rechts van de bezochte webpagina toe zodat de grootte van je browservenster niet gebruikt kan worden om je te identificeren.

https://www.torproject.org/

TAILS 4.0

Van Tails (The Amnesic Incognito Live System) is versie 4.0 uitgekomen, de eerste versie gebaseerd op Debian 10 (Buster). Zoals het versienummer al aangeeft, bevat Tails 4.0 grotere vernieuwingen dan ooit. Zo is KeePassX vervangen door het actiever onderhouden KeePassXC en de Tor Browser heeft een upgrade gekregen naar versie 9.0. De Bitcoin-wallet Electrum werkt opnieuw en onder de motorkap draait Linux-kernel 5.3.2. De desktopomgeving is GNOME 3.30. De Tails Greeter die de gebruiker verwelkomt, is gebruiksvriendelijker geworden, het on-screen toetsenbord is gemakkelijker te gebruiken en Thunderbolt-apparaten zijn nu ook ondersteund. Bovendien start Tails 4.0 20 procent sneller, vraagt het besturingssysteem 250 MB minder RAM en is het image 47 MB kleiner dan Tails 3.16.

https://tails.boum.org/

ONIONSHARE 2.2

In versie 2.2 heeft het programma OnionShare om anoniem bestanden te delen op het Tor-netwerk er een nieuw tabblad bijgekregen: **Publish Website**. Sleep gewoon de bestanden die je wilt publiceren naar het tabblad en klik op **Start Sharing**. Dat start een webserver op je computer die deze bestanden deelt en maakt die beschikbaar op een .onion-adres. Dat adres is alleen bereikbaar voor wie met het Tor-netwerk verbonden is, en bezoekers hebben geen idee wie je bent, omdat ze je ip-adres of locatie niet zien.

https://onionshare.org/

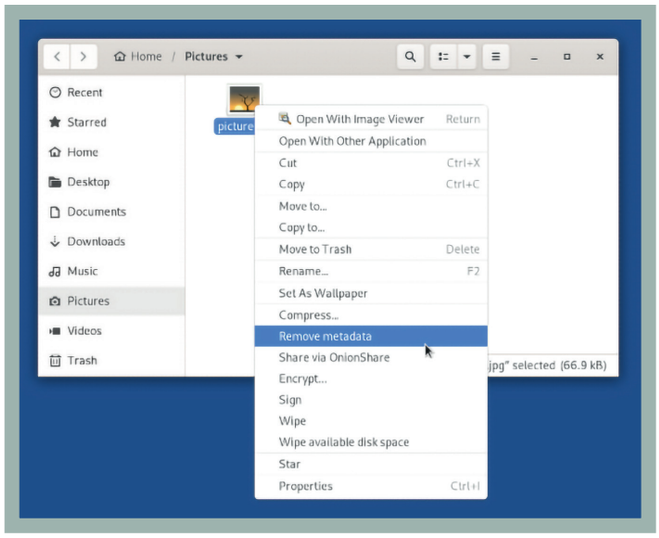
CODE UIT STACK OVERFLOW KOPIËREN IS NIET VEILIG

Veel ontwikkelaars die tegen een programmeerprobleem aanlopen, stellen hun vraag op websites zoals Stack Overflow en kopiëren blindelings codevoorbeelden die ze daar als antwoord krijgen. Dat is een groot beveiligingsrisico, blijkt uit een onderzoek door een groep computerwetenschappers uit Iran en Canada. Ze onderzochten meer dan 72.000 codevoorbeelden in C++ uit 1325 berichten op Stack Overflow. Daarvan bevatten 69 codevoorbeelden een kwetsbaarheid. Dat lijkt weinig, maar die 69 kwetsbare codevoorbeelden werden wel door 2589 GitHub-projecten gekopieerd. De onderzoekers waarschuwden al die GitHub-projecten. Ze hebben ook een browserextensie voor Chrome ontwikkeld die een Stack Overflow-gebruiker waarschuwt als hij onveilige code post.

