SIXGILL

SIXGILL Threat Report

PROTON - A New MAC OS RAT

07/02/17

SIXGILL THREAT REPORT: **PROTON - A New MAC OS RAT**

BACKGROUND

Sixgill researchers have encountered a post in one of the leading, closed Russian cybercrime message boards. The author of the thread announced a RAT dubbed Proton, intended for installation exclusively on MAC OS devices. The author offered this product in one of the leading underground cybercrime markets. This report contains information about the malware.

CAPABILITIES

The author claims to have written the malware in native Objective C, the advantage being that the malware does not require any dependencies. The author also claims the app is fully-undetected by any existing MAC OS anti-viruses currently in the market. He then continues to mention a comprehensive list of capabilities:

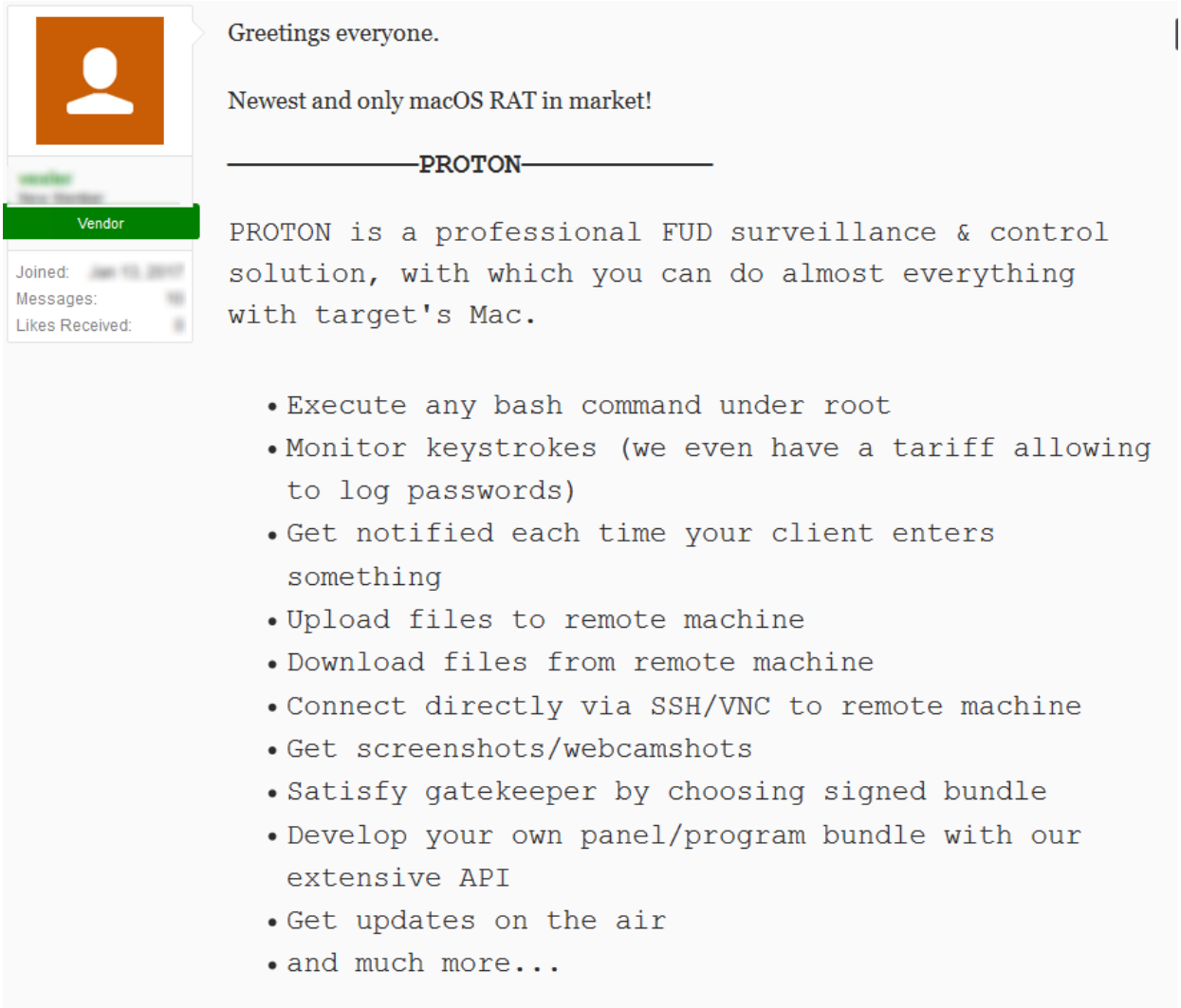

Figure 1: Proton's ad as published in a major cybercrime marketplace.

