Be careful what you OSINT with

MwOsint OSINT March 23, 2020 4 Minutes

There are lots of neat OSINT platforms out there to make your life easier. But how many of you vet the software before using it? Not every platform should be entrusted with sensitive data as this case reveals.

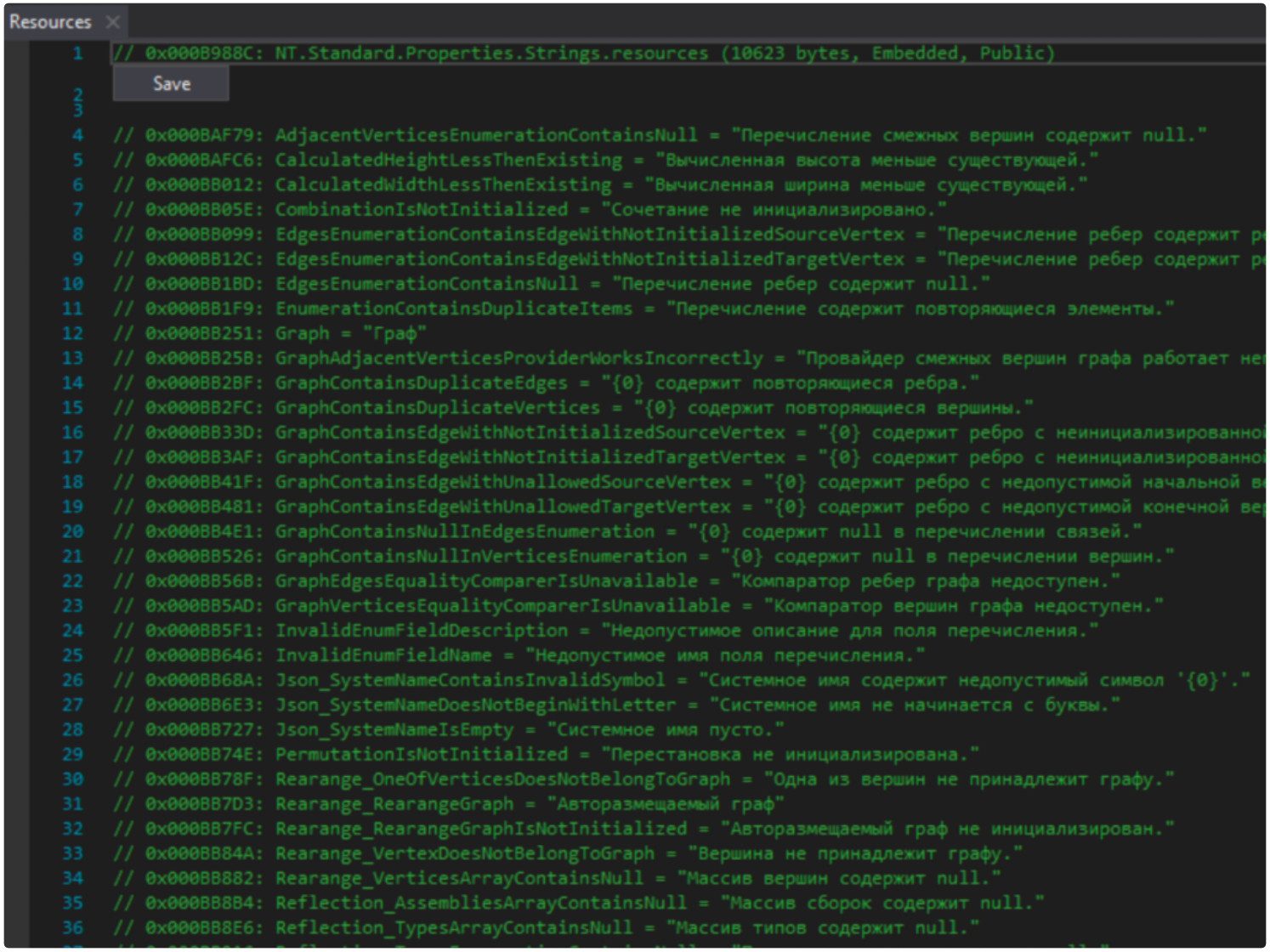
In January 2019 I was tagged on Twitter, asking for my input on an OSINT platform named Lampyre. Before I use any type of software, I try to vet it as good as possible. This includes OSINT research on the company, asking tech-savy people I know for their opinion and ultimately reaching out to the company itself. No one had really heard of the software at that time, no one was using it, and I couldn't really find much background information online. I ended up contacting Lampyre and asking them where they came from, what their background was and a couple of other questions. Unfortunately, they only sent evasive answers. They wouldn't even tell me which country they were based in. I tried the software on one of my VMs and tested it with fake or non-relevant data. To be honest, I did like what I saw, but I decided not to use it

operationally. As time passed, I noticed that many OSINTers started using the software and decided to have another look into the company and people behind it. It turns out, I was right not to use this platform. Lampyre isn't who they claim they are. I teamed up with several helpful elves (to be honest, they did most of the work) and we found some pretty disturbing information.

