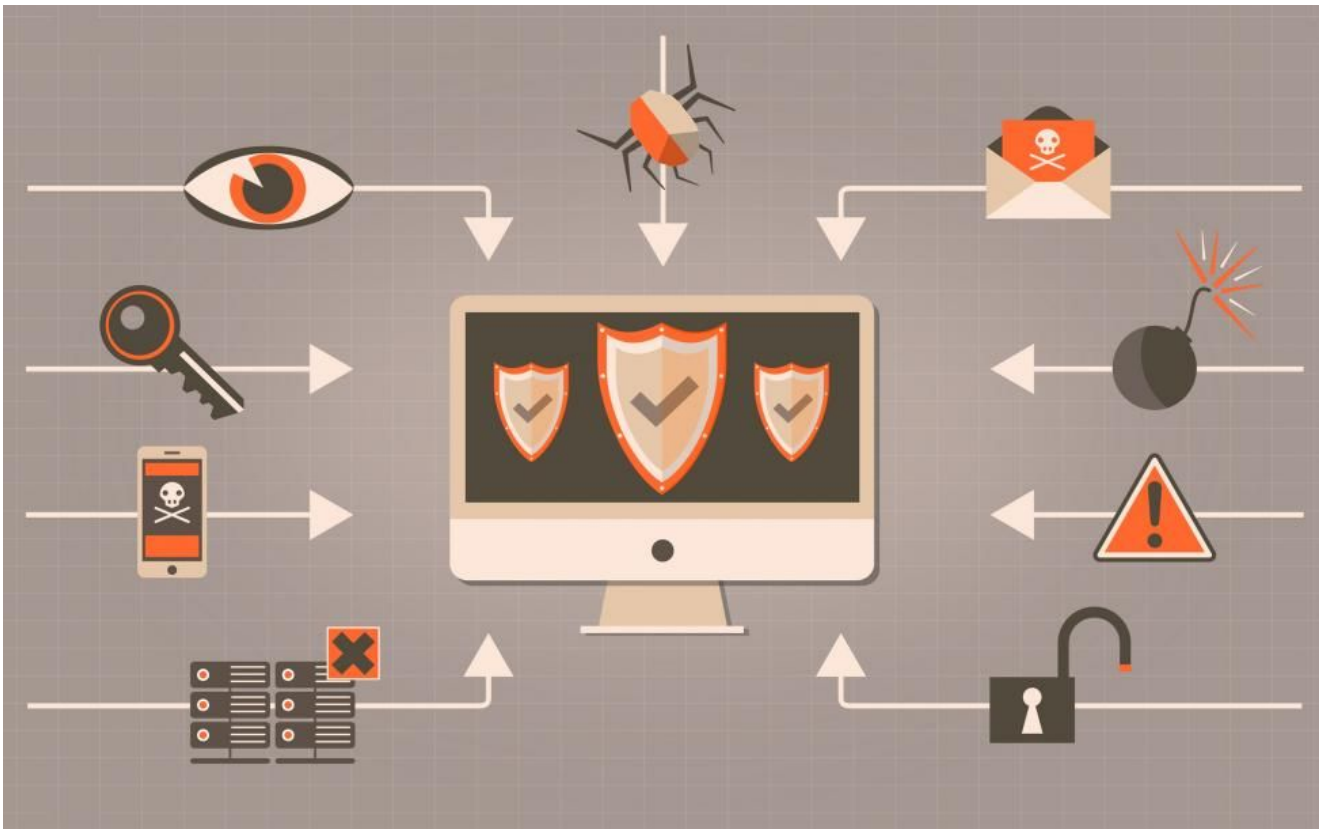
New Backdoor Allows Full Access to Mac Systems, Bitdefender Warns

