Emissary Panda APT group hit Government Organizations in the Middle East

May 30, 2019 By Pierluigi Paganini

Chinese Cyber-Spies Target Government Organizations in Middle East

Chinese APT group Emissary Panda has been targeting government organizations in two different countries in the Middle East.

Experts at Palo Alto Networks reported that the Chinese APT group Emissary Panda (aka APT27, TG-3390, Bronze Union, and Lucky Mouse) has been targeting government organizations in two different countries in the Middle East.

The Emissary Panda APT group has been active since 2010, targeted organizations worldwide, including U.S. defense contractors, financial services firms, and a national data center in Central Asia.

The group was involved in cyber espionage campaigns aimed at new generation weapons and in surveillance activities on dissidents and other civilian groups.

The cyber espionage group leverage both readily available tools and custom malware in their operations, many tools are available for years, but in recent attacks, their code was updated.

In April 2019, the group targeted organizations of two different countries in the Middle East. Hackers hit webservers to install of webshells on SharePoint servers, threat actors leveraged the CVE-2019-0604 vulnerability to compromise SharePoint servers.

Once compromised the network, attackers will upload a variety of tools to perform additional activities, including dumping credentials, and locating and pivoting to additional systems on the network.

Experts pointed out that attackers used tools to scan the network for systems vulnerable to CVE-2017-0144, the flaw exploited by the NSA-linked EternalBlue exploit.

The campaign appears related to attacks exploiting CVE-2019-0604 reported by the Saudi Arabian National Cyber Security Center and the Canadian Center for Cyber Security. The report by the Saudi Cyber Security Centre suggests threat actors are primarily targeting organizations within the kingdom. The Canadian Cyber Security Centre reported similar attacks aimed at delivering the China Chopper web-shell to ensure persistence in the target networks.

"the actors used these webshells to upload legitimate executables that they would use DLL sideloading to run a malicious DLL that has code overlaps with known Emissary Panda attacks. We also found the China Chopper webshell on the SharePoint servers, which has also been used by the Emissary Panda threat group." states the report published by PaloAlto Networks.a

PaloAlto experts observed between April 1 and April 16, the threat actors-using webshells to upload 24 unique executables on three SharePoint servers hosted by two different government organizations. Experts noticed that the same tools were uploaded across the three webshells, suggesting the involvement of the same attacker.

The longest activity involving one of the three webshells was observed on April 16, 2019.

The list of the tools uploaded by cyberspies included legitimate applications such as cURL, post-exploitation tools like Mimikatz, tools to scan for and exploit potential vulnerabilities in the target network, and custom backdoors such as HyperBro, which was used by Emissary Panda in the past.

One of the webshells used by the attackers is a variant of the Antak webshell, other webshells appear related to the China Chopper webshell.

"We were able to gather one of the webshells with which we saw the actor interacting, specifically the error2.aspx file listed above. The error2.aspx file (SHA256: 006569f0a7e501e58fe15a4323eedc08f9865239131b28dc5f95f750b4767b38) is a variant of the Antak webshell, which is part of a tool created for red teaming called Nishang. " continues the report.

Cyber spies also uncovered the use of additional sideloaded DLLs in this campaign.

"The Emissary Panda threat group loaded the China Chopper webshell onto SharePoint servers at two Government organizations in the Middle East, which we believe with high confidence involved exploiting a remote code execution vulnerability in SharePoint tracked in CVE-2019-0604," Palo Alto Networks concludes.

"Once the adversary established a foothold on the targeted network, they used China Chopper and other webshells to upload additional tools to the SharePoint server to dump credentials, perform network reconnaissance and pivot to other systems. "

If you appreciate my effort in spreading cybersecurity awareness, please vote for Security Affairs in the section "Your Vote for the Best EU Security Tweeter"

Thank you

Pierluigi Paganini

(SecurityAffairs – cyberespionage, Emissary Panda)

Share this...

APT | Cyberespionage | Emissary Panda | Hacking | information security news | malware | Pierluigi Paganini | Security Affairs | Security News | SharePoint

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Nansh0u campaign already infected 50,000 MS-SQL and PHPMyAdmin Servers

NEXT ARTICLE
VPNpro research: this Chinese-linked company secretly owns 10 VPNs with 86 million installs

YOU MIGHT ALSO LIKE

Thousands of Coronavirus-related malicious domains are being created every day
March 18, 2020 By Pierluigi Paganini

VMware fixes high severity privilege escalation and DoS in its products
March 18, 2020 By Pierluigi Paganini