Lampyre is apparently made by a company in Budapest (Hungary) called Data Tower. The company itself was registered in February 2019 and the CEO and sole shareholder is Laszlo Schmidt. The original address used to register the company leads to a law firm and the phone number that Data Tower provides belongs to another law firm in which Laszslo Schmidt is working as a lawyer. This information points to the fact that Data Tower is merely a shell company. So, how do you we get to the people behind Lampyre?

Looking into their online presence doesn't lead to any notable individuals either. Some of the names used, such as John Galt, are most likely pseudonyms or fake accounts. Since searching for people didn't provide any leads, we decided to look into the traffic that Lampyre sends to its back end in each query. The queries contain a brief description on what is requested and apparently the local language used by the developers is Russian, as each description is written not only in English but also in Russian.

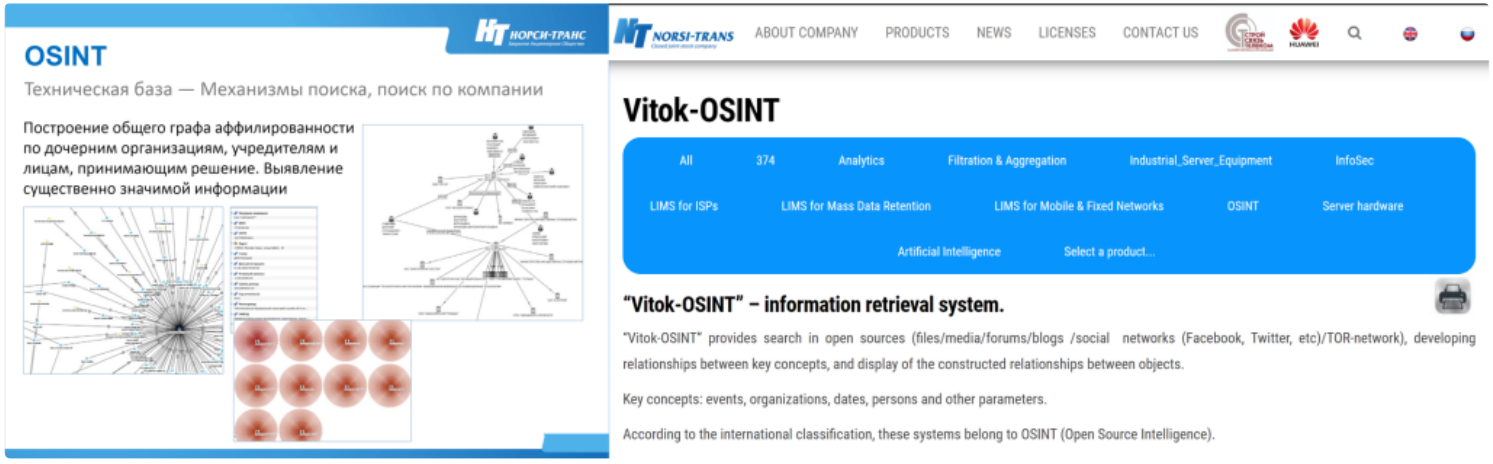
Why should a company based in Hungary use Russian as their local language setting? Of course, the developers could be Russians working in Budapest, but again something just doesn't seem right here: an organization that shows signs of being a shell company, the lack of transparency when directly confronted and now indications that point towards Russia. Decompiling the software showed further Russian language embedded in the code:



