Kaspersky Lab says Muddy Water extends attacks towards government targets in Asia, Europe and Africa

Kaspersky Lab researchers monitoring the activity of Muddy Water, an advanced threat actor first seen targeting Iraq and Saudi Arabia in 2017, have uncovered a massive operation focused on government entities and more in Jordan, Turkey, Azerbaijan, Pakistan and Afghanistan, alongside its original targets. The malware is distributed through a highly personalized spear-phishing campaign featuring office documents and asking users to enable embedded macros. The attacks are ongoing.

Muddy Water is a relatively new threat actor that surfaced in 2017 with a campaign focused on government targets in Iraq and Saudi Arabia. Earlier this year, Kaspersky Lab researchers detected a continuous stream of spear-phishing emails targeting a much wider range of countries than previously seen for this threat actor. The campaign peaked in May and June 2018, but is still ongoing.

The content of the spear-phishing messages suggests the main targets are government and military entities, telecoms companies and educational institutions. The emails carry an MS Office 97-2003 file attachment and infection is activated as soon as the user has been persuaded to enable macros.

Kaspersky Lab researchers have analyzed the first stages of the attack and are publishing their findings now in order to help organizations across the target regions to protect themselves. The investigation continues into the attackers' arsenal of PowerShell, VBS, VBA, Python and C# scripts, tools and RATs (Remote Access Trojans).

Once the infection is activated, the malware establishes contact with its command server by picking a random URL from an embedded list. After scanning for the presence of security software, the malware drops a number of scripts onto the victim computer, with a final PowerShell payload establishing basic backdoor functionality and destructive capabilities (the ability to delete files). The use of legitimate MS files means the malware can bypass any blacklisting. In addition, the PowerShell code disables the 'Macro Warnings' and 'Protected View' features to ensure future attacks will not require any user interaction. The malware's infrastructure comprises a range of compromised hosts.

Attack targets were detected in Turkey, Jordan, Azerbaijan, Iraq and Saudi Arabia, as well as in Mali, Austria, Russia, Iran, and Bahrain.

It is not known for certain who is behind the Muddy Water operation, although the attacks are clearly geopolitically motivated, targeting sensitive personnel and organizations. The code used in the current attacks carries a number of features that appear designed to distract and mislead investigators. This includes the insertion of Chinese into the code and the use of names such as Leo, PooPak, Vendetta and Turk in the malware.

"Over the last year, we have seen the Muddy Water group implement a large number of attacks, as well as the continuous development of new methods and techniques. The group has active developers improving its toolkit in order to minimize exposure to security products and services.

This suggests to us that this type of attack is likely to intensify in the short term. That is why we decided to share our first findings publicly – to raise awareness of the threat so that organizations can take action to defend themselves. We are still analysing the attackers' arsenal and will keep a close eye on their progression, their strategies and their mistakes." said Amin Hasbini, senior security researcher at Kaspersky Lab's GReAT team.

Kaspersky Lab recommends that to reduce the risk of falling victim to operations like Muddy Water, organizations may wish to consider the following actions:

-Implement a comprehensive approach to the detection, prevention and investigation of targeted attacks, involving advanced anti-targeted attack security solutions and training.

-Provide security staff with access to the latest threat intelligence data, which will arm them with helpful tools for targeted attack prevention and discovery, such as indicators of compromise and YARA rules.
Make sure enterprise grade patch management processes are well established.

-Double check all system configurations and implement best practices.

-Educate staff on how to spot and what to do when they receive a suspicious email.

For further details of the first stages of this Muddy Water operation, including indicators of compromise, read the blog on Securelist. https://securelist.com/muddywater/88059