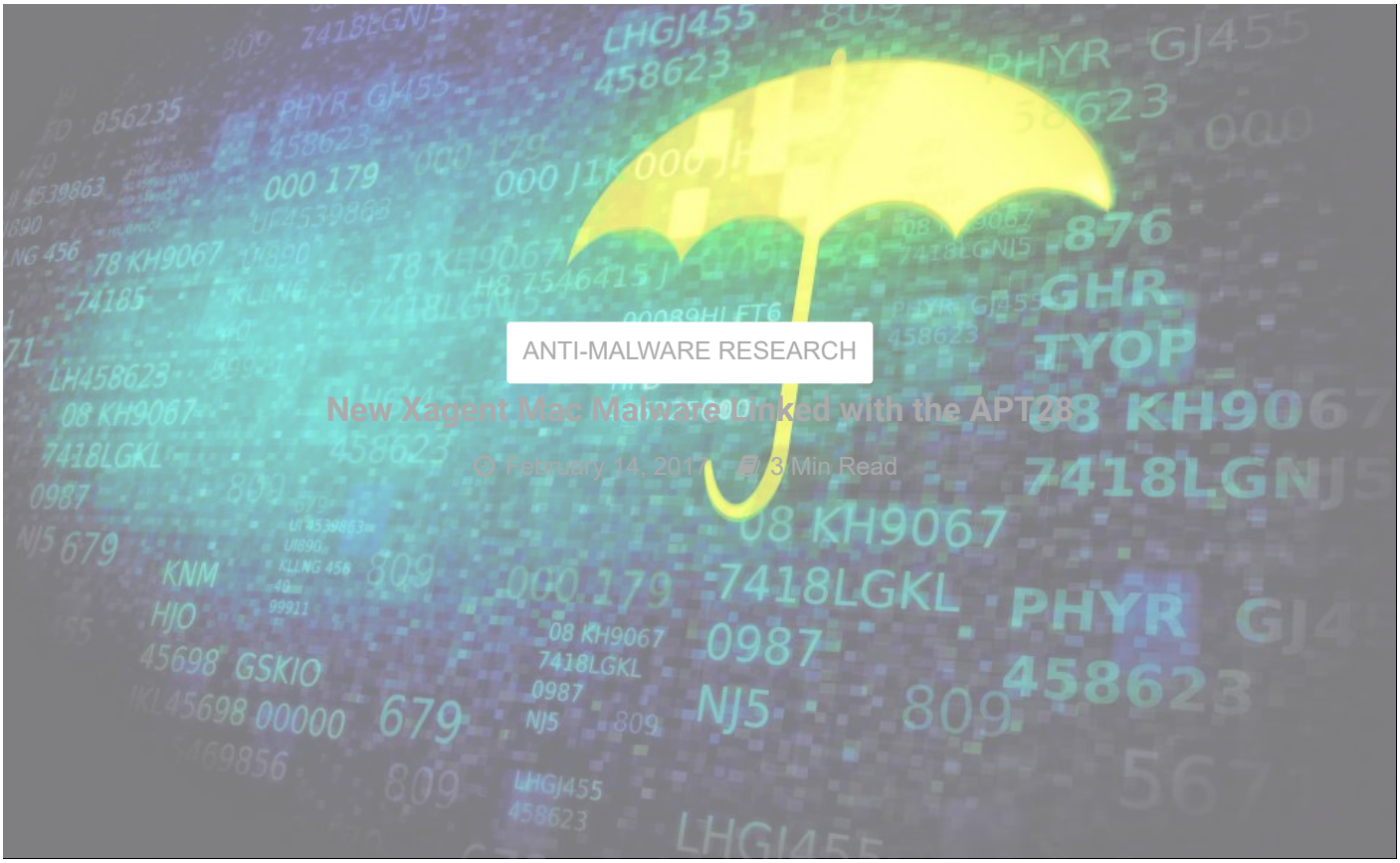

APT28 operators have upped their game – the Xagent payload now can target victims running Mac OS X to steal passwords, grab screens and steal iPhone backups stored on the Mac.

Last year we fully documented what appears to be one of the largest cyber-espionage campaigns ever, allegedly linked to the Russian territory.

The sample we are discussing today has been linked to the Mac OSX version of Xagent component from Sofacy/APT28/Sednit APT. This modular backdoor with advanced cyber-espionage capabilities is most likely planted on the system via the Komplex downloader.

Once successfully installed, the backdoor checks if a debugger is attached to the process. If it detects one, it terminates itself to prevent execution. Otherwise, it waits for an Internet connection before initiating communication with the C&C servers. After the communication has been established, the payload starts the modules.

Our preliminary analysis shows most of the C&C URLs impersonate Apple domains.

Once connected to the C&C, the payload sends a HelloMessage, then spawns two communication threads

The analysis reveals the presence of modules that can probe the system for hardware and software configurations, grab a list of running processes and run additional files, as well as get desktop screenshots and harvest browser passwords.

But the most important module, from an intelligence-gathering perspective, is the one that allows the operator(s) to exfiltrate iPhone backups stored on a compromised Mac.

All these modules are pending analysis – a detailed paper documenting all the functionalities of the modules will be made available shortly.

Our past analysis of samples known to be linked to APT28 group shows a number of similarities between the Sofacy/APT28/Sednit Xagent component for Windows/Linux and the Mac OS binary that currently forms the object of our investigation. For once, there is the presence of similar modules, such as FileSystem, KeyLogger and RemoteShell, as well as a similar network module called HttpChanel.

Other indicators show that today's sample also reports to a C&C URL that is identical to the Sofacy/APT28/Sednit Komplex OSX Trojan, minus the TLD (apple-[*******].net for Komplex vs apple-[*******].org for Xagent).

Forensic evidence recovered from the binary also reveals identical binary strings in both Komplex and Xagent clients, as follows:

Komplex binary string: "/Users/kazak/Desktop/Project/komplex"
Xagent Mac binary string: "/Users/kazak/Desktop/Project/XAgentOSX"

We conclude this brief teaser with the assertion that the Komplex component discovered in September has been exclusively used as a downloader and installer for the Xagent binary.

The investigation is ongoing so there is much we can't say yet. Make sure to check back here for an in-depth analysis.

Many thanks to Tiberius Axinte, Technical Lead, Antimalware Lab, for documenting the sample.

Tags APT APT28 Backdoor cyber-warfare iPhone Mac backdoor Mac OS X Sednit Sofacy trojan Xagent

About the author