labs.bitdefender.com/2016/07/new-mac-backdoor-nukes-os-x-systems/

Anti-Malware Research
2 min read

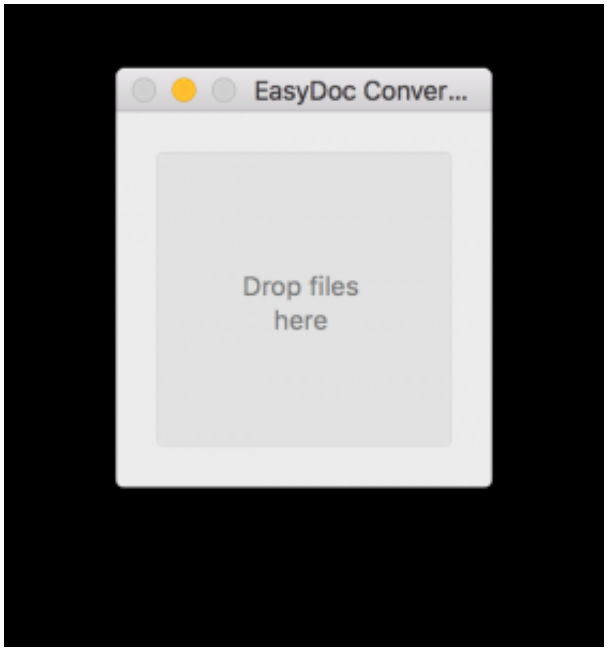
Alexandra GHEORGHE
July 05, 2016



A new piece of malware, dubbed **Backdoor.MAC.Eleanor** by Bitdefender researchers, exposes Apple systems to cyber-espionage and full, clandestine control from malicious third-parties.

[Read the full report here].

The backdoor is embedded into a fake file converter application that is accessible online on reputable sites offering Mac applications and software. The EasyDoc Converter.app poses as a drag-and-drop file converter, but has no real functionality – it simply downloads a malicious script.



The script installs and registers the following components to system startup:

Tor Hidden Service

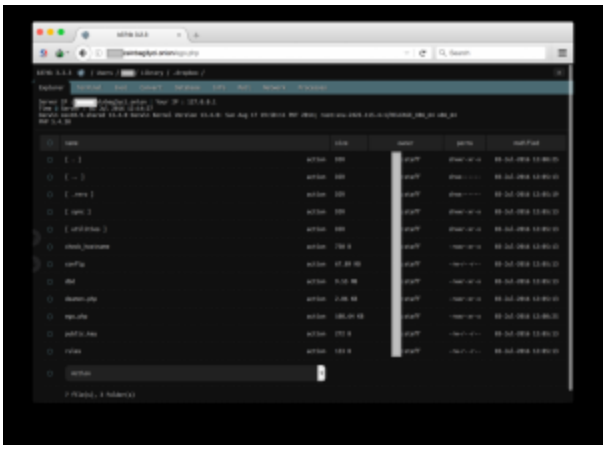
This component creates a Tor hidden service that allows an attacker to anonymously access the control-and-command center from the outside – a local web server dubbed Web Service (PHP) – via a Tor-generated address.

Web Service (PHP)

