TA505’s modified loader means new attack campaign could be coming

intel471.com/blog/ta505-get2-loader-malware-december-2020

After months of inactivity, hacking group TA505's Get2 Loader has sprung back into operation, possibly signaling that the group is ready for a new round of malicious activity.

On December 14, 2020, the Get2 loader had resurfaced with new download and execute configuration parameters named "LD" and "ED." Intel 471 last observed the loader in operation on September 14, 2020.

The "LD" parameter reflectively loads a downloaded dynamic-link library (DLL) file into the address space of the current process and calls its entry point. The "ED" parameter copies the DLL into executable memory and invokes the entry point directly. The preexisting "RD" parameter that was used to inject the downloaded DLL into EXCEL.EXE can now perform injection into WINWORD.EXE as well.

The reconfigured loader is meant to allow the group to carry out its operations without drawing the attention of enterprise defenses. In the past, it has been used to download the SDBbot, FlawedGrace and other malware.

TA505 is a prolific Russian-speaking, financially-motivated group that is known for launching large-scale targeted attacks. The group was most recently discovered going after German-speaking targets with weaponized CVs. Intel 471 also observed the group going after targets in Japan, South Korea, United Arab Emirates in 2019. Once the group's malware or actions are caught by researchers or the press, the group tends to go silent in an effort to reconfigure its tools.

Drawing from past experiences, Intel 471 believes that new, undiscovered malware campaigns will follow with the introduction of the reconfigured Get2 Loader.

"TA505 can be somewhat deliberate in how they operate, more so than most of the financially-motivated groups we track," said Intel 471 COO Jason Passwaters. "Once things start ramping up like this, rest assured they are back at it with a target list in hand."

The Intel 471 adversary intelligence on major threat groups such as TA505 and our unique insight into its capabilities, intent and motivations, can be leveraged by threat intelligence teams to remain proactive and resilient against attacks as cybercriminals modify TTPs.