

Approaching stealers devs : a brief interview with LummaC2

 g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-lummac2-94111d4b1e11

g0njxa

November 16, 2023



[g0njxa](#)



To completely understand what's going on in a market that has been growing in the last years I found mandatory to know which players are dominating it. Always remember that behind every user of the Internet there is another human like you, so if you can be kind enough to reach them and they agree, you can have a little talk. Asking things is not a crime.

Let's see, LummaC2: [@lummanowork](#)

LummaC2 Bugs

Ah, so it's you, g0njxa

g0njxa

Do you know me?

LummaC2 Bugs

Certainly

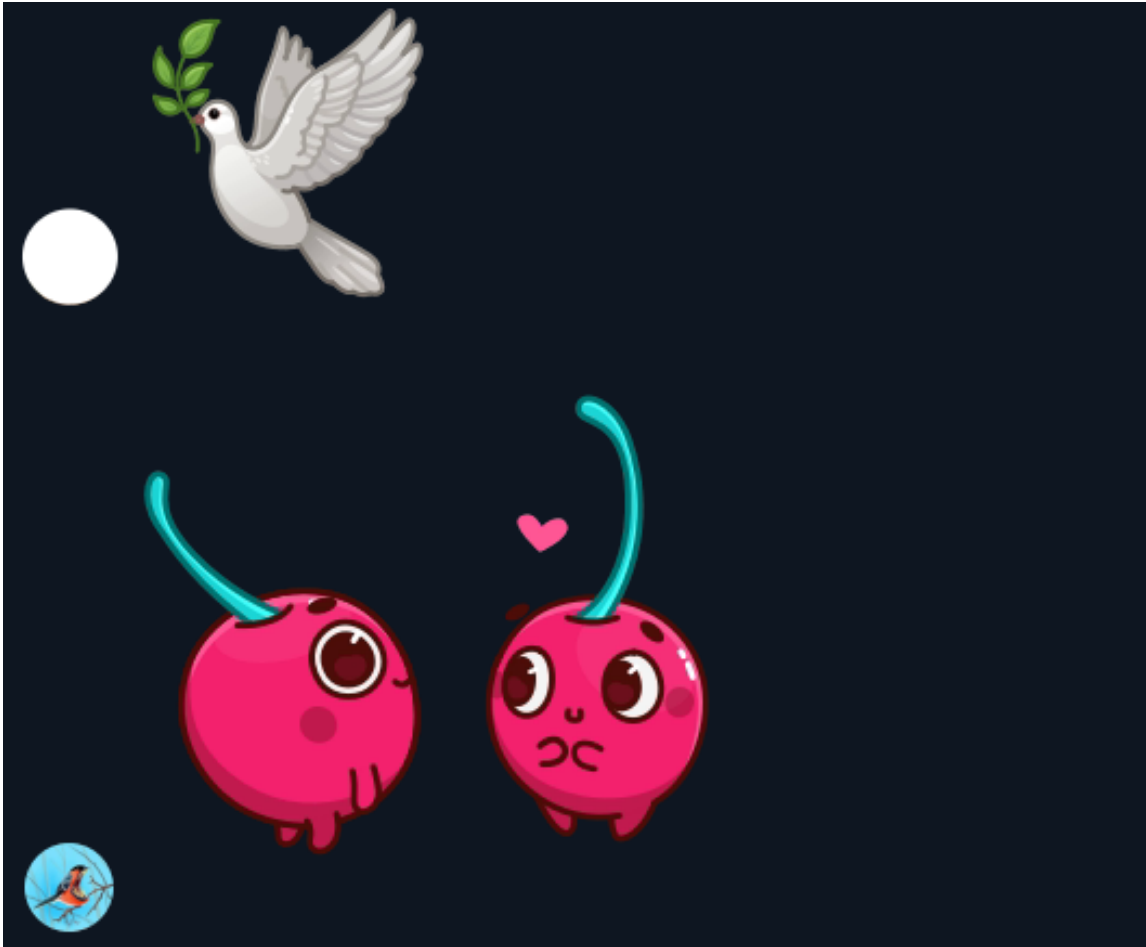
g0njxa

I like malware, there's nothing personal about people

I try to be good people

LummaC2 Bugs

That's right. It would be nice if you didn't send reports to our domains
👉❤️ so often



English translations from Russian

The Lumma guy seemed to know me before I even started to talk to him. I'm actively tracking Lumma C2s and reporting them to Abuse ThreatFox. So yes, the stealer guys also seem to be looking at us :)

He shows himself as a kind and open person, and I have nothing to reproach. He was, indeed, very kind to me.

The interview was made in Russian. Since I was using a translator, questions will be shown in original english, and answers will be given both in original Russian (in case translation is misled) and translations to english.

g0njxa

how would you describe Lumma?

