# Moriya: An advanced and very dangerous 'stealth' Rootkit

Rootkit Moriya created by hackers in which country? Learn about Rootkit Moriya, why Rootkit Moriya is dangerous for Windows computer users

During 4 years of monitoring, from 2018 until now, Kaspersky's security experts still do not know who / which organization is behind Rootkit Moriya, friends.

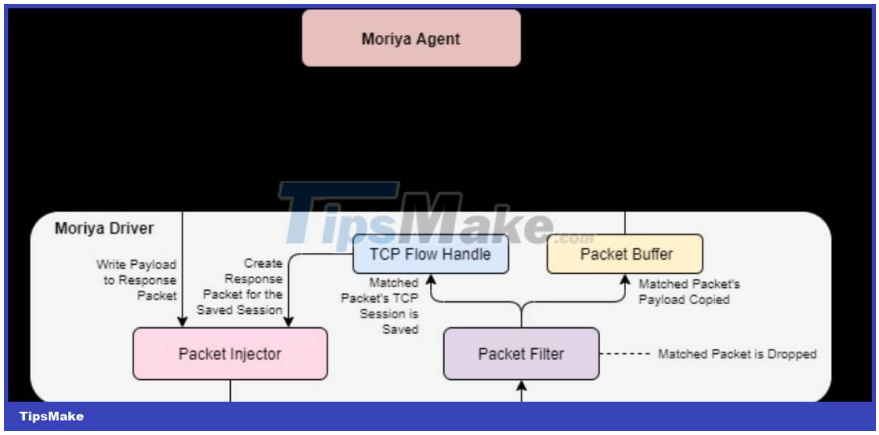

Kaspersky speculates that Moriya is part of an advanced APT (Advanced Persistent Threat) attack campaign called TunnelSnake operated by Chinese hackers.

TunnelSnake is said to have evolved a lot in terms of stealth or in other words stealth, comes with advanced auxiliary tools, and it is very well invested in infiltrating organizations. large, multinational/multi-region of Asia and Africa to sabotage and steal data.

## #first. Rootkit Moriya challenges Microsoft 's Windows operating system


It is sad that with Microsoft's constant efforts to improve the performance and security of the Windows operating system by constantly updating new and powerful features, it is still surpassed by this rootkit:

1. **Driver Signature Enforcement** to prevent malicious code execution in kernel space, modified/unsigned drivers will be blocked.
2. **Kernel Patch Protection (PatchGuard)** to prevent system files/programs from being modified. If malicious code tries to modify the system, the legendary Blue Screen of Death error on Windows will appear immediately.
3. Deeply integrate Windows Security security program into the system (from Firewall to anti-virus ability).



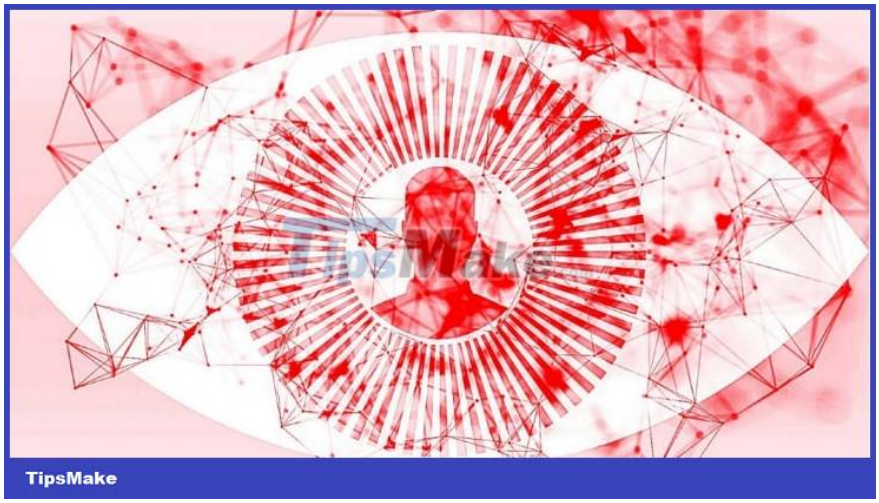

You should remember, Moriya is a rootkit, so once it gets into the system, almost every security mechanism of the operating system is manipulated by it.

