
***Issued 10/19/17***

## A Complex Mac Virus That May Signal the Shape of Tomorrow's Malware

Macs are the go-to device for professionals and high-level officials the world over. Beautifully designed, extremely optimized for performance, and tagged with a price that reflects a premium product, Macs are more than a tool – they are a statement. In keeping with this reputation, you would not expect malware designed for Macs to be the run-of-the-mill, easy-to-block creations we see on other platforms. Advanced Mac threats cost a fortune to develop— but when they hit the designated target, it's jackpot for the cyber-criminals

One of these pieces of advanced malware was discovered earlier this year and was linked to a group of attackers known as Sofacy Group or Fancy Bear, a Russian threat actor that became widely known after the cyberattacks on the German parliament, French television station TV5Monde, and the White House.

Besides select victim targeting, the APT28 virus can selectively download components for each victim, including those running Mac OS. The XAgent modular backdoor delivered via the

Komplex downloader can install various espionage modules, ranging from key-logging to screen grabbing and file exfiltration.