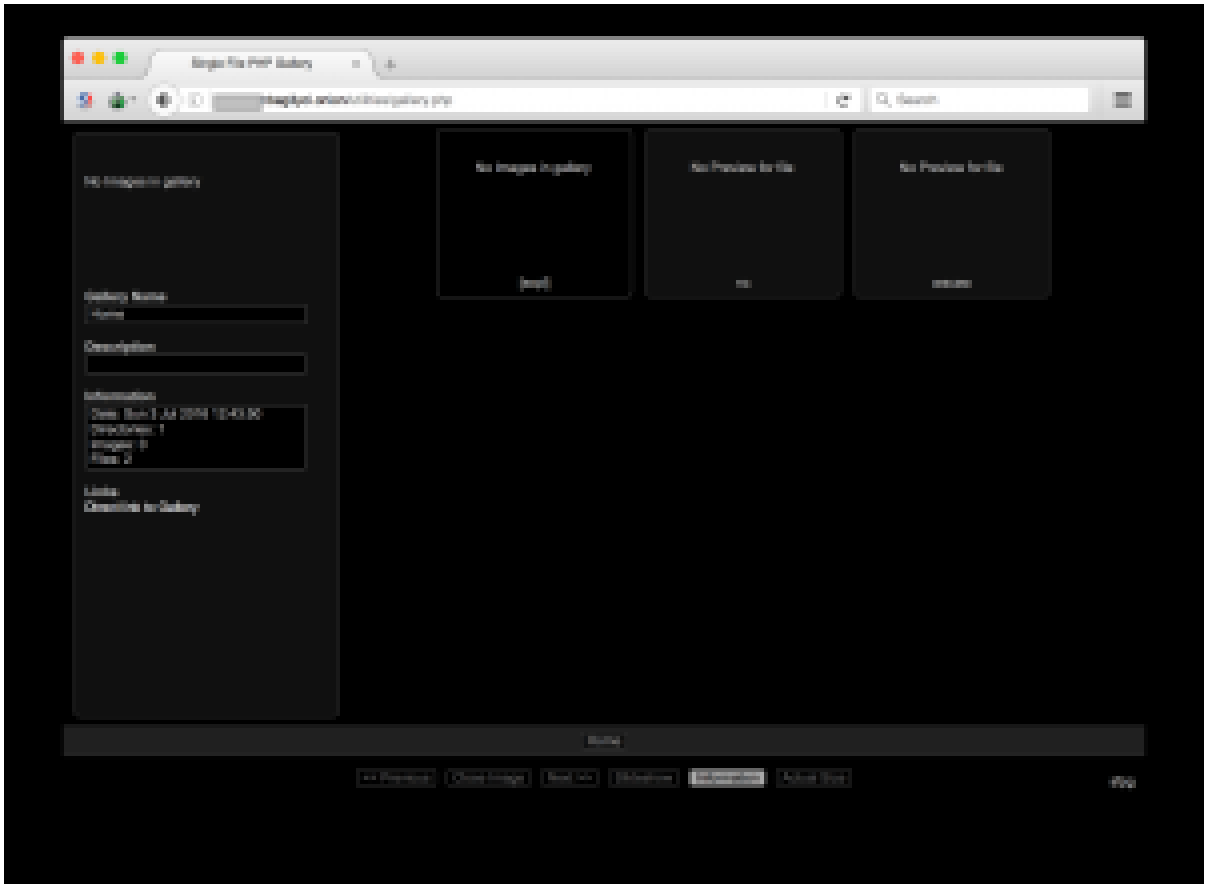
This component acts as the C&C center and gives the attacker full control over the infected machine. The web service is set up locally and can be accessed through the “onion” address. After authenticating with the correct password, attackers gain access to a web-based control panel with the following abilities:

• File manager (view, edit, rename, delete, upload, download, and archive files)
• Command execution (execute commands)
• Script execution (execute scripts in PHP, PERL, Python, Ruby, Java, C)
• Shell via bind/reverse shell connect (remotely execute root commands)
• Simple packet crafter (probe firewall rule-sets and find entry points into a targeted system or network)
• Connect and administer databases
• Process list/Task manager (access the list of processes and applications running on the system)
• Send emails with attached files

Attacker control panel



The malware uses a tool named “wacaw” to capture images and videos from built-in webcams.



Gallery Panel

It also uses a daemon to grab updates and fetch files from the user’s computer or execute shell scripts.

Pastebin Agent

Every infected machine has a unique Tor address that the attacker uses to connect and download the malware. All the addresses are stored on pastebin.com using this agent, after being encrypted with a public key using RSA and base64 algorithms.

Consequences

“This type of malware is particularly dangerous as it’s hard to detect and offers the attacker full control of the compromised system,” says Tiberius Axinte, Technical Leader, Bitdefender Antimalware Lab. “For instance, someone can lock you out of your laptop, threaten to blackmail you to restore your private files or transform your laptop into a botnet to attack other devices. The possibilities are endless.”

This app is not digitally signed by Apple. As a good safety precaution, Bitdefender recommends downloading applications exclusively from reputable websites, and using a security solution for Apple devices to fend off Mac-targeting malware and other specific threats.

[Read the full report here]

Technical analysis was provided by Tiberius Axinte, Technical Leader at Bitdefender Antimalware Lab and Dragos Gavrilut, Antimalware Research Manager.

TAGS

anti-malware research

AUTHOR

Alexandra GHEORGHE

Alexandra started writing about IT at the dawn of the decade - when an iPad was an eye-injury patch, we were minus Google+ and we all had Jobs.

View all posts