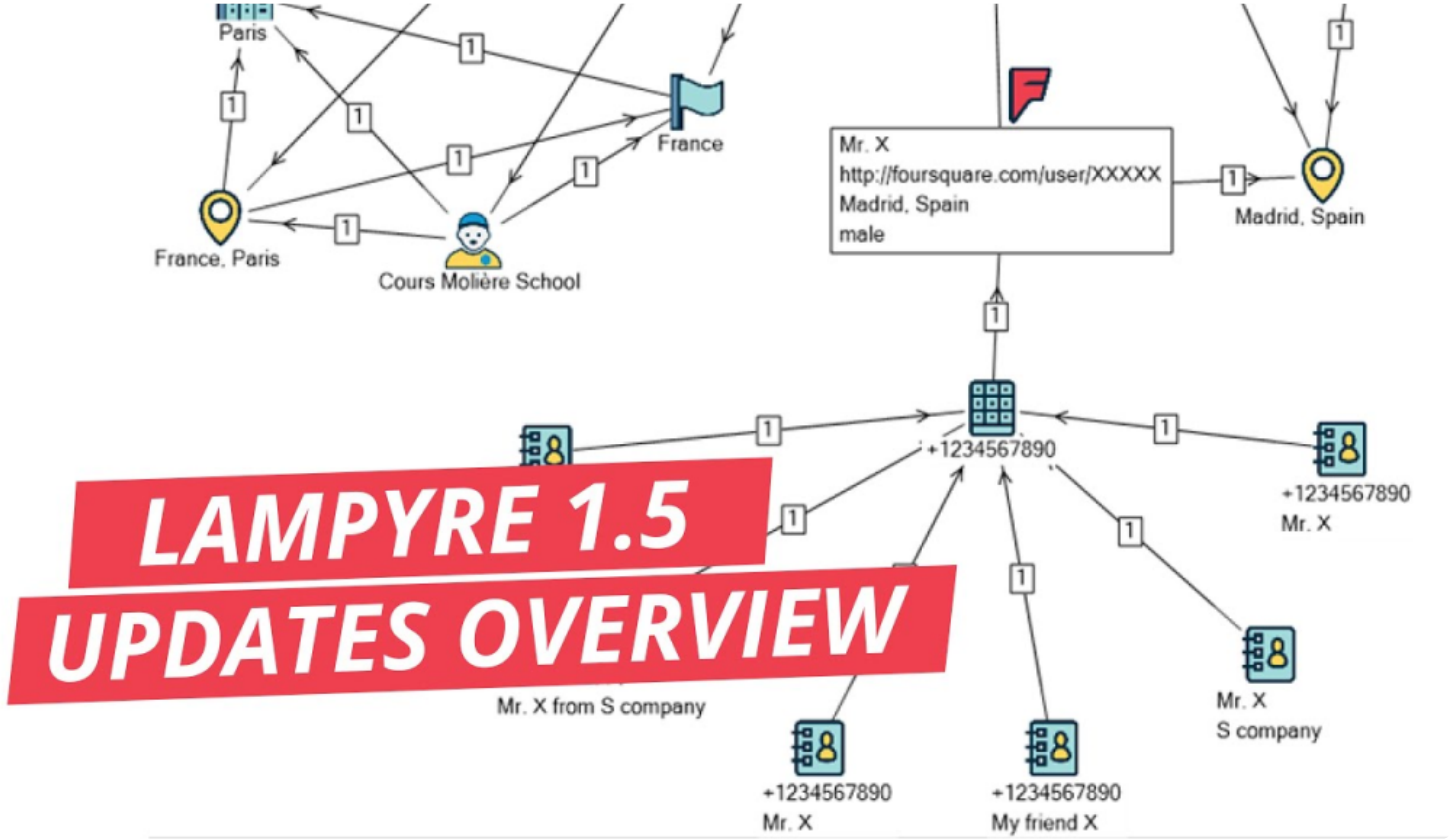
While this was being done, more OSINT research revealed a person named Andrey Skhomenko. This guy posted Python modules for Lampyre on Github and knew about the product in March 2018, way before it was released to public in October 2018.

Andrey is based in Moscow and used to have a LinkedIn profile as well (which has been deleted in the meantime).

According to his LinkedIn, Andrey worked for the Russian Federal Security Service (also known as FSB) in the past and is now working for a company called Norsi-Trans. Norsi-Trans produces SIGINT and lawful interception equipment and software for the Russian government. It turns out that Norsi Trans also sells an OSINT platform called Vitok-ROI (or Vitok-OSINT).



The overall look of this platform reminded me of something I had seen before. Oh, that's right! Both Lampyre and Vitok-OSINT have that Win95/Win98 appearance, not only in the network visualization, but also the software itself.



