ESET Research discovers MoustachedBouncer targeting European and other diplomats in Belarus via network tampering

DUBAI, UNITED ARAB EMIRATES, August 14, 2023 /EINPresswire.com/ -- ESET Research has discovered a new cyberespionage group, MoustachedBouncer. It is named after its presence in Belarus and is aligned with the interests of the local government. Active since at least 2014, the group targets only foreign embassies, including European ones, in Belarus. Since 2020, MoustachedBouncer has most likely been able to perform adversary-in-the-middle (AitM) attacks at the ISP level, within Belarus, in order to compromise its targets. The group uses two separate toolsets that ESET has named NightClub and Disco. The research was exclusively presented during the Black Hat USA 2023 conference on August 10, 2023, by ESET researcher Matthieu Faou.

According to ESET telemetry, the group targets foreign embassies in Belarus, and ESET has identified four countries whose embassy staff have been targeted: two from Europe, one from South Asia, and one from Africa. ESET assesses that MoustachedBouncer is very likely aligned with Belarus interests and specializes in espionage, specifically against foreign embassies in Belarus. MoustachedBouncer uses advanced techniques for Command and Control (C&C) communications, including network interception at the ISP level for the Disco implant, emails for the NightClub implant, and DNS in one of the NightClub plugins.

While ESET Research tracks MoustachedBouncer as a separate group, we have found elements that make ESET assess with low confidence that it is collaborating with another active espionage group, Winter Vivern, which has targeted government staff of several European countries, including Poland and Ukraine, in 2023.

To compromise their targets, MoustachedBouncer operators tamper with their victims' internet access, probably at the ISP level, to make Windows believe it's behind a captive portal. For IP

ranges targeted by MoustachedBouncer, network traffic is redirected to a seemingly legitimate, but fake, Windows Update page," says ESET researcher Matthieu Faou, who discovered the new threat group. "This adversary-in-the-middle technique occurs only against a few selected organizations, perhaps just embassies, not countrywide. The AitM scenario reminds us of the Turla and StrongPity threat actors, who have trojanized software installers on the fly at the ISP level."

"While the compromise of routers in order to conduct AitM attacks on embassy networks cannot be fully discarded, the presence of lawful interception capabilities in Belarus suggests the traffic mangling is happening at the ISP level rather than on the targets' routers," explains the ESET researcher.

Since 2014, the malware families used by MoustachedBouncer have evolved, and a big change happened in 2020, when the group started to use adversary-in-the-middle attacks. MoustachedBouncer operates the two implant families in parallel, but on a given machine, only one is deployed at a time. ESET believes that Disco is used in conjunction with AitM attacks, while NightClub is used for victims where traffic interception at the ISP level isn't possible because of a mitigation such as the use of an end-to-end encrypted VPN where internet traffic is routed outside of Belarus.

"The main takeaway is that organizations in foreign countries where the internet cannot be trusted should use an end-to-end encrypted VPN tunnel to a trusted location for all their internet traffic in order to circumvent any network inspection devices. They should also use top-quality, updated computer security software," advises Faou.

The NightClub implant uses free email services, namely the Czech webmail service Seznam.cz and the Russian Mail.ru webmail provider, to exfiltrate data. ESET believes the attackers created their own email accounts, instead of compromising legitimate ones.

The threat group focuses on stealing files and monitoring drives, including external ones. The capabilities of NightClub also include audio recording, taking screenshots, and logging keystrokes.

For more technical information about MoustachedBouncer, check out the blog post "MoustachedBouncer: Espionage against foreign diplomats in Belarus" on WeLiveSecurity. Make sure to follow ESET Research on Twitter (X) for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in

real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
