MiniDuke relation ‘CozyDuke’ Targets White House

Posted on April 27, 2015 by Staff Writer Leave a comment

Kaspersky Lab’s Global Research and Analysis Team has published a report describing a new, advanced cyberespionage campaign using malware to hit very specific, high-profile entities. Targets in the U.S. are believed to include the White House and the State Department, while the attacker’s list also includes government organisations and commercial entities in Germany, South Korea and Uzbekistan.

Alongside its very precise targeting of the highest profile victims, the threat actor exhibits other worrying, although fascinating features. These include the use of crypto and anti-detection capabilities. For example, the code hunts for the presence of several security products in order to attempt to evade them, namely: Kaspersky Lab, Sophos, DrWeb, Avira, Crystal and Comodo Dragon.

Connection to other cyberespionage actors

Kaspersky Lab’s security experts uncovered strong malicious program functionality, as well as structural similarities that matched this toolset with the MiniDuke, CosmicDuke and OnionDuke cyberespionage campaigns; operations that, according to a number of indicators, are believed to be managed by Russian-speaking authors. Kaspersky Lab observations show that MiniDuke and CosmicDuke are still active and targeting diplomatic organisations/embassies, energy, oil and gas companies, telecoms, military, and academia/research institutions in a number of countries.

Method of distribution

The CozyDuke actor often spearphishes targets with emails containing a link to a hacked website – sometimes to high profile, legitimate ones such as ‘diplomacy.pl’ – which hosts a ZIP archive rigged with malware. In other highly successful runs, this actor sends out phony flash videos with malicious executables included as email attachments.

CozyDuke use a backdoor and a dropper. The malicious program sends information about the target to the command and control server, and retrieves configuration files and additional modules implementing any extra functionality needed by the attackers.

“We have been monitoring both MiniDuke and CosmicDuke for couple of years. Kaspersky Lab was the first to warn about MiniDuke attacks in 2013, with the “oldest” known samples for this cyberthreat dating back to 2008. CozyDuke is definitely connected to these two campaigns, as well as to the OnionDuke cyberespionage operation. Every one of these threat actors continues to track their targets, and we believe their espionage tools are all created and managed by Russian-speakers,” commented Kurt Baumgartner, Principal Security Researcher at Kaspersky Lab’s Global Research and Analysis Team.

Kaspersky Lab’s products detect all the known samples and protect users against this threat.

Tips for users

- Don’t open attachments and links from people you don’t know
- Regularly scan your PC with an advanced antimalware solution
- Beware of ZIP archives with SFX files inside
- If you are unsure about the attachment, try to open it in a sandbox
- Make sure you have a modern operating system with all patches installed
- Update all third party applications such as Microsoft Office, Java, Adobe Flash Player and Adobe Reader

tagged with Avira, CosmicDuke, CozyDuke, cyberespionage, Cyberthreat, DrWeb, Featured, Kaspersky Lab, malware, MiniDuke, OnionDuke, Sophos, White House

- Malware
- Threats