Emissary Panda targets Middle East governments with webshells on Sharepoint servers

Search

Search

Newsletter

Since August 28th 2018 all our Newsletters are active. Subscribe! Every Saturday you will receive a weekly report of everything we have published.

Recent Posts

- Cyber Security, WordPress adds auto-update for themes and plugins
18 March 2020
- Syria, Russia-Turkey patrols in Idlib blocked by population and militias
18 March 2020
- Coronavirus, boom of Fake News via instant messenger
17 March 2020
- Syria: Kurds prepare for Coronavirus, which mainly damages Isis
17 March 2020
- Cyber Security, Microsoft patches the Windows 10 “SMBGhost”
16 March 2020

Emissary Panda targets Middle East governments with webshells on Sharepoint servers

3 June 2019   Francesco Bussoletti   Cyber, Defence and Security

Palo Alto’s Unit 42: Emissary Panda Chinese APT attacked Middle East governments with webshells on sharepoint servers to upload a variety of tools

Emissary Panda Chinese APT is attacking Middle East government sharepoint servers. It has been discovered by Palo Alto’s Unit 42 cyber security experts. According to the researchers, the threat group (AKA APT27, TG-3390, Bronze Union, Lucky Mouse) is installing webshells on Sharepoint servers to compromise Government Organizations of two different countries in the region. It exploits a recently patched vulnerability in Microsoft SharePoint, which is a remote code execution vulnerability used to compromise the server and eventually install a webshell. The actors uploaded a variety of tools that they used to perform additional activities on the compromised network, such as dumping credentials, as well as locating and pivoting to additional systems on the network. Of particular note is their use of tools to identify systems vulnerable to CVE-2017-0144, the same vulnerability exploited by EternalBlue that is best known for its use in the WannaCry attacks of 2017.

The cyber security experts: The threat actor upload 24 unique executables, from Mimikatz to HyperBro, commonly associated to Emissary Panda

Emissary Panda is active since 2010, targeting organizations worldwide, financial services firms, and national data centers. The group is involved in cyber espionage aimed at new generation weapons and in surveillance activities on dissidents and other civilian groups. According to Palo Alto, the webshell activity agains Middle East governments took place across three SharePoint servers hosted by two different organizations between April 1 and 16, 2019, where actors uploaded a total of 24 unique executables. They range from legitimate applications such as cURL to post-exploitation tools such as Mimikatz. Emissary Panda also uploaded tools to scan for and exploit potential vulnerabilities in the network, such as the well-known SMB vulnerability patched in MS17-010 commonly exploited by EternalBlue to move laterally to other systems on the network. Cyber security expers also observed the chinese actors uploading custom backdoors such as HyperBro, commonly associated with the APT.

Facebook   Twitter   LinkedIn   WhatsApp   Telegram   Facebook Messenger

APT   APT27   Bronze Union   cyber espionage   cyber security   cyber warfare   cybercrime   Emissary Panda   HyperBro   infosec   Lucky Mouse   Middle East   Mimikatz   Palo Alto   Sharepoint Server   state sponsored hackers   TG-3390   Unit 42   webshells

Related Posts

Syria, an entire village in Deir Ezzor reacts to the presence of Isis in the area
The inhabitants of al-Nimiliyah attacked al-Naitel, which housed

Cyber Espionage, Twitter confirms attacks to match usernames to phone numbers
The social media platform: State-sponsored actors used a large

Mandiant, How US Government Agencies are Facing Cyber Security Challenges
They use 4 strategies: Proactive cyber threat hunting, Increased use

« Syria, Isis returns to its origins and target population: double attack in Raqqa

Isis is hunted in Iraq and Syria with its own tactics »