https://www.securityweek.com/cozyduke-apt-responsible-white-house-state-department-attacks-kaspersky

# CozyDuke APT Behind White House, State Department Attacks: Kaspersky

April 22, 2015

An advanced persistent threat (APT) actor dubbed “CozyDuke” (also known as CozyBear and CozyCar) is believed to be responsible for recent cyberattacks targeting the US Department of State and the White House, according to Kaspersky Lab.

In a blog post containing numerous technical details on the group’s tools and activities, Kaspersky researchers revealed that the APT actor targeted various high-profile organizations in the second half of 2014.

According to the security firm, CozyDuke shares similarities with components spotted in previously documented APTs such as MiniDuke, CosmicDuke and OnionDuke.

In some of its attacks, CozyDuke used spear-phishing emails containing links to compromised websites hosting malware. In other operations, the attackers relied on malicious Flash videos attached directly to emails in order to deliver malware.

“A clever example is ‘Office Monkeys LOL Video.zip’. The executable within not only plays a flash video, but drops and runs another CozyDuke executable. These videos are quickly passed around offices with delight while systems are infected in the background silently,“ Kaspersky researchers explained.

Once it infects a system, the malware checks for the presence of security products from Kaspersky, Crystal Security, Sophos, Dr. Web, Avira, and Comodo. Researchers have noted that many of the malware components used in CozyDuke attacks are signed with fake Intel and AMD digital certificates.

Kaspersky experts have determined that one of the second stage CozyDuke modules has been built on the same platform as the OnionDuke malware family. Evidence suggests that the authors of CozyDuke and OnionDuke are either the same or they work together. Similarities have also been identified between CozyDuke and MiniDuke, and the command and control (C&C) server communication methods used by CozyDuke are similar to the ones seen at CosmicDuke.

“[CozyDuke’s] custom backdoor components appear to slightly evolve over time, with modifications to anti-detection, cryptography, and trojan functionality changing per operation. This rapid development and deployment reminds us of the APT28/Sofacy toolset, especially the coreshell and chopstick components,” Kaspersky researchers noted.

While Kaspersky hasn’t mentioned anything about the CozyDuke threat group’s affiliations, the media reports on the State Department and White House attacks named Russia as the main suspect. Furthermore, MiniDuke and OnionDuke are believed to have Russian roots.

Kaspersky Lab isn’t the first company to publish a report on the activities of the CozyDuke APT group. Back in March, a couple of Poland-based security firms published some technical details on the threat actor’s activities after it was seen targeting Polish government institutions.

| ID | Name | Description |
|---|---|---|
| T1566.002 | Spearphishing Link | In some of its attacks, CozyDuke used spear-phishing emails containing links to compromised websites hosting malware. |
| T1566.001 | Spearphishing Attachment | In some of its attacks, CozyDuke used spear-phishing emails containing links to compromised websites hosting malware. In other operations, the attackers relied on malicious Flash videos attached directly to emails in order to deliver malware. |
| T1204.001 | Malicious Link | In some of its attacks, CozyDuke used spear-phishing emails containing links to compromised websites hosting malware. |
| T1204.002 | Malicious File | In some of its attacks, CozyDuke used spear-phishing emails containing links to compromised websites hosting malware. In other operations, the attackers relied on malicious Flash videos attached directly to emails in order to deliver malware. |
| T1518.001 | Software Discovery: Security Software Discovery | Once it infects a system, the malware checks for the presence of security products from Kaspersky, Crystal Security, Sophos, Dr. Web, Avira, and Comodo. |
| T1036.001 | Masquerading: Invalid Code Signature | Researchers have noted that many of the malware components used in CozyDuke attacks are signed with fake Intel and AMD digital certificates. |