SIXGILL THREAT REPORT: **PROTON - A New MAC OS RAT**

The malware includes root-access privileges and features allowing an attacker to obtain full control of the victim's computer. Its capabilities include: running real-time console commands and file-manager, keylogging, SSH/VNC connectivity, screenshots, webcam operation and the ability to present a custom native window requesting information such as a credit-card, driver's license and more. The malware also boasts the capability of iCloud access, even when two-factor authentication is enabled.

The real threat behind the software is this: The malware is shipped with genuine Apple code-signing signatures. This means the author of Proton RAT somehow got through the rigorous filtration process Apple places on MAC OS developers of third-party software, and obtained genuine certifications for his program. Sixgill evaluates that the malware developer has managed to falsify registration to the Apple Developer ID Program or used stolen developer credentials for the purpose. Sixgill also believes that gaining root privileges on MAC OS is only possible by employing a previously unpatched 0-day vulnerability, which is suspected to be in possession of the author. Proton's users then perform the necessary action of masquerading the malicious app as a genuine one, including a custom icon and name. The victim is then tricked into downloading and installing Proton.

The purchase process occurs on a dedicated website. The website includes some promotional material related to the malware, a login system and the possibility to pay for the product.

Figure 2: The official website for Proton

SIXGILL THREAT REPORT: **PROTON - A New MAC OS RAT**

Ever the cynics, fraudsters keep finding new ways of advertising their malware under the premise of legitimate cover stories. Proton's website is no different:

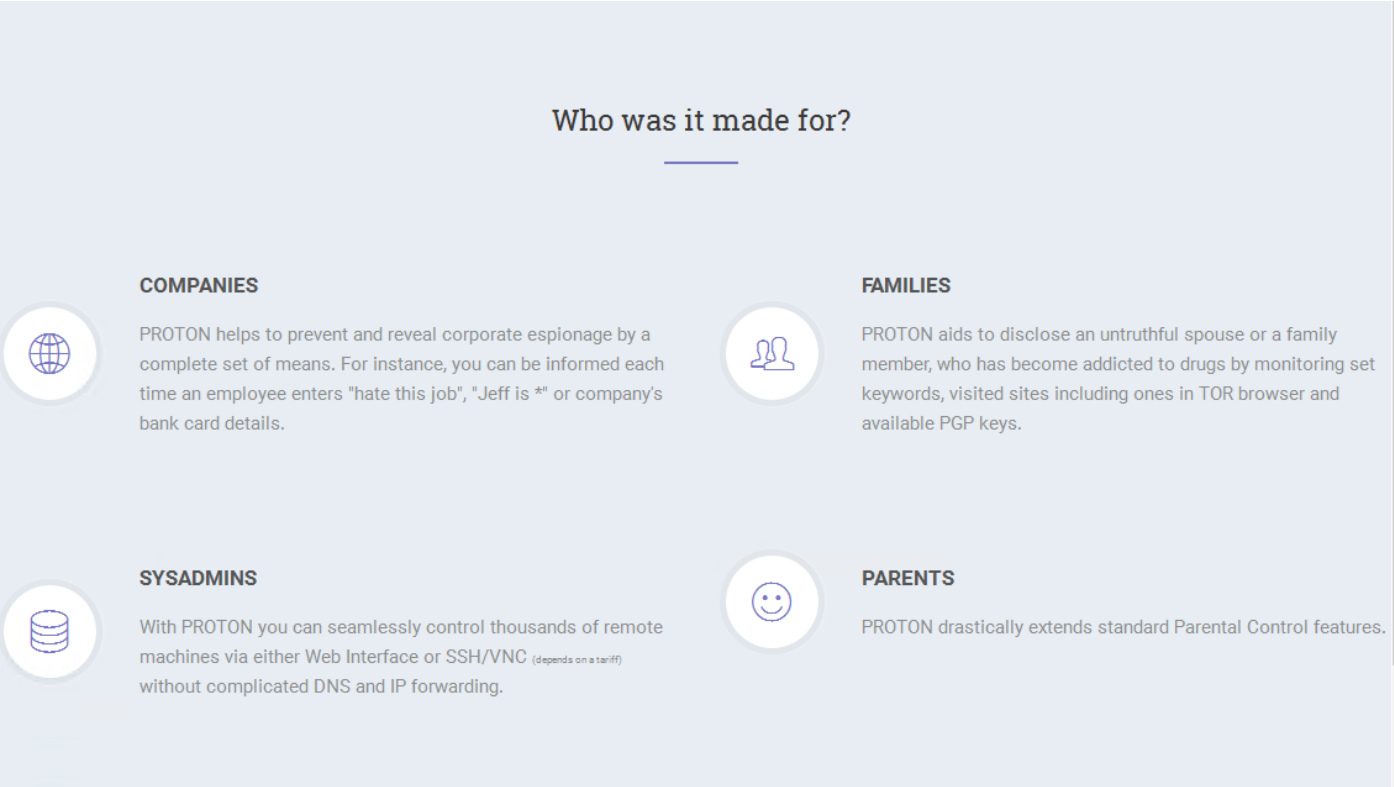

Figure 3: Product description, found in Proton's official website

A short video demonstrating the installation process for Proton was uploaded to YouTube.

