Security researchers at Symantec and Kaspersky identify a highly advanced piece of malware, one that has been stalking the world for years-- Regin, a customisable piece of software with a scarily wide array of capabilities.

Described by Symantec as nothing less than "groundbreaking and almost peerless," Regin is as sophisticated as the famous Stuxnet and Duqu malware, and possibly nastier than both. It has been around since at least 2008, runs within the kernel layer of Windows PCs and uses a complex architecture involving multiple layers of encryption and an own virtual filesystem.

"Customisable with an extensive range of capabilities depending on the target, it provides its controllers with a powerful framework for mass surveillance and has been used in spying operations against government organisations, infrastructure operators, businesses, researchers, and private individuals," the Symantec report on the malware reads. Meanwhile Kaspersky ominously describes it as "a cyber-attack platform which the attackers deploy in the victim networks for ultimate remote control at all possible levels."

In fact, security researchers suggest Regin is the product of nothing less than a nation-state, as nothing less can spare the time and resources to create such a beast. Not to mention Regin does not steal personal financial information or the like-- instead it collects intelligence from telecoms, government institutions, multi-national political bodies, financial institutions, research institutions and individuals involved in mathematical or cryptographically research. It can even hack through GSM phone networks, and can receive commands over cell networks.

To do so it installs many custom payloads, such as remote access trojans to swipe keystrokes and screenshots, tools to steal process information and memory utilization, and means to recover deleted files.

One famous Regin victim is Belgian cryptographer Jean Jacques Quisquater, who reported his being the victim of a "sophisticated cyber intrusion incident" in February 2014. Another interesting victim is "The Magnet of Threats," a PC belonging to a research institution used to attract advanced threats such as Turla, Mask/Careto, Itaduke and Animal Farm, as well as others lacking a public name.

Kaspersky identifies 14 countries under Regin attack, including Germany, Belgium, Russia, Algeria, Afghanistan, Pakistan and India, among others. Tellingly, none of the listed nations belong to the "Five Eyes" intelligence alliance (meaning the US, UK, Canada, Australia and New Zealand), pointing out either the NSA and UK intelligence agency GCHQ (or both) might have had a hand in its creation. In fact, one Regin victim is the Belgian telecom Belgacom, whose lines deliver traffic between Africa, the M. East and Africa.

So far none of the security experts can even start talking on a means to combat Regin, and infections appear to be ongoing. As such, expect the number of infections to continue growing.

Go Regin: Top Tier Espionage Tool Enables Stealthy Surveillance

Go Regin: Nation-State Ownage of GSM Networks

Go The Regin Espionage Toolkit