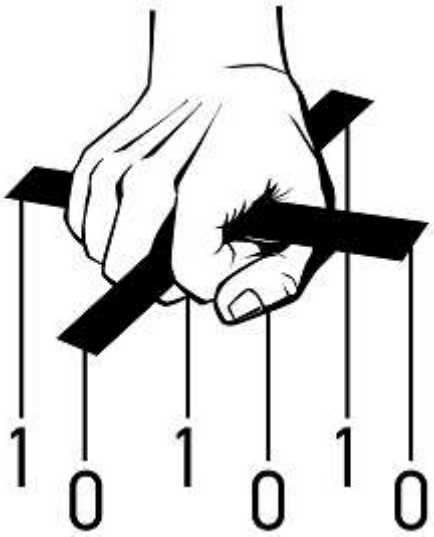
Shellter Pro – License Infringement Investigation Report



Prepared by Kyriakos Economou - Shellter Project Author

Incident

In 2021 we were notified by one of our contacts that a Shellter Pro version was leaked by a customer and advertised on RaidForums (now seized by the FBI).

It wasn't long before some people started selling our software via several telegram channels. The version leaked at that point was v3.5, but there is a chance that v3.4 was also leaked.

We later noticed that they were changing the version of the binary using a hex editor or similar tools. At some point they were advertising that the binary being sold was version 3.7, but in reality, it was just an older modified version, possibly 3.4/3.5.

We used several contacts to get the advertised binaries, but unfortunately at that stage the leaker had not shared the original license file, since this was merely a formality and not really part of a DRM. So, even though the application would issue a warning without a valid license present, it would still operate normally.

In addition, the fact that the person selling this leaked version did not have immediate access to the latest version, which was 3.7 at that point, made us think that people advertising and selling this they were not the original owner(s) of the license, but someone that probably bought/go it from one of our customers.

As mentioned above, they advertised several 3.x versions such as 3.6 and 3.7, but for some time these were just older versions of the binary that were modified to display a different version number. They even got as far as advertising version 4.0 before it was even released. No need to say that they scammed several people by doing this, but at that point they well deserved it.

Taking the extra step

“Knowing your own darkness is the best method for dealing with the darknesses of other people.” (Carl Gustav Jung).

Whoever decided that profiting from our software, or just recklessly sharing it with everyone, including potential criminals, was a good idea, definitely relied on the fact that the there was no actual DRM protection. The license file which was the only thing that could be used to trace a copy back to the actual owner, was not necessary to operate the software.

At that stage we were also getting close to the release of version 4.0 and we definitely wanted to deal with those guys first. Unfortunately, there will always be people that can potentially do the same, but this was no excuse to release the new major version without first trying to find the source of that leak.

So, we decided to keep the absence of DRM so that the leaker could “safely” leak their copy without sharing also their license file.

That said, we do employ a strict vetting process to potential buyers before we decide to sell a copy. Considering the time spent on doing this, versus the reckless and irresponsible behaviour of one of our customers, it didn’t leave us much choice but to act as fast as possible.

Indeed, something had changed in version 3.7 of Shellter Pro. Some files exchanged with customers were watermarked. So, we decided to sit down and wait for the fish to eat the bait.

Game over

“The fox has many tricks. The hedgehog has but one, but that is the best of all.” (— Archilochus, Carmina Archilochi: The Fragments of Archilochos)

A few months later, the 14th of February 2022, just like an irony of fate, flirting with the leaker paid off. One of our contacts notified us that there was a potential leak of version 3.7. Since there were some fake ones already, we didn’t have much hope, but things changed rapidly.

The copy was sent to us, and as expected all files were in the archive except from the actual license file. Little did they know, we didn’t need the license file anymore to trace some data back to the actual owner.

We managed to trace the source of the leak back to a Polish company (ITWILLROCK SP. Z O.O.) operated by an individual named Artem Panfilov, originally from Russia, but resident in Poland as stated here. It looks like he now also owns a subsidiary/branch based in San Francisco, USA.

We contacted them immediately by providing a license infringement notice and asking for further information regarding this matter. At first, Artem was cooperative and for this reason we provided further information such as access logs related to their account.

A few days later, they came back mentioning as the source of this leak to be a former employee that was contacted by a known, at the time, Russian hacker going by name Pavel Sitnikov. Pavel was arrested already in connection to other crimes, but it looks that sometime later he was released. He has now become a “white – ethical hacker”; he even owns his own cybersecurity firm.

Please note that this is the information provided by Artem based on their own internal investigation and we have no way to verify any of it. We are just presenting the facts as provided by them.

Artem tried to deny any responsibility around this incident at some point. However, the license was purchased and owned by his company, and not by any former employee. He was indeed the person that initiated and handled the purchase process on behalf of his company.

According to our EULA the owner of the license is responsible for any leaks intentional or not and this comes with a compensation fee equivalent to 50-users license at the price on date the infringement is discovered.

After several back and forth, in March 2022 Artem agreed to pay a reduced compensation fee and asked for an invoice on April 2022 (after disappearing again for another month). We did provide an invoice and waited for them to take action.

Unfortunately, 6 months have now passed by since our original license infringement notice and we haven't received any compensation whatsoever. We did our best to settle this in a private manner without causing any more noise.

We finally decided to publish this report in order to inform people about the irresponsible and reckless behaviour of people involved with this company.

That said, we did give them the heads-up and also provided a copy of this report before publishing it. Unfortunately, we haven't received any reply whatsoever to date (09.09.2022).

Final note

The damages caused by such incidents go far beyond any type and size of financial losses. Software like Shellter Pro when leaked, are used by cyber criminals to create more damages against individuals and companies.

Our vetting process is there to reduce this risk and protect the online community from such unfortunate events. Looking at professionals ignoring these efforts is extremely disappointing to say the least.

We did try to carry this weight in full, but we reached the point where it's time for offenders to take some of this burden off from our shoulders.

THIS SPACE INTENTIONALLY LEFT BLANK.