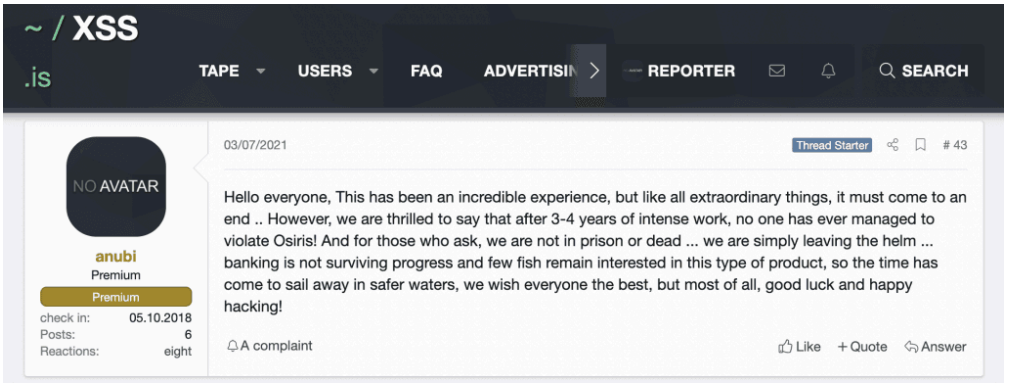
Osiris banking trojan shuts down as new Ares variant emerges

By Catalin Cimpanu

Published: 2022-12-09 · Archived: 2026-04-06 00:59:39 UTC

The creator of the Osiris banking trojan has shut down its operation in March, citing a lack of interest for banking trojans in the cybercriminal underground.

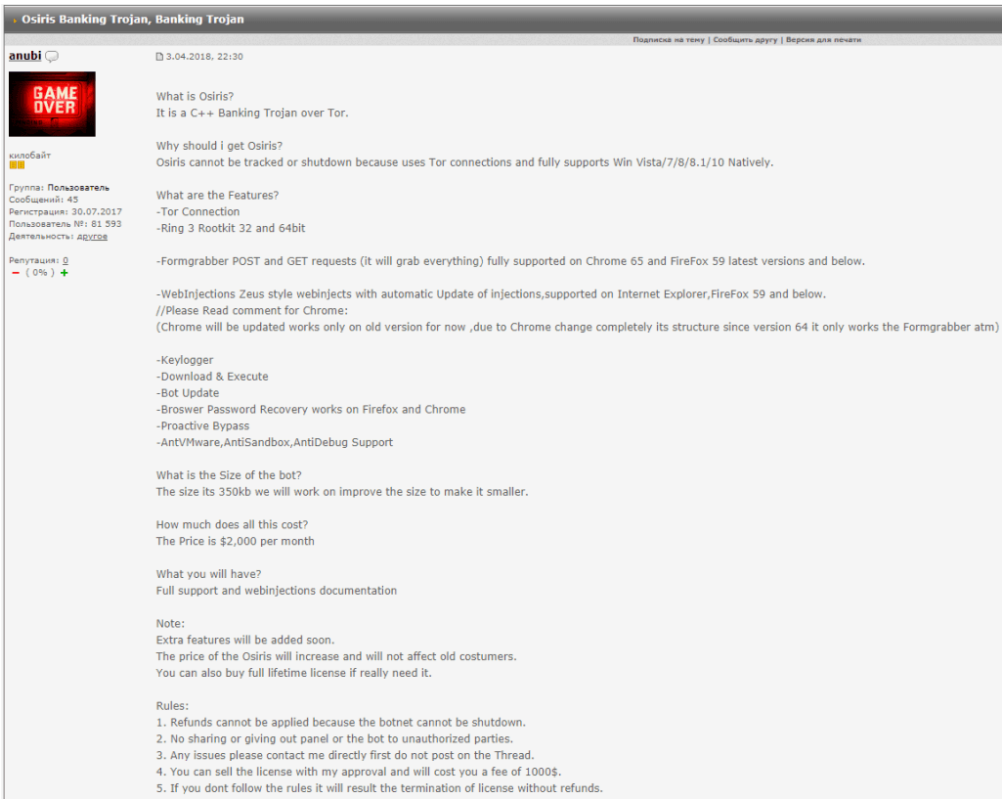
The shutdown announcement was posted in a hacking forum thread where the Osiris author, an individual named Anubi, initially started advertising the trojan back in April 2018.