SIXGILL THREAT REPORT: **PROTON - A New MAC OS RAT**

PRICING

At first, the asking price for the product was extremely steep (~100BTC, equivalent to roughly $100,000), but after meeting critique from his peers, the prices were significantly lowered. A version with unlimited installations costs ~40BTC, while a license to install on a single PC with genuine apple certifications would set a cybercriminal back only 2BTC.

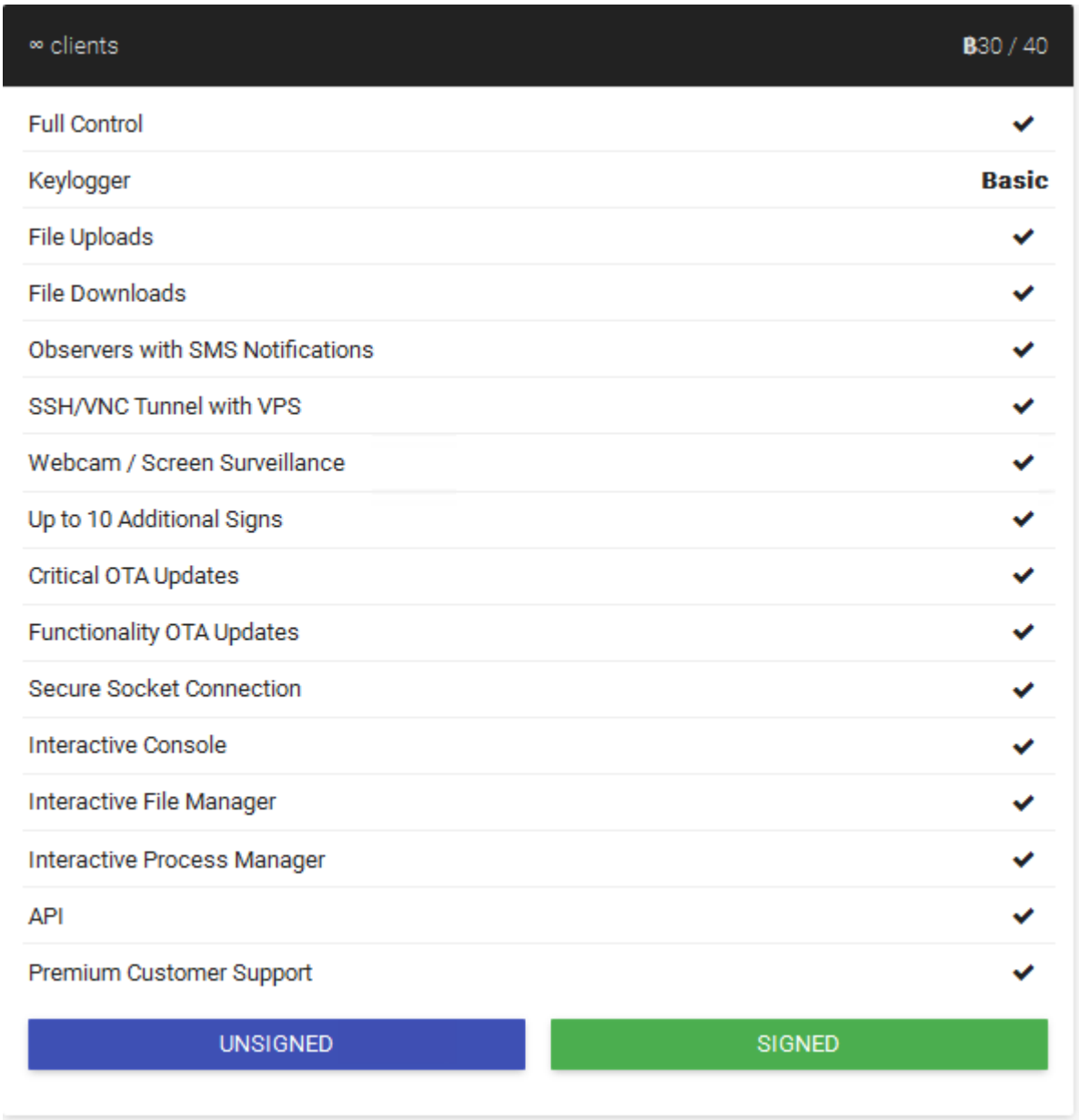

Figure 4: Proton pricing plan and features covering an infinite amount of bots, taken from Proton's official website.