ESET Research investigates Donot Team: Cyberespionage targeting military & governments in South Asia

eset.com/int/about/newsroom/press-releases/research/eset-research-investigates-donot-team-cyberespionage-targeting-military-governments-in-south-asia/

Editor18 Jan 2022

- ESET has analyzed two variants of the yty malware framework: Gedit and DarkMusical. ESET researchers have decided to call one of the variants DarkMusical because many of the names the attackers chose for their files and folders are inspired by the movie High School Musical.
- These attacks are focused on government and military organizations, Ministries of Foreign Affairs, and embassies and are motivated by cyberespionage.
- Targets are primarily located in South Asia – Bangladesh, Sri Lanka, Pakistan and Nepal. However, targeting embassies of these countries in other regions, such as the Middle East, Europe, North America, and Latin America, has been observed.
- ESET's investigation spans more than a year from September 2020 to October 2021.
- A recent report by Amnesty International links the group's malware to an Indian cybersecurity company that may be selling the spyware.
- The group has consistently targeted the same organizations for at least the last two years and it's possible that the attackers have compromised the email accounts of some of their victims.

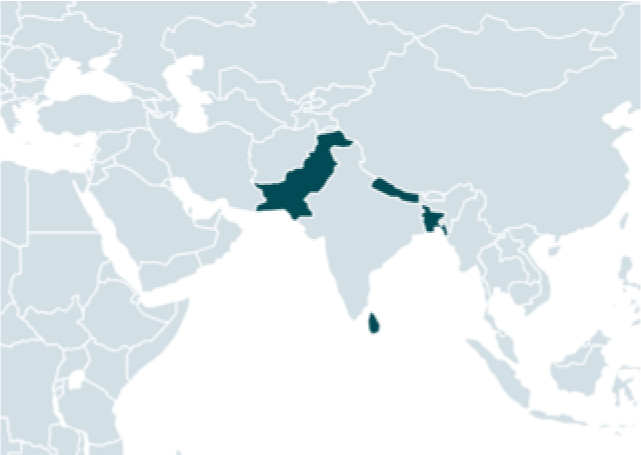
BRATISLAVA, MONTREAL — January 18, 2022 — ESET researchers have uncovered recent campaigns and an updated threat arsenal of the infamous APT group Donot Team (also known as APT-C-35 and SectorE02). According to research findings, the group is very persistent and has consistently targeted the same organizations for at least the last two years. For this research, ESET monitored Donot Team for more than a year from September 2020 to October 2021. According to ESET telemetry, the APT group focuses on a small number of targets primarily in South Asia — Bangladesh, Sri Lanka, Pakistan and Nepal. However, targeting embassies of these countries in other regions, such as the Middle East, Europe, North America, and Latin America, is not outside the group's realm. These attacks are focused on government and military organizations, Ministries of Foreign Affairs, and embassies and are motivated by cyberespionage.

Donot Team is a threat actor operating since at least 2016 that is known for targeting organizations and individuals in South Asia with Windows and Android malware. A recent report by Amnesty International links the group's malware to an Indian cybersecurity company that may be selling the spyware or offering a hackers-for-hire service to governments of the region.

“We have been closely following the activities of Donot Team, and have traced several campaigns that leverage Windows malware derived from the group’s signature yty malware framework,” says ESET researcher Facundo Muñoz, who led the investigation into the group’s activities.

The main purpose of the “yty” malware framework is to collect and exfiltrate data. The malicious framework consists of a chain of downloaders that ultimately download a backdoor with minimal functionality, used to download and execute further components of Donot Team’s toolset. These include file collectors based on file extension and year of creation, screen capturers, keyloggers, reverse shells, and more.

Countries targeted in recent Donot Team campaigns



According to ESET telemetry, Donot Team has been consistently targeting the same entities with waves of spearphishing emails every two to four months. The spearphishing emails have malicious Microsoft Office documents attached that the attackers use to deploy their malware.

Interestingly, the emails that ESET researchers were able to retrieve and analyze did not show signs of spoofing. “Some emails were sent from the same organizations that were being attacked. It’s possible that the attackers may have compromised the email accounts of some of their victims in earlier campaigns, or the email server used by those organizations,” says Muñoz.

In the latest blogpost, ESET has analyzed two variants of the yty malware framework: Gedit and DarkMusical. ESET researchers have decided to call one of the variants DarkMusical because of the names the attackers chose for their files and folders: many are western celebrities or characters in the movie High School Musical. This variant was used in campaigns targeting military organizations in Bangladesh and Nepal.

For more technical details about the Donot Team’s latest campaigns, read the blogpost “DoNot Go! Do not respawn!” 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.