LummaC2 Bugs

I think it's one of the most technologically advanced stealers on the market right now, the technology comes from us first, and then it comes from the competition. We are always working to improve the product, despite the fact that we already have a lot of customers. Many people rest on their laurels, we don't.

How would you describe Lumma?

Я думаю сейчас это один из самых технологичных стиллеров(stealer) на рынке, технологии сначала появляются у нас, а потом они появляются у конкурентов. Мы всегда работаем над совершенствованием продукта, несмотря на то, что у нас уже много клиентов. Многие останавливаются на достигнутом, мы — не останавливаемся.

If you need a further description on Lumma by its owners you can always check: [LummaC2 — universal stealer, a malware for professionals. — Telegraph](#)

g0njxa

What does the name Lumma mean?

LummaC2 Bugs

The logo has been in my head for a long time. The bird is a symbol of peace, lightness and tranquility. Therefore, it was necessary to come up with an equally light and calm name. Making money with us is just as easy.

What does the name “Lumma” means?

Логотип у меня был в голове давно. Птица — символ мира, легкости и спокойствия. По этому нужно было придумать такое же легкое и спокойное название. Зарабатывать с нами так же легко.

g0njxa

What makes Lumma different from other products?

LummaC2 Bugs

Manufacturability, support. Notice how quickly I respond to you

What makes Lumma different from other products?

Технологичность, поддержка. Обратите внимание как быстро я вам отвечаю

g0njxa

How many people do you think have tested this product?

Approximately

LummaC2 Bugs

We have about 400 active clients. That's a lot

У нас около 400 активных клиентов. Это очень много

From what I'm learning, having such a large number of customers can be considered big. Most of the projects doesn't want too much attention, some others want to grow as big as they can!

g0njxa

Since when has LUMMA been working?

LummaC2 Bugs

21.12.22

Soon we will be one year :)

21.12.22Скоро нам год :)

Please find at the bottom of this interview some news about this incoming event

g0njxa

In June 2023, a very big update came out. Since then, the use of LUMMA has been on the rise.

LummaC2 Bugs

The biggest update of 25 points came out last week

g0njxa

I say this because I believe that since that day, people have been using LUMMA more often. Do you agree?

LummaC2 Bugs

The use of Lumma is growing gradually, for example, in the past week our customers have become more than 20 people

In June 2023, a very big update came out. Since then, the use of LUMMA has been on the rise.

Самое большое обновление из 25 пунктов вышло на прошлой неделе

I say this because I believe that since that day, people have been using LUMMA more often. Do you agree?

Использование Lumma растет постепенно, например за прошлую неделю нашими клиентами стали больше 20 человек

When asking about the “June ’23 Update” I was trying to refer to the moment that I got very interested in Lumma: when I noticed the first domain being used by this stealer as a C2. I don’t know if I was late or fast, just that since that moment Lumma was using custom domains. More updates were done, and the notoriety of Lumma increased exponentially.

2023-06-18 15:28:44	http://private-cloud-server.pro/c2sock	Lumma Stealer	HENDRo Lumma rUwoHq stealer	g0njxa
2023-06-17 16:41:13	217.12.206.230:80	Lumma Stealer	Lumma LummaStealer	Ishusoka
2023-06-16 22:15:55	http://217.12.206.230/c2sock	Lumma Stealer	Lumma stealer	g0njxa

First?

The “past week update” was shared on Twitter:

<https://x.com/g0njxa/status/1722664597478384095>

And you can check it here: [Update 8.11 — Telegraph](#)

It is alledgely called as “the biggest update since the opening of the project”

g0njxa

Who came up with the idea of placing poems in the Lumma infrastructure?

Will we see more poems?

