Malicious ad campaigns abuse Chrome to steal 500 million iOS user sessions

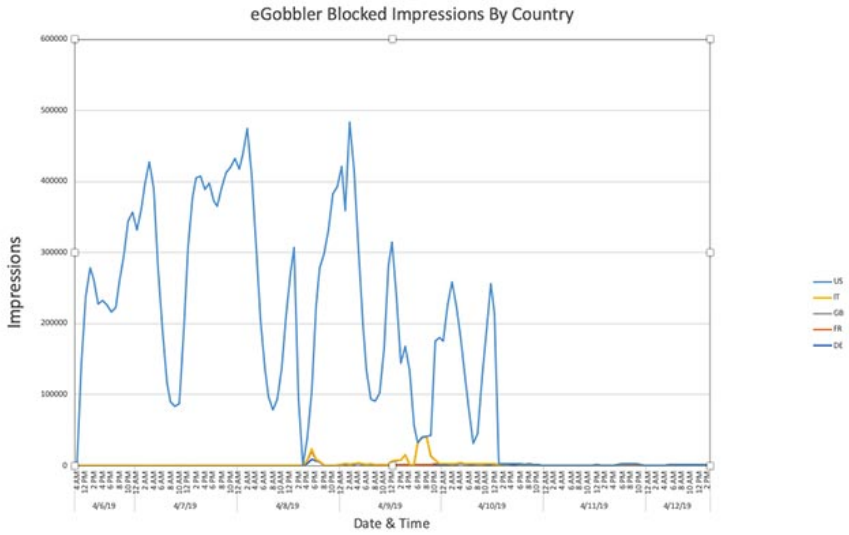
In recent times, many large malvertising attacks targeted iOS users from the United States and many European Union countries have been deployed.

In recent times, many large malvertising attacks targeted iOS users from the United States and many European Union countries have been deployed extensively. The latest case was recorded as an attack campaign that took place for nearly a week, using the Chrome platform vulnerability for iOS to bypass the pop-up blocker built into the browser.

1. Adblock Plus filter can be exploited to run malicious code

eGobbler, the alleged culprit behind the attack, used both "8 individual attacks and more than 30 fake ads" throughout the process, during which each campaign spoofed deployed within 24 to 48 hours. According to researchers from Confiant, an organization that has detected and tracked targeted attacks on eGobbler's iOS, there were a total of about 500 million user sessions (user sessions).) has been appropriated to push fake ads in this large-scale campaign.

EGobber attacks usually only work for a maximum of 48 hours, after which a short "hibernation" period will be completed, ending when the next attack begins to be discovered by experts. of Confiant.