So far, this was just a gut feeling. Could anymore evidence be found that would link these two products and thus Norsi Trans and Data Tower? You bet? We pulled the certificates used by Lampyre and saw that they were registered in Russia and even more compelling: one of the certificates made a direct reference to Vitok.

```
lampyre-io.stage.dmz.nt-com.ru
lighthouse.lampyre-io.stage.dmz.nt-com.ru
slb.account-lampyre-io.prod.dmz.nt-com.ru
vitok-info-rest.lampyre-io.prod.dmz.nt-com.ru
oapi.lampyre-io.stage.dmz.nt-com.ru
crm.lampyre-io.prod.dmz.nt-com.ru
rapi.lampyre-io.stage.dmz.nt-com.ru
api.lighthouse.lampyre-io.stage.dmz.nt-com.ru
oapi.lampyre-io.dev.int.nt-com.ru
doc.lampyre-io.stage.dmz.nt-com.ru
rapi.lampyre-io.prod.dmz.nt-com.ru
dc.lampyre-io.prod.dmz.nt-com.ru
web.lampyre-io.stage.dmz.nt-com.ru
slb.lampyre-io.stage.dmz.nt-com.ru
```

This was the final nail in the coffin. Lampyre and Norsi Trans are in fact connected! While there is still plenty to be discovered, I think we have proof that Lampyre and Data Tower are not fully honest. And as everything you query in Lampyre is probably sent to Russian servers, I am happy I decided not to use this tool in my private and professional investigations. After all, Russia mandates decryption for domestic services.

Maybe Lampyre is Norsi Trans' attempt to sell their software in the western world, maybe it is a rogue operation by a Norsi Trans employee (or a few). Although, I personally have doubts about that second theory. The software is quite powerful and receives regular updates. To create something like this, you'd surely need more than one person and having a rogue team within a company try to pull this off would surely not go unnoticed. What I find most interesting, is the fact that Andrey stated he had worked for the FSB. To put it in the words of one of my former colleagues: You don't leave Russian intelligence services, you just change your cover and continue working for them.

Matthias Wilson / 23.03.2020

Like

Be the first to like this.

Related

Using the Microsoft Video Indexer for OSINT

In "OSINT"

Interdisciplinary Intelligence Preparation of Operations - (I2PO)

In "OSINT"

The Impact of OSINT on Christmas

In "Intelligence"

Tagged: DFIR, Forensic, InfoSec, INTEL, Intelligence, OSINT, Research

Published by MwOsint

View all posts by MwOsint

Published

March 23, 2020

‹ Using the Microsoft Video Indexer for OSINT

4 thoughts on “Be careful what you OSINT with”

Info

March 24, 2020 at 1:20 pm

very interesting

★ Like

↳ Reply

Audiard

March 25, 2020 at 11:02 am

very interesting study, which brings other questions : I see a lot of tools using only Chrome, and that are not adapted to Firefox (some linkedin addon, Hunchly, etc.).
But I do not see anyone asking question about that : Chrome is not neutral. Can’t we have better tools based on real opensource software ?

★ Like

↪ Reply

Laszlo Schmidt

March 26, 2020 at 5:22 pm

We earlier posted our response to Matthias on Twitter, but we think it's only fair to provide it here as well. So everyone could read it below the post above.

@lampyre_io: Dear Matthias, as always, your content is the top of the tops. The info that you found is indeed partially true, apart from implying that Data Tower is merely a shell company and that our customers' data might be disclosed to third parties.

Contacting Data Tower directly in 2020 again could be a better choice, but apparently, you preferred jumping to conclusions before updating your info first. The only time you contacted us was in Jan 2019.

Here is the info on Data Tower and Norsi-Trans:
https://medium.com/@lampyre.io/everything-you-wanted-to-know-about-lampyre-326f62c2b325

★ Like

↪ Reply

Key Findings

March 26, 2020 at 5:49 pm

A reply that doesn't really answer the open questions in my article and 'Lazslo' using Alex' email to post this here? Come on, this isn't letting things look better for you. It's actually even making it worse.

★ Like

↳ Reply

Leave a Reply

Enter your comment here...

Suchen

Search ...

Follow Blog via Email

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 141 other followers

Enter your email address

Follow

Tags

+1-844-947-4746 Activate Norton AndroidEmulation AssetTracing attribution Baidu CompanyRegister CompetitiveIntelligence CovertOps cyberattack Data Protection DeepL Domaindata Due Diligence Email permutator Email verification Ermittlungen EXIF Facebook FirstPost FlightTracking Forensic Forensic Linguistics GDPR Geolocation GoogeStreetView GoogleAnalytics GoogleDorks GoogleMaps Google Translate hacking HUMINT Hunchly I2PO InfoSec Instagram INTEL Intelligence Investigations Investigative Journalism IS itsecurity LawEnforcement LinkedIn Metadata Norton Norton Support Offline OpenCorporates OPSEC OSINT phishing PrimarySources Recherche Research Scam SEO SIGINT SocialEngineering Social Media SocialMedia Social Networks SockPuppets Strava Strave Syria Telegram Text Analysis TikTok Tinder Translate Twitter VLOG VUMINT WhatsApp