Keranger: the first “in-the-wild” ransomware for Macs. But certainly not the last.

macworld.com/article/3234650/macs/keranger-the-first-in-the-wild-ransomware-for-macs-but-certainly-not-the-last.html

By Liviu Arsene,

Ransomware has been one of the most lucrative threats for cybercriminals. With the FBI estimating financial losses were up $1 billion dollars in 2017 alone, by the end of 2018 it’s reasonable to speculate that those numbers will be significantly higher.

Although most ransomware targets systems running Windows, Mac ransomware became a reality when Brazilian researchers posted a proof-of-concept (dubbed Mabouia) in early 2015. Whether by coincidence or design, the first truly damaging ransomware sample for Macs emerged about a month later, delivered using a tampered version of a popular file-sharing application known as Transmission.

The Keranger Mac Ransomware

Dubbed Keranger, the Mac ransomware had the same ability as its Windows counterpart, meaning once loaded it could encrypt locally stored files, documents, and even Time Machine backups while demanding a bitcoin payment for the decryption key.

Although Macs have a built-in system that prevents installation of unauthorized or un-signed applications from third-party marketplaces, the Keranger ransomware was bundled inside Transmission – a torrent application – after attackers managed to breach the official Transmission website and replace the legitimate .dmg file with a tampered version.

Interestingly, to dodge GateKeeper's app validation mechanism, attackers signed the tampered Transmission app with a valid Apple developer certificate, making it seem legitimate. Unsuspecting users who visited the official website and installed the application while it was live became the first-ever Mac ransomware victims.

More Evidence of Mac Ransomware

While Keranger was the first "in-the-wild" and documented ransomware outbreak for Macs, it was not the last, by far. Security researchers have identified a ransomware-as-a-service that enabled interested "customers" to purchase Mac-hostile ransomware in exchange for up-front payments or shared revenue from infected victims.

While ransomware-as-a-service is not uncommon for Windows-based systems, its emergence for Macs suggests an increased interest from "customers" to start buying ransomware kits that can be deployed on Mac OS.

A great example that further bolsters the case of Mac ransomware-as-a-service: the Keranger's source code is publicly available to anyone interested in writing their own variant of Mac ransomware—and its developer only asks for 30% of what the "customer" gets from paying victims.

Staying away from both ransomware and any other type of Mac threat is a simple matter of installing a Mac security solution that can accurately identify potentially malicious applications or threats. This type of security solution also keeps Mac users safe from phishing, fraudulent, or malware-serving websites that might trick users into installing or revealing sensitive data.

Note: When you purchase something after clicking links in our articles, we may earn a small commission. Read our affiliate link policy for more details.

Related:

- Mac
- Viruses
- Malware