa0325d377a24fbd96933b32efee/tumblr_nlm9l2sz5h1qflx2go1_540.png)

XP Antispyware 2011
![image]
(https://40.media.tumblr.com/71e6e4a7571d9474e956709e573a341b/tumblr_nlm9jpDqdC1qflx2go6_540.png)

In february 2011 a new version appeared with slightly updated names and GUI layout:

XP Anti-Virus 2011
![image]
(https://36.media.tumblr.com/ea60a11c422d1f2233789ff79339c48a/tumblr_nlm9jpDqdC1qflx2go7_540.png)

XP Home Security 2011
![image]
(https://40.media.tumblr.com/ab67d2347efbee4e2681aff2252b7f5b/tumblr_nlm9jpDqdC1qflx2go8_540.png)

XP Anti-Spyware
![image]
(https://36.media.tumblr.com/77c2d08a661d9eade02489f8481a0b56/tumblr_nlm9jpDqdC1qflx2go5_540.png)

In the end of June 2011 another updated version was released. Again some updated OS based name mangling changes and updated GUI:

XP Internet Security 2012
![image]
(https://41.media.tumblr.com/f6ccfca28167ff0be1c69b8a0c0fad7f/tumblr_nlm9jpDqdC1qflx2go10_540.png)

Win7 Internet Security 2012
![image]
(https://40.media.tumblr.com/69d2cdb2fb8045d640e8af24907c9f22/tumblr_nlm9jpDqdC1qflx2go3_540.png)

Another slightly updated version appeared in the end of November 2011, still based on the OS based name mangling:
![image]
(https://40.media.tumblr.com/ccefe37c48d122181c49ae3d55ae3c87/tumblr_nlm9l2sz5h1qflx2go2_1280.png)

January 2012 a new updated version, GUI mostly, got pushed:
![image]
(https://40.media.tumblr.com/4ff19de42c53029791b1880d26e68b9e/tumblr_nlm29udmth1qflx2go5_r2_1280.png)

In the start of October 2012 another slightly updated version appeared. Mostly GUI changes and again still based on the OS version name mangling:
![image]
(https://41.media.tumblr.com/3e2317efabcdcb6337bf24b8a852c27e/tumblr_nlm29udmth1qflx2go4_r2_1280.png)

Then almost a year later at the start of September 2014 the version from my analysis appeared. An entirely updated GUI and new names showed a big change. It appeared under the following names (with OS version names displayed, although not all use it):

* Sirius (Win 7|Win 8|Vista) Protection 2014
* Zorton (Win 7|Win 8|Vista) Protection 2014
* Rango (Win 7|Win 8|Vista) Protection 2014
* A-Secure 2015
* AVbytes (Win 7|Win 8|Vista) Antivirus 2015
* AVC Plus

GUI wise it looks like this (name stripped as its templated in the GUI at runtime):
![image]
(https://40.media.tumblr.com/607c1b287180d19cb4af11305f968453/tumblr_nlm9l2sz5h1qflx2go3_r1_1280.png)

However in the end of September 2011 a sort of offspring appeared as well named Advanced PC Shield 2012, another one appeared in August 2012 called Win 8 Security System:
![image]
(https://40.media.tumblr.com/c82429e29a4ac13a317c7de16d66a01b/tumblr_nlm29udmth1qflx2go1_r2_540.png)
![image]
(https://40.media.tumblr.com/4e86a2d0b47ef0891329a41fd93a5e57/tumblr_nlm9jpDqdC1qflx2go2_1280.png)

Eventhough this version is also ranked in the Braviax/Fakerean family it looks somewhat different in setup.

## Conclusion
The Braviax/Fakerean family has been around for a long time appearing as early as April 2009 and seems to be a success as new reincarnations appear every year.
While they aren't as big as a threat as banking malware or ransomware it does pay well for these criminals. Because of their 'low' volume and simply being scareware not a lot of attention is given to them. I'll be keeping an eye on them for future campaigns for sure though :)

## IOC's & Samples

The following is a list of samples for the last version spreading from September 2014 to December 2014. No new ones have appeared as of writing this blog article.

* [42f25bda3f8de7c99b1ebbab83f742e8f98528cb466511c3426ca59ba6a0d06c]
(https://www.virustotal.com/en/file/42f25bda3f8de7c99b1ebbab83f742e8f98528cb466511c3426ca59ba6a0d06c/analysis/)
* [f25bf1897ac640c8f9e4cf87897e94f717acffa825fedf772861c8ac68bcc913]
(https://www.virustotal.com/en/file/f25bf1897ac640c8f9e4cf87897e94f717acffa825fedf772861c8ac68bcc913/analysis/)
* [3b93570e402935d2b898c4f07851ea5f597a136d8b88a9e1ab2eb67bcd143f11]
(https://www.virustotal.com/en/file/3b93570e402935d2b898c4f07851ea5f597a136d8b88a9e1ab2eb67bcd143f11/analysis/)
* [55806f8d10acda611dd291fd7ef9205cc5e3845cbfbb44de298387724d979f9c]
(https://www.virustotal.com/en/file/55806f8d10acda611dd291fd7ef9205cc5e3845cbfbb44de298387724d979f9c/analysis/)
* [1d01611a1f88c7015c54efedacfcbc8fec55ad6de9a438087abff3be78c19901]

