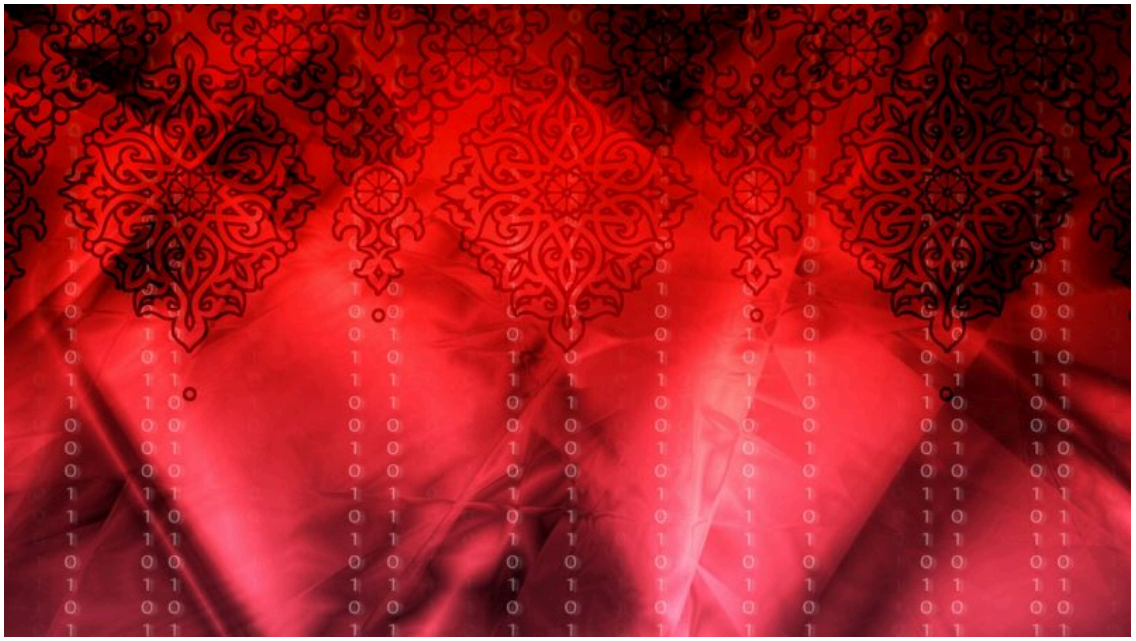
Lyceum group reborn

By Mark Lechtik

Published: 2021-10-18 · Archived: 2026-04-05 18:12:03 UTC

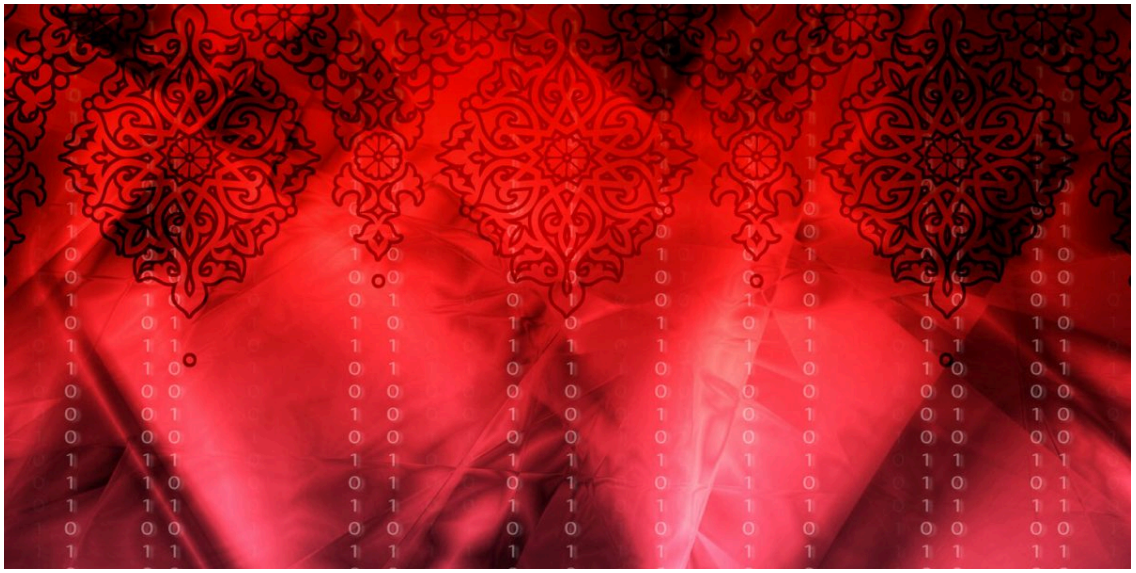


APT reports

APT reports

18 Oct 2021

1 minute read



This year, we had the honor to be selected for the thirty-first edition of the Virus Bulletin conference. During the live program, we presented our research into the Lyceum group (also known as Hexane), which was first exposed by Secureworks in 2019. In 2021, we have been able to identify a new cluster of the group's activity, focused on two entities in Tunisia.

According to older public accounts of the group's activity, Lyceum conducted targeted operations against organizations in the energy and telecommunications sectors across the Middle East, during which the threat actor used various PowerShell scripts and a .NET-based remote administration tool referred to as "DanBot". The latter supported communication with a C&C server via custom-designed protocols over DNS or HTTP.

Our investigation into Lyceum has shown that the group has evolved its arsenal over the years and shifted its usage from the previously documented .NET malware to new versions, written in C++. We clustered those new pieces of malware under two different variants, which we dubbed "James" and "Kevin", after recurring names that appeared in the PDB paths of the underlying samples.

As in the older DanBot instances, both variants supported similar custom C&C protocols tunneled over DNS or HTTP. That said, we also identified an unusual variant that did not contain any mechanism for network communication. We assume that it was used as a means to proxy traffic between two internal network clusters. Our paper elaborates on the C&C protocol mechanics, the timeline of using the variants and the differences between them.

In addition to the revealed implants, our analysis allowed us to get a glance into the actor's modus operandi. Thus, we observed some of the commands the attackers used within the compromised environments, as well as the actions taken to steal user credentials. These included the use of a PowerShell script designed to steal credentials stored in browsers and a custom keylogger deployed on some of the targeted machines.

Finally, we noticed certain similarities between Lyceum and the infamous DNSpionage group, which, in turn, was associated with the OilRig cluster of activity. Besides similar geographical target choices, and the use of DNS or fake websites to tunnel C&C data as a TTP, we were able to trace significant similarities between lure documents delivered by Lyceum in the past and those used by DNSpionage. These were made evident through a common code structure and choices of variable names.

Our presentation from the conference, detailing some of the aspects described above, can be viewed here:

An even more detailed outline with technical specifics can be found in the paper that accompanied the presentation, now available on the Virus Bulletin website.

- 

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
