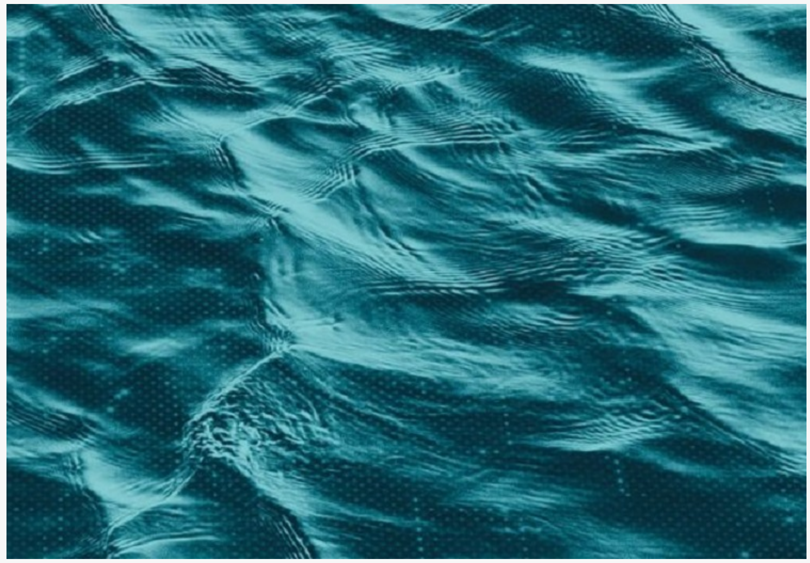
APT groups muddying the waters for MSPs



DUBAI, UNITED ARAB EMIRATES, May 4, 2023 /EINPresswire.com/ -- James Shepperd, Content Manager at ESET takes a quick dive into the murky world of cyberespionage and other growing threats facing managed service providers – and their customers

ESET telemetry from Q4 2022 saw the start of a new campaign by MuddyWater, a cyberespionage group linked to Iran's Ministry of Intelligence and Security (MOIS) and active since at least 2017. The group (primarily) targets victims in the Middle East, Asia, Africa, Europe, and North America, focusing on telecommunications companies, governmental organizations, and the oil & gas and energy verticals.

For the MSP-interested reader, what stands out in their October 2022 campaign is that four victims, three in Egypt and one in Saudi Arabia, were compromised via the abuse of SimpleHelp, a legitimate remote access tool (RAT) and remote support software used by MSPs. This development signals the importance of visibility for MSPs. In deploying hundreds or even thousands of software types have no choice but to employ automation and ensure that SOC teams, customer-facing security admins, and detection and response processes are mature and constantly improving.

Good tools for bad guys?
ESET Research discovered that when SimpleHelp was present on a victim's disk, MuddyWater operators deployed Ligolo, a reverse tunnel, to connect the victim's system to their Command and Control (C&C) servers. How and when MuddyWater came into possession of the MSP's tooling or entered the MSP's environment is unknown. We have reached out to the MSP.

While this campaign continues, MuddyWater's use of SimpleHelp has, thus far, successfully obfuscated the MuddyWater C&C servers – the commands to initiate Ligolo from SimpleHelp have not been captured. Regardless, we can already note that MuddyWater operators are also pushing MiniDump (an lsass.exe dumper), CredNinja, and a new version of the group's password dumper MKL64.

In late October 2022, ESET detected MuddyWater deploying a custom reverse tunneling tool to the same victim in Saudi Arabia. While its purpose was not immediately apparent, the analysis continues, and progress can be tracked in our private APT Reports.

Alongside using MiniDump to obtain credentials from Local Security Authority Subsystem Service (LSASS) dumps and leveraging the CredNinja penetration testing tool, MuddyWater sports other tactics and techniques, for example, using popular MSP tools from ConnectWise to gain access to victims' systems.

ESET has also tracked other techniques connected to the group, such as steganography, which obfuscates data in digital media such as images, audio tracks, video clips, or text files. A 2018 report from ClearSky Cyber Security, MuddyWater Operations in Lebanon and Oman, also documents this usage, sharing hashes for malware hidden in several fake resumes – MyCV.doc. ESET detects the obfuscated malware as VBA/TrojanDownloader.Agent.

While four years have passed since the publication of the ClearSky report, and the volume of ESET detections fell from seventh position (with 3.4%) in T3 2021 Threat Report to their most recent ranking in "last" position (with 1.8%) in T3 2022 Threat Report, VBA/TrojanDownloader.Agent remained in our top 10 malware detections chart.

VBA macros attacks leverage maliciously crafted Microsoft Office files and try to manipulate users (including MSP employees and clients) into enabling the execution of macros. If enabled, the enclosed malicious macro typically downloads and executes additional malware. These malicious documents are usually sent as email attachments disguised as important information relevant to the recipient.

A call to action for MSPs and enterprises

MSP Admins, who configure leading productivity tools like Microsoft Word/Office 365/Outlook, run their hands over the very threat vectors carrying threats to the networks they manage. Simultaneously, SOC team members may or may not have their own EDR/XDR tools well configured to identify whether APTs like MuddyWater or criminal entities are attempting to leverage techniques, including steganography, to access their own or clients' systems.

MSPs require both trusted network connectivity and privileged access to customer systems in order to provide services; this means they accumulate risk and responsibility for large numbers of clients. Importantly, clients can also inherit risks from their chosen MSP's activity and environment. This has shown XDR to be a critical tool in supplying visibility into both their own environments and customer endpoints, devices, and networks to ensure that emerging threats, risky employee behavior, and unwanted applications do not risk their profits or reputation. The mature operation of XDR tools by MSPs also communicates their active role in providing a specific layer of security for the privileged access granted to them by clients.

When mature MSPs manage XDR, they are in a much better position to counter a diversity of threats, including APT groups that might seek to leverage their clients' position in both physical and digital supply chains. As defenders, SOC teams and MSP admins carry a double burden, maintaining internal visibility and visibility into clients' networks. Clients should be concerned about the security stance of their MSPs and understand the threats they face, lest a compromise of their provider leads to a compromise of themselves.

Sanjeev Kant
Vistar Communications
0559724623
email us here