LummaC2 Bugs

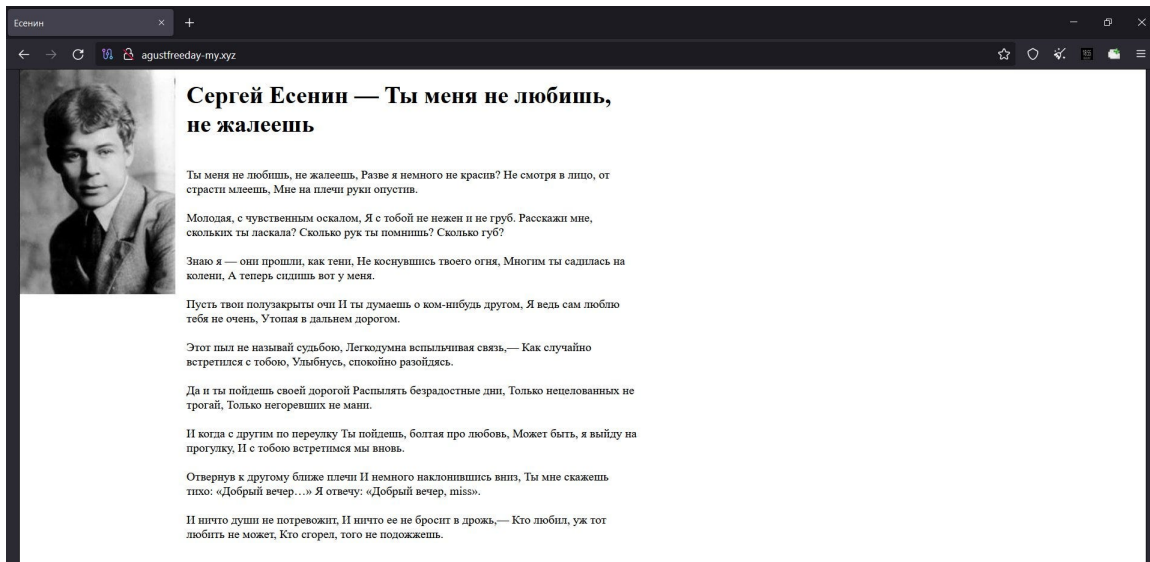
Yes, somehow unanimously. I won't say anything about the poems yet.
We love Russian poets and Russian literature 🤗

Who came up with the idea of placing poems in the Lumma infrastructure? We will see more poems?

Да как-то единогласно. Про стихи пока ничего не скажу. Мы любим русских поэтов и русскую литературу 🤗

One fancy thing about the Lumma C2s were the poems added to their domains. We had “Sergey Yesenin — You don't love me, you don't regret me” and “CHARLES BAUDELAIRE, “FLOWERS OF EVIL”, VERSE 29”.

They got deleted, in fact, having these texts on C2s helped to track them more easily. It wasn't that bad to have a non-boring C2, hope one day we will see more things on their domains. (So we can look for them :p)



The screenshot shows a web browser window with the address bar displaying "agustfreeday-my.xyz". The page content is as follows:

Сергей Есенин — Ты меня не любишь, не жалеешь

Ты меня не любишь, не жалеешь, Разве я немного не краше? Не смотря в лицо, от страсти млеешь, Мне на плечи руки опустишь.

Молодая, с чувственным оскалом, Я с тобой не нежен и не груб. Расскажи мне, сколько ты ласкала? Сколько рук ты помнишь? Сколько губ?

Знаю я — они прошли, как тени, Не коснувшись твоего огня, Многим ты садилась на колени, А теперь сидишь вот у меня.

Пусть твои полузакрыты очи И ты думаешь о ком-нибудь другом, Я ведь сам люблю тебя не очень, Утопая в дальнем дорогом.

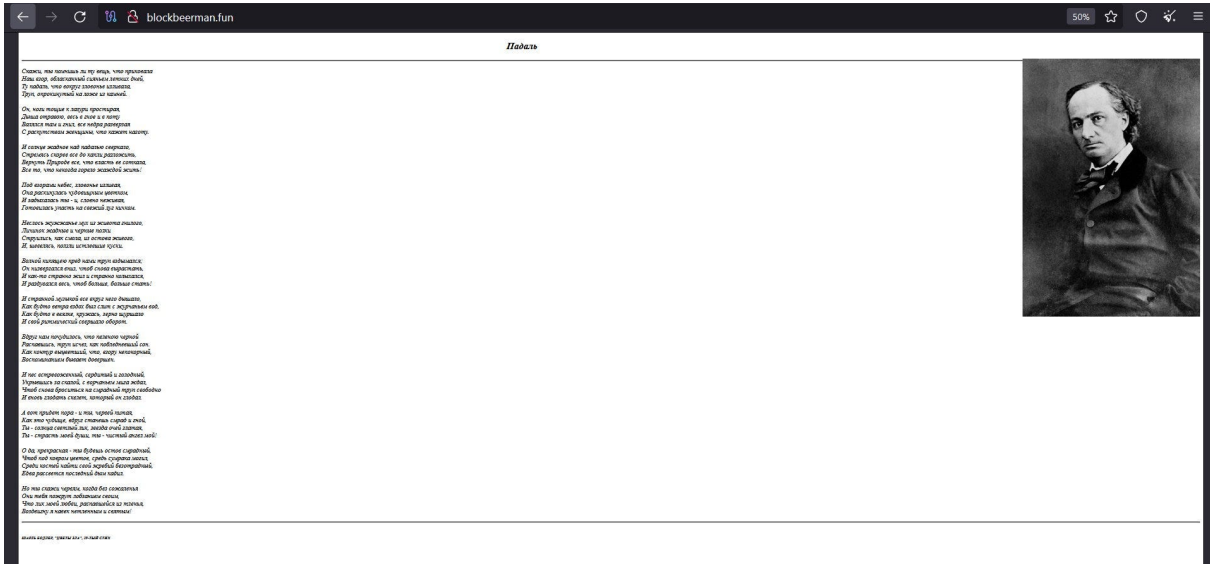
Этот пыл не называй судьбою, Легкодумна испальчивая связь,— Как случайно встретился с тобою, Улыбнись, спокойно разойдись.

