BIZCOMMUNITY

Beware of MiniDuke

MOSCOW, RUSSIA: Kaspersky Lab has identified 'MiniDuke', a new malicious programme designed for spying on multiple government entities and institutions across the world. The new threat actors combine sophisticated "old school" malware writing skills with newly advanced exploits in Adobe Reader to collect geopolitical intelligence from high-profile targets.

Kaspersky Lab's team of experts has published a new research report that analysed a series of security incidents involving the use of the recently discovered PDF exploit in Adobe Reader (CVE-2013-6040) and a new, highly customised malicious programme known as MiniDuke. The MiniDuke backdoor was used to attack multiple government entities and institutions worldwide during the past week. Kaspersky Lab's experts, in partnership with CrySys Lab, analysed the attacks in detail and published their findings.

According to Kaspersky Lab's analysis, a number of high-profile targets have already been compromised by the MiniDuke attacks, including government entities in Ukraine, Belgium, Portugal, Romania, the Czech Republic and Ireland. In addition, a research institute, two think tanks, and a healthcare provider in the United States were also compromised, as was a prominent research foundation in Hungary.

An unusual attack

"This is a very unusual cyber attack," said Eugene Kaspersky, founder and CEO of Kaspersky Lab. "I remember this style of malicious programming from the end of the 1990s and the beginning of the 2000s. I wonder if these types of malware writers, who have been in hibernation for more than a decade, have suddenly awoken and joined the sophisticated group of threat actors active in the cyber world. These elite, 'old-school' malware writers were extremely effective in the past at creating highly complex viruses, and are now combining these skills with the newly advanced sandbox-evading exploits to target government entities or research institutions in several countries."

"MiniDuke's highly customised backdoor was written in Assembler and is very small in size, being only 20kb," added Kaspersky. "The combination of experienced old school malware writers using newly discovered exploits and clever social engineering to compromise high profile targets is extremely dangerous."

Kaspersky Lab's primary research findings:

- The MiniDuke attackers are still active at this time and have created malware as recently as 20 February 2013. To compromise victims, the attackers used extremely effective social engineering techniques, which involved sending malicious PDF documents to their targets. The PDFs were highly relevant - with well-crafted content that fabricated human rights seminar information (ASEM) and Ukraine's foreign policy and NATO membership plans. These malicious PDF files were rigged with exploits attacking Adobe Reader versions 9, 10, and 11, bypassing its sandbox. A toolkit was used to create these exploits and it appears to be the same toolkit that was used in the recent attack reported by FireEye. However, the exploits used in the MiniDuke attacks were for different purposes and had their own customised malware.
- Once the system is exploited, a very small downloader is dropped onto the victim's disc that's only 20kb in size. This downloader is unique per system and contains a customised backdoor written in Assembler. When loaded at system boot, the downloader uses a set of mathematical calculations to determine the computer's unique fingerprint, and in turn uses this

data to encrypt its communications uniquely later. It is also programmed to avoid analysis by a hard coded set of tools in certain environments like VMware. If it finds any of these indicators it will run idle in the environment instead of moving to another stage and exposing more of its functionality by decrypting itself further; this indicates the malware writers know exactly what antivirus and IT security professionals are doing in order to analyse and identify malware.

- If the target's system meets the pre-defined requirements, the malware will use Twitter (unbeknownst to the user) and start looking for specific tweets from pre-made accounts. These accounts were created by MiniDuke's Command and Control (C2) operators, and the tweets maintain specific tags labelling encrypted URLs for the backdoors. These URLs provide access to the C2s, which then provide potential commands and encrypted transfers of additional backdoors onto the system via GIF files.
- Based on the analysis, it appears that MiniDuke's creators provide a dynamic backup system that also can fly under the radar. If Twitter isn't working or the accounts are down the malware can use Google Search to find the encrypted strings to the next C2. This model is flexible and enables the operators to constantly change how their backdoors retrieve further commands or malcode as needed.
- Once the infected system locates the C2, it receives encrypted backdoors that are obfuscated within GIF files and disguised as pictures that appear on a victim's machine. Once they are downloaded to the machine they can download a larger backdoor that carries out several basic actions, such as copy file, move file, remove file, make directory, kill process, and, of course, download and execute new malware.
- The malware backdoor connects to two servers, one in Panama and one in Turkey, to receive instructions from the attackers.

To read the full research report by Kaspersky Lab and the recommendations for protecting against MiniDuke attacks, please visit Securelist.

To read CrySys Lab's report, visit this page.

Kaspersky Lab's system detects and neutralises the MiniDuke malware, classified as HEUR:Backdoor.Win32.MiniDuke.gen and Backdoor.Win32.Miniduke. Kaspersky Lab also detects the exploits used in the PDF documents, classified as Exploit.JS.Pdfka.giy.