APT30 behind a long-running cyber espionage campaign

April 13, 2015 By Pierluigi Paganini

Researchers at FireEye uncovered a new threat actor dubbed APT30 that run a decade-long cyber espionage campaign backed by the Chinese Government.

Security experts at FireEye have uncovered a new long-running cyber espionage campaign, the researchers speculate that the campaign is active since at least 2005.

The threat actor behind the campaign was dubbed APT30 by the researchers, its operation involved seasoned high-skill software developers.

The APT30 group targeted various industries demonstrating a predilection for organizations involved in governmental intelligence activities. The APT30 targeted organizations located in Asian countries, including Malaysia, Vietnam, Thailand, Nepal, Singapore, Philippines and Indonesia.

> *"APT30 predominantly targets entities that may satisfy governmental intelligence collection requirements. The vast majority of APT30's victims are in Southeast Asia. Much of their social engineering efforts suggest the group is particularly interested in regional political, military, and economic issues, disputed territories, and media organizations and journalists who report on topics pertaining to China and the government's legitimacy" states the report published by FireEye.*

The researchers at FireEye explained that the APT30 uses three strains of malware specifically designed to infect and exfiltrate data from system inside air-gapped networks.

"While APT30 is certainly not the only group to build functionality to infect air-gapped networks into their operations, they appear to have made this a consideration at the very beginning of their development efforts in 2005, significantly earlier than many other advanced groups we track," continues the report.

The APT30 has many other tools in its arsenal that includes backdoors, malware with the ability to compromise air-gapped networks, downloaders and many others. Some of these tools were used only by the APT30 operators.

Figure 4: BACKSPACE controller GUI with sample victim data

Differently from other APT, hackers of the APT30 haven't changed their attack tools, tactics, and procedures (TTPs) over the years.

" The group (or the developers supporting them) systematically labels and keeps track of their malware versioning. The malware uses mutexes and events to ensure only a single copy is running at any given time, and the malware version information is embedded within the binary. Malware C2 communications include a version check that allows the malware to update itself to the latest copy, providing a continuous update management capability." states the report.

Who is behind the APT30?

By the analysis of the technical capabilities of the attackers, its TTPs, and the nature of the targets, the experts speculate that operations are backed by the Chinese government.

"Advanced threat group like APT 30 illustrate that state-sponsored cyber espionage affects a variety of governments and corporations across the world," explained Dan McWhorter, VP of threat intelligence at FireEye. "Given the consistency and success of APT 30 in Southeast Asia and India, the threat intelligence on APT 30 we are sharing will empower the region's governments and businesses to quickly begin to detect, prevent, analyze and respond to this established threat."

Pierluigi Paganini

(Security Affairs – APT30, FireEye)

Share this...

air gapped networks APT30 China cyber espionage FireEye Intelligence state sponsored hackers

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Hackers took over social media accounts of Iranian state Al Alam TV

NEXT ARTICLE
A global operation took down the Simda botnet

YOU MIGHT ALSO LIKE

Trump signed a bill to help small telecoms replace Huawei equipment

March 14, 2020 By Pierluigi Paganini

Most of the attacks on Telecom Sector in 2019 were carried out by China-linked hackers

March 5, 2020 By Pierluigi Paganini