Threat Bulletin

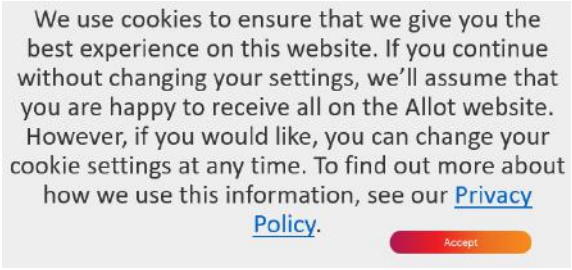
Browser Trackers (.trk)

February 2021

Introduction

Browser cookies store tiny bits of information about our online activity and are used by website owners to allow them to provide a better browsing experience, personalize content and advertisements, and keep users logged in to their various accounts. Justified concerns about online privacy spawned legislation that now requires site owners to disclose their cookies policies and get consent from users before tracking their activity. Today all legitimate websites haves a cookies policy notice and link to full information about the site's privacy policy.

Legitimate Cookie Policy Notice



But every Internet technology has a dark side, and while legitimate websites have adopted responsible policies and procedures, cybercriminals abuse the technology to install tracking cookies without user's knowledge or consent, and use the information peeped to customize phishing attacks, build and sell personal profiles on the black market and commit other fraud.

How are Users Infected?

The most common way users get infected with malicious tracking cookies is by simply visiting a tracker webpage containing the malicious cookies that then begin collecting the user's navigation information. Unfortunately, the average user will have no reason to be suspicious nor have the technical know-how to inspect and detect malicious browser cookies.

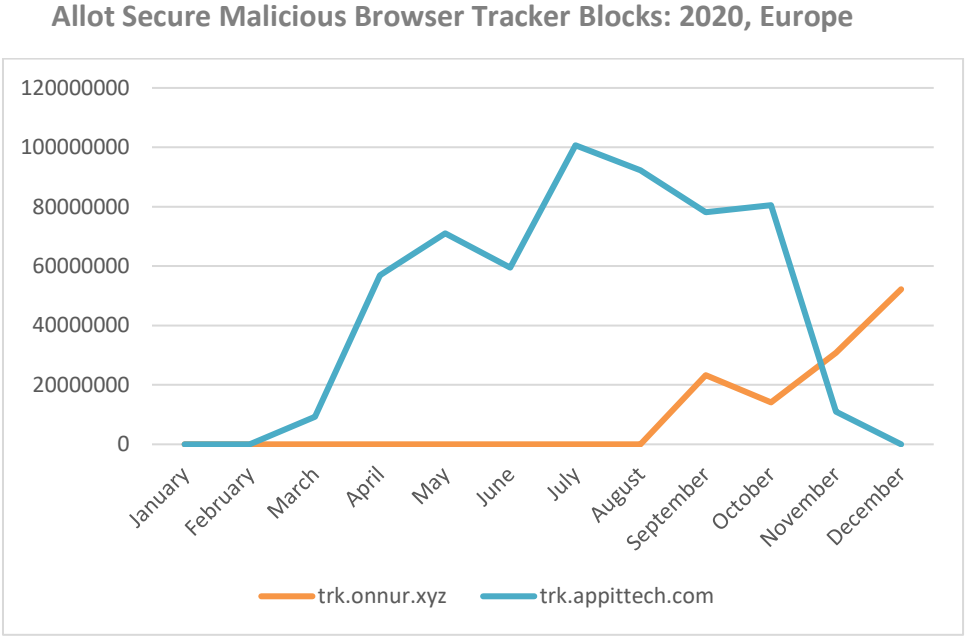
Malicious Activity

Once infected the tracker will continue to follow the user's online activity, monitoring and storing whatever information it wants, then send it off to a server controlled by the cybercriminals. The personal data collected is so immense and so sensitive it can be used for almost any kind of attack. Phishing attacks often use personal browsing data to learn about a victim's interests, social media accounts, what kind of ecommerce sites and product they tend to buy and even which financial apps they use. By gathering large amounts of online navigation information, cybercriminals can build in-depth personal profiles and sell them on the black market, build highly targeted personal spear phishing attacks that closely mimic routine online behavior or even intercept online banking credentials.

The sensitive browser navigation data is syphoned out via a connection made to a malicious website. If the user is protected by Allot Secure, that communication will be blocked and the information gathered never reaches the hands of cybercriminals.

Allot Secure Malicious Browser Tracking Blocks

During 2020 Allot Secure protected users in Europe from sending their personal navigation information to cybercriminals 679,686,161 times



Conclusion

Protect Subscribers with Allot Secure

Allot Secure allows CSPs to protect their subscribers from all types of cyberthreats by offering security as a service (SECaaS) from the network. Up-to-date threat intelligence and in-line anti-virus scanning protects users malicious browser trackers, and all types of malware, banking Trojans, crypto jacking, ransomware, and IoT specific attacks such as Mirai and its variants.

Allot Secure unifies network-based security, home and business gateway security and security clients into the CSP's own branded security service. It delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling.

To learn more about how service providers can increase customer satisfaction, NPS and ARPU by offering Allot Network Security Solutions, download the Telco Security Trends Report:

How Effective are CSP Security Services for the Mass Market?
or watch this video: **How Allot NetworkSecure Works**.