https://arxiv.org/abs/1910.01321

RISICO'S NPM-ECOSYSTEEM HEEL GECONCENTREERD

Onderzoekers van de TU Darmstadt hebben de beveiligingsrisico's van het npm-ecosysteem van JavaScript-bibliotheken onderzocht. Ze komen in hun analyse met enkele cijfers die je doen nadenken. Als je een willekeurig npm-pakket installeert, vertrouw je impliciet gemiddeld 79 third-party pakketten en 39 maintainers. Populaire pakketten worden zelfs door meer dan 100.000 andere pakketten gebruikt (en vormen dus het ideale doelwit om aan te vallen). Sommige maintainers hebben op die manier rechtstreekse impact op honderdduizenden pakketten. Tot 40% van alle npm-pakketten hangt zelfs af van code met minstens één publiek bekende kwetsbaarheid. Laat dit even bezinken de volgende keer dat je `npm install` intypt…



Tails 4.0

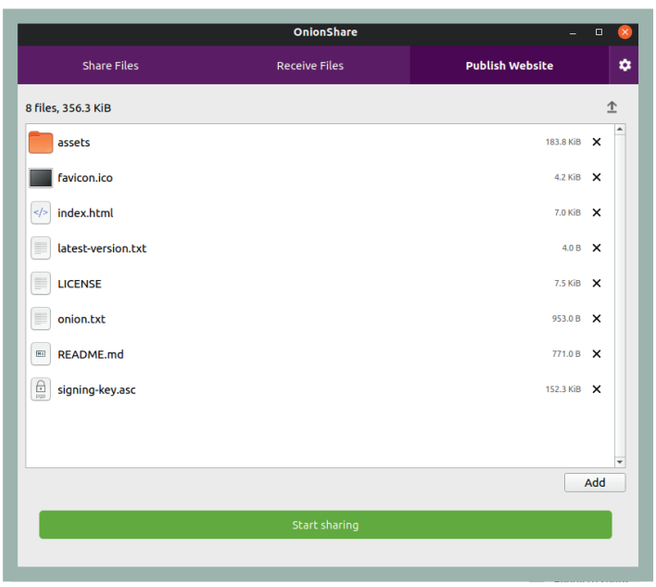
EN VERDER

OpenSSH heeft experimentele ondersteuning voor U2F/FIDO-hardwaresleutels gekregen. De implementatie gebruikt Yubico's libfido2 dat compatibel is met elk standaard USB HID U2F- of FIDO2-token, zoals recente modellen van de YubiKey. Dat laat authenticatie met een hardwaresleutel toe, tenminste als de ssh-server het nieuwe sleuteltype ondersteunt.

Door een verandering in het systeem van uitbreidingen van de e-mailclient Thunderbird zal versie 68.x de laatste zijn die de OpenPGP-extensie Enigmail ondersteunt. De ondersteuning voor Thunderbird 68.x stopt in de herfst van 2020. Thunderbird 78, gepland voor de zomer van 2020 zal OpenPGP-ondersteuning ingebouwd hebben, die de Enigmail-extensie vervangt.

Er werd weer een ernstig lek in Exim gevonden, waardoor aanvallers op afstand kwetsbare mailservers konden overnemen. En door een kwetsbaarheid in php-fpm konden sommige configuraties van de webserver nginx uitgebuit worden om op afstand willekeurige code uit te voeren. Onder andere Nextcloud gebruikte een kwetsbare configuratie.

Vanaf versie 70 toont Firefox bij een website zonder https een hangslot met een rode streep erdoor. Het klassieke 'groene slotje' voor websites met https wordt vervangen door een donkergrijs slotje. En terwijl bij een Extended Validation-certificaat voorheen de naam van het bedrijf in de adresbalk getoond wordt, komt die informatie in Firefox 70 in het informatiepaneel dat je bij een klik op het hangslot tevoorschijn brengt. Er komt ook een nieuw 'beschermingsicoontje' links van het hangslot voor toegang tot bescherming tegen trackers en cryptominers.



Onionshare 2.2