Basically, because the rootkit operates in the Kernel space (a memory area containing the trusted code of the system kernel), every command it executes has absolute authority over the operating system. Like Administrator rights, the highest right.

It can install malicious drivers into the operating system to both ensure executable code is easily deployed (later) and has absolute system permissions.

With the ability to change I/O activities (files, network traffic) at the highest and earliest levels, it helps to create stealth armor for Moriya.

## #2. Moriya's Stealth Armor



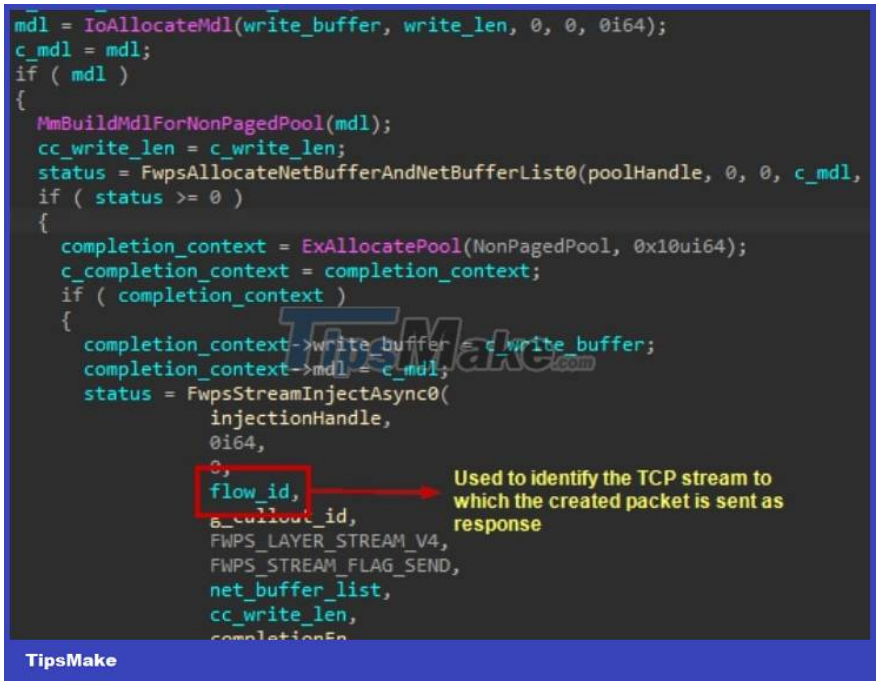

Malware in general is easily detected by constantly contacting C&C servers to receive execution orders, when these C&C servers are blacklisted by security firms, malware is easy to detect.

But the Moriya rootkit is different, it creates a Passive backdoor in the waiting area, but one thing is that the server in the victim's own network is the C&C server of the network!

In addition, it also has a hidden mechanism that makes security programs "cry", Moriya will filter network traffic packets (one step before any security program, because it is a rootkit) to see the packet. which contains the 'execution command' from the C&C server or intermediate zombie servers.

When it catches these packets, it immediately saves that 'instruction' to its own file/TCP stream for later reading, and then removes the 'command' from the packet.

Thus, network traffic/packets when reaching the hands of security programs will be just normal packets, combined with naming/impersonating tools/processes that are no different from Windows components, making Moriya can hide like a 'chameleon', friends.



# #3. Summary

– Rootkit Moriya was developed by Chinese hackers (not 100% sure) to create Passive backdoors on public servers of large organizations (Kaspersky has only discovered victims in Asia and Africa).

These Public servers (usually IIS web servers) will then be used to spread this Windows rootkit deeper into the organization through network scanning tools, exploit vulnerabilities, . and these servers will take care of it. always act as an intermediary C&C server.


– This rootkit was first discovered in 2018, active in October 2019 until May 2020, each attack usually lasts several months and then the rootkit erases its own traces.

South Asia is the most active region with a variant with many dangerous functions (used by the notorious Chinese hacker group APT1).

– This rootkit can easily disable security programs (anti-virus), so don't think that you have spent money to buy famous anti-virus software like Kaspersky or ESET.

If you can afford to pay for security, buy Internet Security (more advanced than anti-virus) – see why. And always remember to update the software as well as update the Windows operating system to the latest version on a regular basis!

You finished reading the article "**Moriya: An advanced and very dangerous 'stealth' Rootkit**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---