SC MAGAZINE FOR IT SECURITY PROFESSIONALS

- SC US
- SC UK

Hundreds of porn sites affected in malvertising campaign

OPM launches site for victims to check if personal information stolen

Hackers use Dropbox to target Hong Kong media

November 2015 Issue

Editorial

Pushing past shock and yawn

Threat of the month

Threat of the Month, November 2015

Subscribe

Archive

Robert Abel, Content Coordinator
Follow @RobertJAAbel

December 04, 2015

APT28 stronger, faster in recent months

Share this article:

- facebook
- twitter
- linkedin
- google
- Comments Comments
- Email
- Print

7

Like

Share

Advanced persistent threat group (APT) APT28 has increased its Tweet enfold by going after high profile targets with an updated set of tools, according to researchers at Kaspersky Lab.

APT28 has been has shown increased activity in recent months with more high profile targets and more sophisticated methods.

The security firm's Global Research & Analysis Team said the group also known as Sofacy, Fancy Bear, Sednit, and STRONTIUM has began a new wave of attacks using new tools and leading to an increase in defense-related targets and an increase in activity in Uk according to a Dec. 4 blog post.

0

G+1

"The attackers deploy modification of the AZZY backdoor, which is used for the initial reconnaissance. Once a foothold is established, they try to upload more backdoors, USB stealers as well as other hacking tools such as "Mimikatz" for lateral movement," researchers said in the blog.

Researchers spotted the first versions of the AZZY implant in August and said the group is attacking more frequently than before while using more sophisticated methods including multi-backdoor packages for extreme resilience to attack better defended targets.

"In the months leading up to August, the Sofacy group launched several waves of attacks relying on zero-day exploits in Microsoft Office, Oracle Sun Java, Adobe Flash Player and Windows itself," researchers said in the post.

The most recent waves of attacks also included a new generation of USB stealers that appear to be geared exclusively toward high-profile targets, the report said.

Kurt Baumgartner, principal security researcher at Kaspersky Lab, told SCMagzine.com that the group's activities are classic cyber espionage and that its use of new tools show that the group is developing stronger methods to overcome better defended targets including those that use air gaps.

He said that the group is very technically capable and that they will develop what they need to attack the targets.

"This quick work is a new characteristic of their work, and this stepped up urgency is something that is unusual. In general, APT intrusions can last months or longer, and in these cases, we see Sofacy acting with unusually ramped urgency," Baumgartner said.

Next Article in News

rs said in the post the best defense against targeted attacks is a multi-layered that combines traditional anti-malware technologies with patch management, host etection and, ideally, whitelisting and default-deny strategies.

Share this article:

New Hampshire company hacks smaller competitor for customer list

- facebook
- twitter

- linkedin
- google
- Comments
- Email
- Print

You must be a registered member of SC Magazine to post a comment.
Click here to login | Click here to register

Sponsored Links