(https://www.virustotal.com/en/file/1d01611a1f88c7015c54efedacfcbc8fec55ad6de9a438087abff3be78c19901/analysis/)
* [376f1d7b49b8906ca06feef2291e25a5a205d1cd2e3c37effba4311634ef0b53]
(https://www.virustotal.com/en/file/376f1d7b49b8906ca06feef2291e25a5a205d1cd2e3c37effba4311634ef0b53/analysis/)
* [49c609b289ab86dbb001cacec5ff638380f5a4c78dd7e8ffcd7187123349b5e6]
(https://www.virustotal.com/en/file/49c609b289ab86dbb001cacec5ff638380f5a4c78dd7e8ffcd7187123349b5e6/analysis/)
* [f2d67162f4a4af113977a33846b34d47b63160616e0520c7cc3f76eb52755448]
(https://www.virustotal.com/en/file/f2d67162f4a4af113977a33846b34d47b63160616e0520c7cc3f76eb52755448/analysis/)
* [66eb191716d08898f8cc6f2663ef594279a95ed2542c4086618199c040de67f2]
(https://www.virustotal.com/en/file/66eb191716d08898f8cc6f2663ef594279a95ed2542c4086618199c040de67f2/analysis/)
* [810b40d5b9cff4690eca167edd8765c8875172c2601656f8cd89cf8e66a72cc7]
(https://www.virustotal.com/en/file/810b40d5b9cff4690eca167edd8765c8875172c2601656f8cd89cf8e66a72cc7/analysis/)
* [a7175de9d14b29df0beb653982512e9cc0241ecf53ae91135dbae852724a284a]
(https://www.virustotal.com/en/file/a7175de9d14b29df0beb653982512e9cc0241ecf53ae91135dbae852724a284a/analysis/)
* [2c277f6d5f060192a73e2b918d7c210a876cb11d064fdab1f483947df4d1156f]
(https://www.virustotal.com/en/file/2c277f6d5f060192a73e2b918d7c210a876cb11d064fdab1f483947df4d1156f/analysis/)
* [5b7d7c79786b0461dfd0f6ac144ab03374ee5608062d547f21e3b4c2eb13f50f]
(https://www.virustotal.com/en/file/5b7d7c79786b0461dfd0f6ac144ab03374ee5608062d547f21e3b4c2eb13f50f/analysis/)
* [01a4e7e0297923a40d85b931c4715ddd0fc9b3881de12c4affcaa7595a95407f]
(https://www.virustotal.com/en/file/01a4e7e0297923a40d85b931c4715ddd0fc9b3881de12c4affcaa7595a95407f/analysis/)
* [1cfc14b9532e12a7cc02874d655796dbed6eff5c774b37670ec16b185efe72af]
(https://www.virustotal.com/en/file/1cfc14b9532e12a7cc02874d655796dbed6eff5c774b37670ec16b185efe72af/analysis/)

The following domains and IP addresses were seen for those samples:

| IP Address | Domain |
| ——————— |———|
| 146.185.239.110 | evcash.net |
| 146.185.239.110 | softrango.com |
| 146.185.239.111 | ltsectur2.com |
| 146.185.239.111 | ltsectur9.com |
| 146.185.239.111 | fscurat20.com |
| 146.185.239.111 | fscurat21.com |
| 146.185.239.112 | fastprodst5.com |

| 146.185.239.112 | fflord25.com |
| 146.185.239.112 | fflord30.com |
| 146.185.239.112 | giron32.com |
| 146.185.239.112 | glorius11.com |
| 146.185.239.112 | golus27.com |
| 146.185.239.112 | gshsol4.com |
| 146.185.239.112 | holipolks12.com |
| 146.185.239.112 | scara123.com |
| 146.185.239.112 | scara124.com |
| 146.185.239.112 | smart-filins.com |
| 146.185.239.112 | srut12.com |
| 146.185.239.112 | srut19.com |
| 146.185.239.113 | gskskkksa4.com |
| 146.185.239.113 | jarr62737.com |
| 146.185.239.114 | gislat2for8.com |
| 146.185.239.114 | gislat4se2.com |
| 146.185.239.114 | gladi-toriusa.com |
| 146.185.239.114 | holisak-tasek.com |
| 146.185.239.114 | hysotasl.com |
| 146.185.239.114 | kaaalosa-set.com |
| 146.185.239.114 | shatiko-mero.com |
| 146.185.239.114 | svars-sta.com |
| 146.185.239.114 | tauruk-felon.com |
| 146.185.239.114 | trader562.com |
| 146.185.239.114 | veret-sapan.com |
| 146.185.239.114 | vertus-adusa.com |
| 146.185.239.114 | vesm-arast.com |
| 146.185.239.114 | zemo-numeros.com |
| 146.185.239.114 | zumo-afetuk.com |
| 146.185.239.114 | zumo-alibabs.com |
| 146.185.239.114 | zumo-archib.com |
| 146.185.239.114 | tauruk-felon.com |
| 146.185.239.248 | gelun-posak.com |
| 146.185.239.248 | fulo-centums.com |
| 62.122.74.111 | golen-mortales.com |