Serianu Cyber Security Advisory

FinFisher Spyware

Serianu SOC Advisory Number:

TA – 2020/019

Date(s) issued:

9th November 2020

Systems Affected:

- Desktop and Mobile Operating Systems

Overview:

Serianu threat intelligence team discovered a spyware FinFisher also known as FinSpy. FinSpy is a full-fledged surveillance software suite capable of intercepting communications, accessing private data and recording audio and video from a computer or mobile device it is silently installed on.

According to our research, FinSpy has been proven successful in operations around the world and valuable intelligence have been gathered about Target Individuals and Organizations. When FinSpy is installed on a computer system, it can be remotely controlled and accessed as soon as it is connected to the internet or network. FinSpy is extremely powerful spying software that is being sold as a legal law enforcement tool to governments around the world but has also been found in use by oppressive and suspicious activities to spy on users.

This advisory provides an in-depth research on the FinFisher Spyware, how it can be exploited and recommendations.

FinFisher

FinFisher can target both desktop and mobile operating systems including Android, iOS, Windows, macOS and Linux.
FinSpy can do the following:

- Break WPA encryption and gain access to wireless networks.
- Monitor activity on social network accounts and webmail.
- FinFisher allows remote monitoring of activity on the victim's computer.
- Discover hidden networks and gain access to Bluetooth devices.
- Steal passwords and online account information
- Turning on webcams and microphones
- Recording everything the victim types on the keyboard
- Intercepting calls.

Methods of infection

FinFisher malware is installed in various ways, including:

- Fake software updates.
- Emails with fake attachments.
- Security flaws in popular software.

The malware is capable of collecting personal information such as:

- Contacts, SMS/MMS messages, Phone call recordings and data from the most popular messengers
- Emails and Calendars
- GPS location and Photos
- Files in memory

Conclusion

FinFisher's FinSpy malware is a commercially produced and distributed product aimed at infecting systems for the purposes of spying, stealing data and remotely controlling the target machine. ESET's Free Online Scanner can be used to scan and check for the malware's presence and remove it if detected.

Information Sharing

We encourage any organisation or individual that has access to malware related attacks share it with us through our email: info@serianu.com. To allow us analyze indicators of compromise (IOCs).