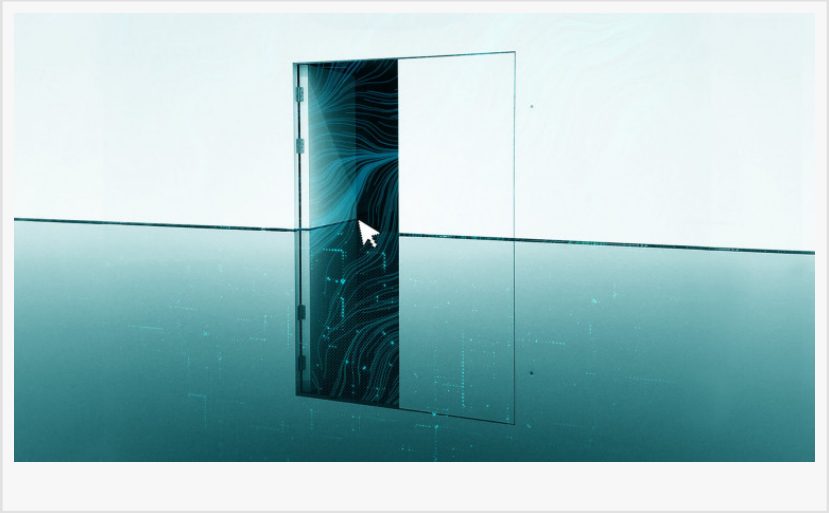
ESET Research: Iran-aligned Ballistic Bobcat targets businesses in Israel with a new backdoor



DUBAI, DUBAI, UNITED ARAB EMIRATES, September 15, 2023 /EINPresswire.com/ -- ESET researchers have discovered a campaign by the Ballistic Bobcat group, which is using a novel backdoor that ESET has named Sponsor. Ballistic Bobcat, previously tracked by ESET Research as APT35/APT42 (also known as Charming Kitten, TA453, or PHOSPHORUS), is a suspected Iran-aligned, advanced, persistent threat group that targets education, government, and healthcare organizations, as well as human rights activists and journalists. It is most active in Israel, the Middle East, and the United States. Its aim is cyberespionage, and a significant majority of the 34 victims were located in Israel, with only two located in Brazil and the UAE. In Israel, automotive, manufacturing, engineering, financial services, media, healthcare, technology and telecommunications verticals have been attacked.

For 16 of the 34 victims of the newly discovered campaign, named Sponsoring Access, it appears that Ballistic Bobcat was not the only threat actor with access to their systems. This may indicate, along with the wide variety of victims and the apparent lack of obvious intelligence value of a few victims, that Ballistic Bobcat engaged in scan-and-exploit behavior, as opposed to a targeted campaign against preselected victims.

Thus, Ballistic Bobcat continues to look for targets of opportunity with unpatched vulnerabilities in internet-exposed Microsoft Exchange servers. “The group continues to use a diverse, open-source toolset supplemented with several custom applications, including the newly discovered Sponsor backdoor. Defenders would be well advised to patch any internet-exposed devices and remain vigilant for new applications popping up within their organizations,” says ESET researcher Adam Burgher, who discovered the Sponsor backdoor and analyzed the latest Ballistic Bobcat campaign.

The Sponsor backdoor uses configuration files stored on disk. These files are discreetly deployed by batch files, and deliberately designed to appear innocuous, in an attempt to evade detection by scanning engines. Ballistic Bobcat deployed the new backdoor in September 2021, while it was wrapping up the campaign documented in CISA Alert AA21-321A and the PowerLess campaign.

During the pandemic, Ballistic Bobcat was targeting COVID-19-related organizations, including the World Health Organization and Gilead Pharmaceuticals, and medical research personnel.

For more technical information about Ballistic Bobcat and its Sponsoring Access campaign, check out the blogpost, "Sponsor with batch-filed whiskers: Ballistic Bobcat's scan and strike backdoor," on WeLiveSecurity. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

Sanjeev Kant
Vistar Communications
0559724623
email us here