Да и ты пойдешь своей дорогой Распылять безрадостные дни, Только нецелованных не трогай, Только негоревших не маш.

И когда с другим по переулку Ты пойдешь, болтая про любовь, Может быть, я выйду на прогулку, И с тобою встретимся мы вновь.

Отвернув к другому ближе плечи И немного наклонившись вниз, Ты мне скажешь тихо: «Добрый вечер...» Я отвечу: «Добрый вечер, miss».

И ничто души не потревожит, И ничто ее не бросит в дрожь,— Кто любил, уж тот любить не может, Кто сторел, того не подожжешь.



g0njxa

LUMMA is used by both individuals and work groups as an option to join. People love LUMMA. Do you think LUMMA can be used more often than REDLINE, META, RACCOON or others?

LummaC2 Bugs

I think so. A lot of customers come to us from the listed products

LUMMA is used by both individuals and teams as a feature. People love LUMMA. Do you think LUMMA can be used more often than REDLINE, META, RACCOON or others?

Думаю, да. К нам приходят много клиентов из перечисленных продуктов

Please note that people will buy a license of a stealer for themselves, and sometimes to work in small groups of 2–4 people. Also note that when talking about a team, everyone has access, so dozens of users are retrieving builds from the same panel. It is a fact that the use of Lumma has been increasing a lot: some people participating actively in the market and with years of experience on this field have switched completely to Lumma. This project has made his way into the *Big Five's*!

g0njxa

Speaking of the market, how do you see it? Is this a good time to work? Or is there a shortage of food? A lot of people I've talked to complain about this

Workers I've Spoken To

LummaC2 Bugs

There is demand in the market, and I think the supply corresponds to the demand. Advise our product to employees

g0njxa

and in the future?

LummaC2 Bugs

In the next 2–3 years, we will be here

*На рынке есть спрос, и думаю предложение спросу соответствует.
Работникам посоветуйте наш продукт*

and in the future?

В ближайшие 2–3 года мы будем тут

To explain this I will say that I have talked with other people working with stealers, and somehow there is a common feeling: the shortage of valid providers of accounts used in malware spreading, and the difficulty to innovate in the ways they share malware. The lack of products have also a common cause: Ukraine War, hope one day I can dive further on the point of view of these users.

There is a demand on the market, he is right.

People have been working for months even years, and we will surely see more people in the following years.

g0njxa

LUMMA does not allow you to work with Russians. LUMMA protects Russians. What is your opinion of people working with Russians?

with other products

LummaC2 Bugs

We have a tradition and a rule "don't shit where you live". I was offered \$25,000 to unblock my work in Russian. We always refuse such clients

LUMMA does not allow you to work with Russians. LUMMA protects Russians. What is your opinion of people working with Russians? with other products

У нас есть традиция и правило «не срать там где живешь». За разблокировку работы по русским мне предлагали 25 тысяч долларов. Мы всегда отказываем таким клиентам

The “anti-CIS” policies are present in most of the malware projects, that shouldn’t be nothing new. “Protect the motherland and the motherland will protect you”.

g0njxa

If only someone could modify LUMMA to work with the Russians (as happened with WHITESNAKE). What are we going to do?

LummaC2 Bugs

No one can do that. We have a different architecture

Никто не сможет этого сделать. У нас другая архитектура

FYI WhiteSnake Stealer project got banned from some Russian forums after “some customer modified the build and removed Anti-CIS module”. As stated before, that’s a red flag and developers must take care of it.

g0jnxа

What would you say to those "information security experts" who are trying to track LUMMA?

LummaC2 Bugs

I say hello to them. I don't mind being tracked. On the contrary, it gives the popularity of Lumma.

What would you say to those "information security experts" who are trying to track LUMMA?

Передаю им привет. Я не против что нас отслеживают. Напротив — это дает популярность Lumma.

привет!

g0njxa

I think that's all))) is there something to say?

Do you have anything ready for the anniversary?

LummaC2 Bugs

Yes, there will be a contest, there will be a big article with what has changed in our country over the year

I think that's all))) is there something to say? Do you have anything ready for the anniversary?

Да, будет конкурс, будет большая статья с тем, что изменилось у нас за год

That's an exclusive: Lumma 1st anniversary will be at December 21st, 2023. He was offering discounts at month anniversaries, but I believe this will be a different moment. As said, Lumma is working on a contest and an article regarding Russia. Expect high activity on those days! Waiting for further news!

The end?

Expect more content,
Best regards.

@g0njxa