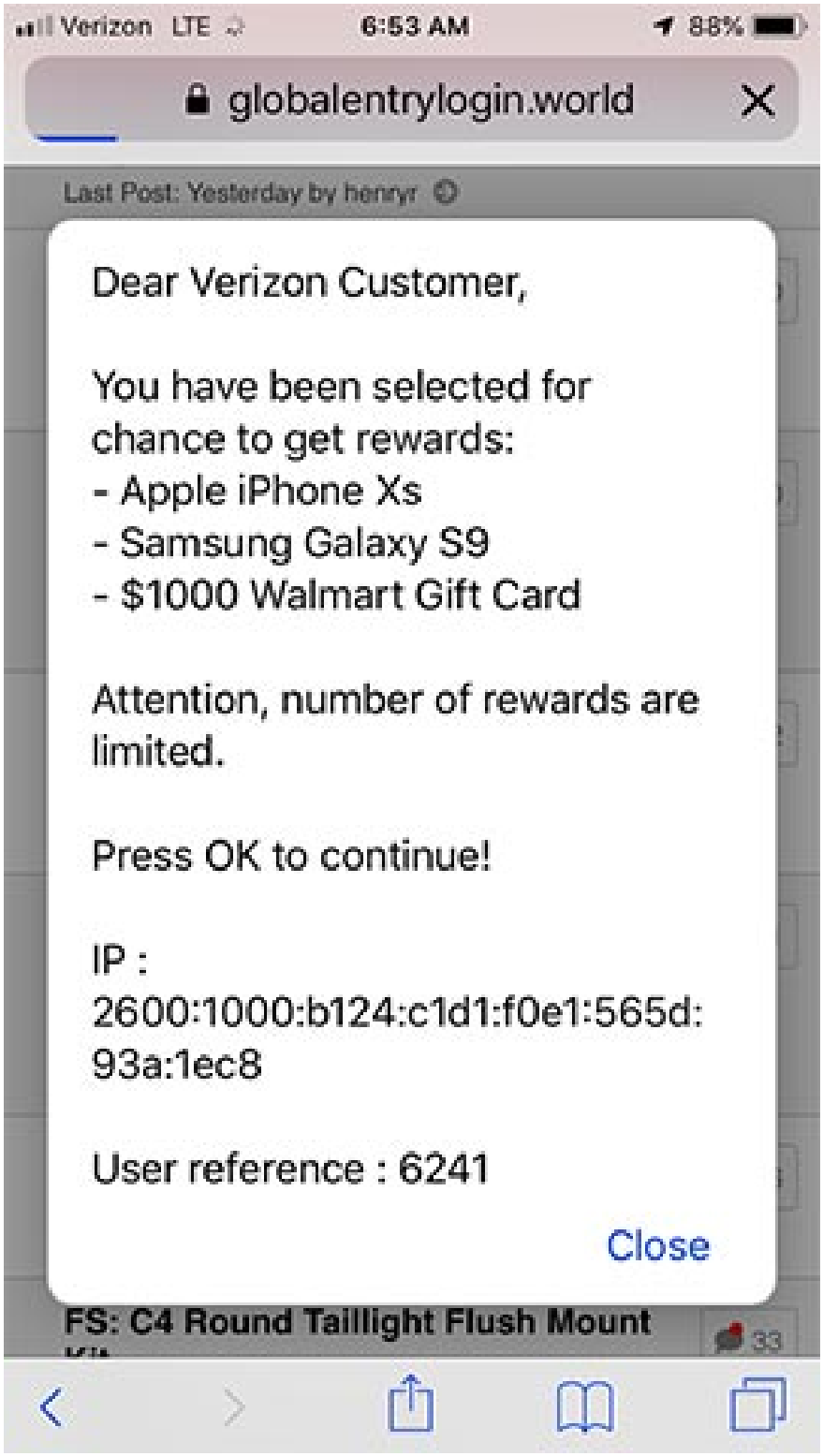


1. Authentication tool on many enterprise VPN applications that are bypassed by hackers

The attacks launched in April used landing pages hosted on multiple .world domains and at the same time used pop-up windows to take control of the user's session, as well as redirect the victim. multiply to malicious landing pages.

In fact, the use of pop-ups has also been observed previously as part of offensive campaigns, similar to a method used to redirect targets to enemy-designed enemy sites. malicious agent for fraud or malware infection purposes. However, this is definitely unusual when we consider the effectiveness of the browser pop-up blocker.

The crook's decision to use a pop-up to hijack a user's session has been revealed after researchers checked the campaign campaign's payload data on more than 2 dozens of devices, both physical and virtual, "as well as" this test split test between iframe (iframe) are deployed in the sandbox and non-sandbox environment '.



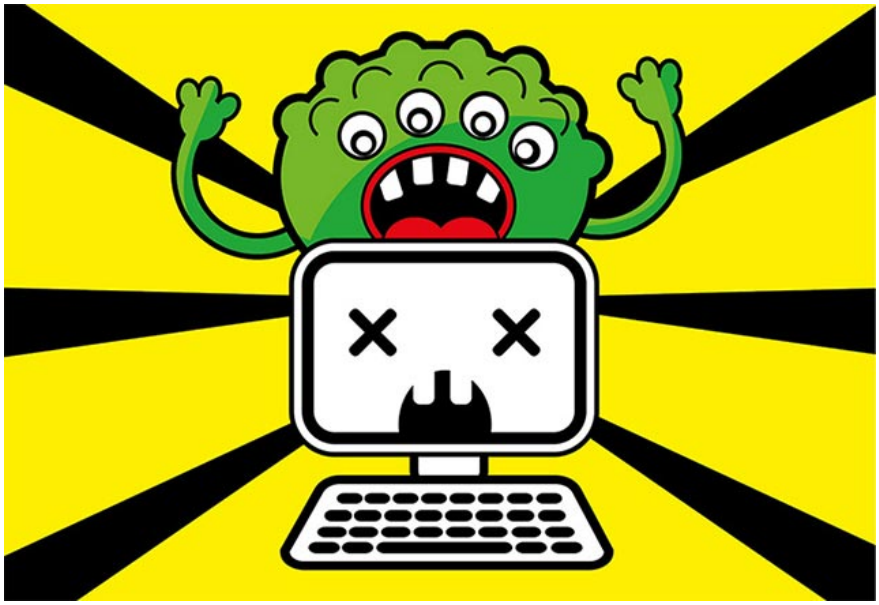
1. 25% of "out-of-the-box" phishing emails are the default security of Office 365

According to the researchers, the reason for the problem 'stems from the availability of payload techniques that have successfully utilized the Chrome iOS platform's ability to detect pop-ups that are triggered by people. use, from there to fool and surpass this feature '.

Sandbox was also outdone

To overcome the sandbox properties, the payloads used by the eGobbler group in these massive malicious campaigns exploited an unpatched vulnerability in the Chrome web browser for iOS - Chrome's security team is started investigating the problem after Confiant reported the vulnerability on April 11.

The problem lies in exploiting malicious ads used by eGobbler that cannot be prevented by standard sandbox attributes. This means that sandbox ad management properties built into Google's ad serving tools such as AdX and EBDA will also be fooled by payloads and their user interaction requirements.



1. The hyperlink test command is being used by hackers to perform DDoS

The attack that exploits this vulnerability can bypass the need for user interaction is absolutely impossible to occur under the same-origin policy because it involves native iframes cross.

Furthermore, this will also completely break the browser 's anti - redirect function, simply because the attacker no longer needs to create a redirect request to hijack the user session.

In fact, this is not the first time that assault campaigns based on similar malicious ads are designed to target a specific set of users, especially iOS. In November 2018, Confiant also tracked another campaign run by the ScamClub team, seeking to take over 300 million iOS users' sessions, and redirect them all to adult and trick content. Island through the form of gift cards. Like the information Confiant described in their report, "this is really an outstanding campaign compared to the other campaigns we've followed, not just based on payloads, but also the level of attack." .

1. Detect spyware targeting iOS users

In addition, after a pause, Confiant security experts also discovered on April 14 that the campaign shifted its focus to another platform, affecting nearly half a billion user sessions. . It can be said that this is one of the largest malicious advertising campaigns recorded in the last 18 months.

tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.