Russia-Linked APT28 group observed using DDE attack to deliver malware

By Pierluigi Paganini

Published: 2017-11-09 · Archived: 2026-04-06 01:31:01 UTC

Pierluigi Paganini November 09, 2017

Security experts at McAfee observed the Russian APT28 group using the recently reported the DDE attack technique to deliver malware in espionage campaign.

Security experts at McAfee observed the Russian APT group APT28 using the recently reported the DDE technique to deliver malware in targeted attacks**.**

The cyber spies were conducting a cyber espionage campaign that involved blank documents whose name referenced the recent terrorist attack in New York City.

"During our monitoring of activities around the APT28 threat group, McAfee Advanced Threat Research analysts identified a malicious Word document that appears to leverage the Microsoft Office Dynamic Data Exchange (DDE) technique that has been previously reported by Advanced Threat Research. This document likely marks the first observed use of this technique by APT28*." reported McAfee.*

The Dynamic Data Exchange (DDE) is a protocol designed to allow data transferring between applications, attackers have devised a method to achieve the execution of malicious code embedded in Office documents without user's interaction by using DDE.

The DDE protocol allows an Office application to load data from another Office application, it was replaced by Microsoft with Object Linking and Embedding (OLE), but it is still supported.

The DDE technique was implemented by several threat actors such as the FIN7 APT group in DNSMessenger malware attacks, and the operators behind the Hancitor malware campaign spotted and detailed by Internet Storm Center (ISC) handler Brad Duncan.

Recently the technique was used by threat actors behind the Necurs botnet to deliver the Locky ransomware.

Unfortunately, Microsoft doesn't plan to introduce security countermeasures to mitigate the DDE attack because the tech giant considers the feature as legit.

In the recent campaign conducted by APT28, hackers used a document referencing the New York City attack to deliver the first-stage payload tracked as Seduploader.

The Seduploader malware, also known as GAMEFISH backdoor, Sednit, JHUHUGIT and Sofacy, is a strain of malware that has been already used by the threat actor in other campaigns against NATO representatives.

The Seduploader is a reconnaissance malware that was used for years by APT28, it is composed of 2 files: a dropper and a payload.

The malware is downloaded from a remote server using PowerShell commands, experts

The analysis of the malware and command and control (C&C) domains used in the campaign revealed the campaign involving DDE started on October 25.

According to the experts, the recent attacks are part of a campaign that also involved documents referencing Saber Guardian, a multinational military exercise involving approximately 25,000 military personnel from over 20 participating nations. The military exercise was conducted by the U.S. Army in Eastern Europe in an effort to deter an invasion (by Russia) into NATO territory.

Just two week ago, researchers with Cisco Talos have spotted another cyber espionage campaign conducted by the APT28 group targeting individuals with spear-phishing messages using documents referencing a NATO cybersecurity conference.

The hackers targeted individuals with a specific interest in the CyCon US cybersecurity conference organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in collaboration with the Army Cyber Institute at West Point on November 7-8 in Washington, D.C.

"APT28 is a resourceful threat actor that not only capitalizes on recent events to trick potential victims into infections, *but can also rapidly incorporate new exploitation techniques to increase its success. Given the publicity the Cy Con U.S campaign received in the press, it is possible APT28 actors moved away from using the VBA script employed in past actions and chose to incorporate the DDE technique to bypass network* defenses." *concluded McAfee. "Finally, the use of recent domestic events and a prominent US military exercise focused on deterring Russian aggression highlight APT28's ability and interest in exploiting geopolitical events for their operations."*

[adrotate banner="9″]	**[adrotate banner="12″]**

Pierluigi Paganini

(Security Affairs – DDE attack, cyber espionage)

[adrotate banner="5″]

[adrotate banner="13″]

Source: http://securityaffairs.co/wordpress/65318/hacking/dde-attack-apt28.html