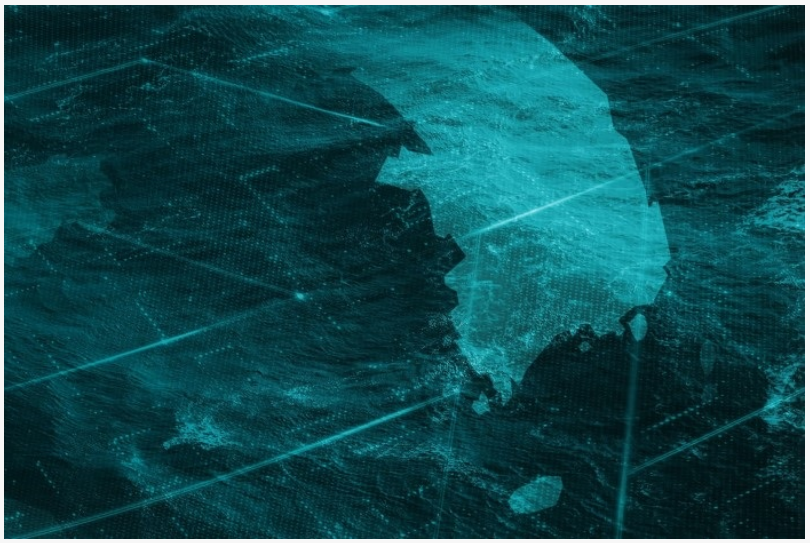
ESET Research: N Korea-linked group launches Dolphin backdoor, steals files of interest, communicates via Google Drive



DUBAI, UNITED ARAB EMIRATES, December 6, 2022 /EINPresswire.com/ -- ESET researchers analyzed a previously unreported sophisticated backdoor used by the ScarCruft APT group. The backdoor, which ESET named Dolphin, has a wide range of spying capabilities, including monitoring drives and portable devices, exfiltrating files of interest, keylogging, taking screenshots, and stealing credentials from browsers. Its functionality is reserved for selected targets, to which the backdoor is deployed after initial compromise using less advanced malware. Dolphin abuses cloud storage services — specifically Google Drive — for Command and Control communication.

ScarCruft, also known as APT37 or Reaper, is an espionage group that has been operating since at least 2012. It primarily focuses on South Korea, but other Asian countries have also been targeted. ScarCruft seems to be interested mainly in government and military organizations, and companies in various industries linked to the interests of North Korea.

“After being deployed on selected targets, it searches the drives of compromised systems for interesting files and exfiltrates them to Google Drive. One unusual capability found in prior versions of the backdoor is the ability to modify the settings of victims’ Google and Gmail accounts to lower their security, presumably to maintain Gmail account access for the threat actors,” says ESET researcher Filip Jurčacko, who analyzed the Dolphin backdoor.

In 2021, ScarCruft conducted a watering-hole attack on a South Korean online newspaper focused on North Korea. The attack consisted of multiple components, including an Internet Explorer exploit and shellcode leading to a backdoor named BLUELIGHT.

“In the previous reports, the BLUELIGHT backdoor was described as the attack’s final payload. However, when analyzing the attack, we discovered through ESET telemetry a second, more sophisticated backdoor deployed on selected victims via this first backdoor. We named this backdoor Dolphin based on a PDB path found in the executable,” explains Jurčacko.

Since the initial discovery of Dolphin in April 2021, ESET researchers have observed multiple versions of the backdoor, in which the threat actors improved the backdoor’s capabilities and made attempts to evade detection.

While the BLUELIGHT backdoor performs basic reconnaissance and evaluation of the compromised machine after exploitation, Dolphin is more sophisticated and manually deployed only against selected victims. Both backdoors are capable of exfiltrating files from a path specified in a command, but Dolphin also actively searches drives and automatically exfiltrates files with interesting extensions.

The backdoor collects basic information about the targeted machine, including the operating system version, malware version, list of installed security products, username, and computer name. By default, Dolphin searches all fixed (HDD) and non-fixed drives (USBs), creates directory listings, and exfiltrates files by extension. Dolphin also searches portable devices, such as smartphones, via the Windows Portable Device API. The backdoor also steals credentials from browsers, and is capable of keylogging and taking screenshots. Finally, it stages this data in encrypted ZIP archives before uploading to Google Drive.

For more technical information about the latest ScarCruft APT group campaign, check out the blogpost “Who’s swimming in South Korean waters? Meet ScarCruft’s Dolphin” on WeLiveSecurity. Make sure to follow ESET Research on Twitter 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