For the past three years, Anubi has been providing copies of the Osiris banker to cybercrime groups, which have been distributing them using email spam campaigns to victims all over the world.

The trojan, which is a revamped and improved version of the Kronos malware (2014), is a classic banking trojan that infects Windows computers and then injects malicious code in web browsers to steal e-banking credentials and alter banking transactions.

According to an analysis by security firm Check Point, the trojan also employed advanced rootkits to get a permanent foothold inside infected hosts and could also steal credentials from multiple local apps, data that it later sent to a command and control (C&C) server via the Tor protocol.



Osiris Banking Trojan, Banking Trojan

Подписка на тему | Сообщить другу | Версия для печати

anubi

3.04.2018, 22:30

GAME OVER

килобайт

Группа: Пользователь
Сообщений: 45
Регистрация: 30.07.2017
Пользователь №: 81 593
Деятельность: другое

Репутация: 0
− (0%) +

What is Osiris?
It is a C++ Banking Trojan over Tor.

Why should i get Osiris?
Osiris cannot be tracked or shutdown because uses Tor connections and fully supports Win Vista/7/8/8.1/10 Natively.

What are the Features?
-Tor Connection
-Ring 3 Rootkit 32 and 64bit

-Formgrabber POST and GET requests (it will grab everything) fully supported on Chrome 65 and FireFox 59 latest versions and below.

-WebInjections Zeus style webinjects with automatic Update of injections,supported on Internet Explorer,FireFox 59 and below.
//Please Read comment for Chrome:
(Chrome will be updated works only on old version for now ,due to Chrome change completely its structure since version 64 it only works the Formgrabber atm)

-Keylogger
-Download & Execute
-Bot Update
-Broswer Password Recovery works on Firefox and Chrome
-Proactive Bypass
-AntVMware,AntiSandbox,AntiDebug Support

What is the Size of the bot?
The size its 350kb we will work on improve the size to make it smaller.

How much does all this cost?
The Price is $2,000 per month

What you will have?
Full support and webinjections documentation

Note:
Extra features will be added soon.
The price of the Osiris will increase and will not affect old costumers.
You can also buy full lifetime license if really need it.

Rules:
1. Refunds cannot be applied because the botnet cannot be shutdown.
2. No sharing or giving out panel or the bot to unauthorized parties.
3. Any issues please contact me directly first do not post on the Thread.
4. You can sell the license with my approval and will cost you a fee of 1000$.
5. If you dont follow the rules it will result the termination of license without refunds.

But in an interview today with *The Record*, malware analyst 3xp0rt, who spotted the Osiris retirement post, said the shutdown announcement comes as the banking trojan has been seeing less and less usage among cybercriminal groups.

The last major spam campaign distributing a version of the Osiris trojan was spotted in January this year, targeting German users, the researcher said.

Since then, new Osiris campaigns have been rare, although some of Anubi's former customers appear to continue using it in some smaller-scale operations.

While the Osiris source code has not been leaked online, 3xp0rt told *The Record* that they believe that some of the malware's former clients will eventually resell it in second-market backroom deals as they stop using it for their own attacks and move to newer codebases.

New Kronos-variant spotted as Osiris died

But just as Anubi was announcing the Osiris retirement, security firm Zscaler also reported about a new banking trojan named Ares that was based on the old Kronos codebase and shared different components and similarities with the Osiris trojan.

Currently, it is unclear if Anubi is involved in the creation of this new trojan or if they handed over the codebase to a new developer who has now put their own spin on this dangerous malware.

Either way, the connections between the three malware strains are more than evident, although, according to Zscaler researchers, the Ares code is in early stages of development.

"The code contains several bugs and unreferenced code segments that are likely used for debugging purposes," they said. "The threat actor has invested significant resources in building DarkCrypter, BMPack, Ares, and Ares Stealer. Therefore, activity related to this threat is likely to increase as the malware continues to mature."

Featured image via [Rob Koopman](), [CC BY-ND 2.0]()

No previous article

No new articles

[Catalin Cimpanu]()

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.