Firefox Send sends Ursnif malware

hornetsecurity.com/en/security-information/firefox-send-sends-ursnif-malware/

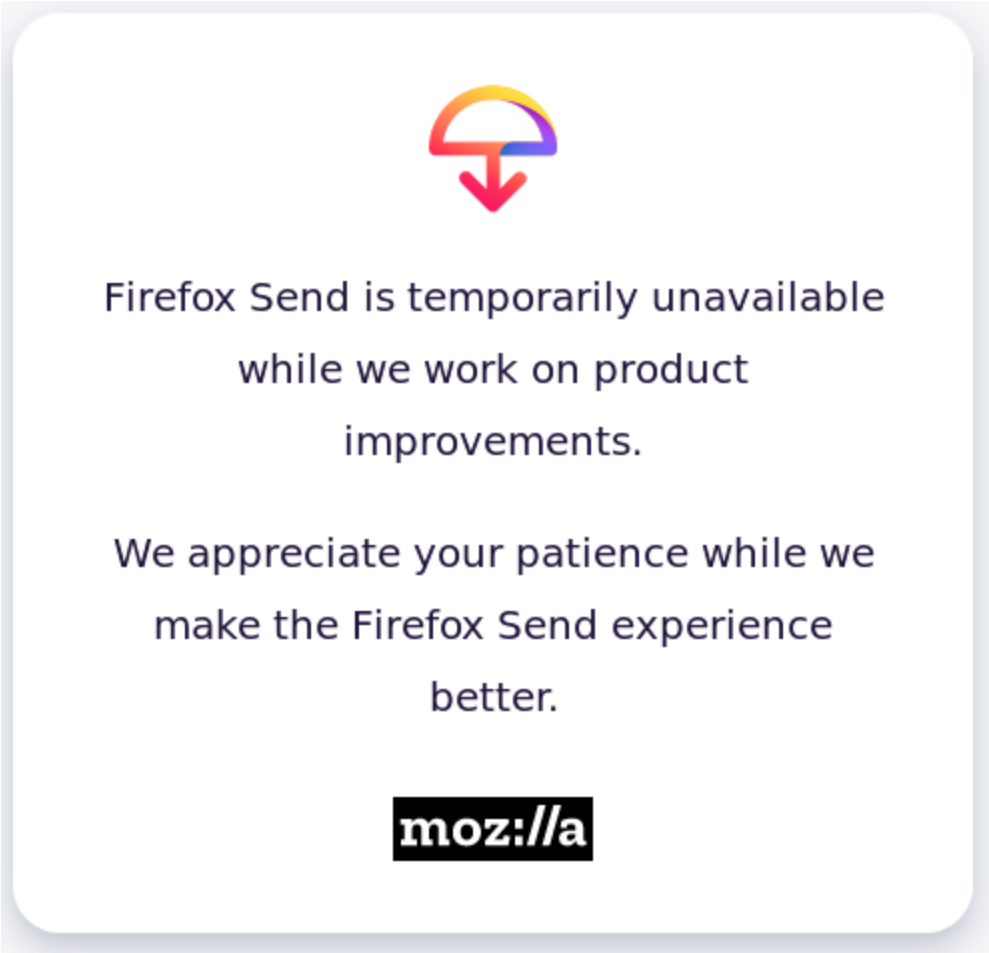
Security Lab July 18, 2020

Summary

On 2020-07-07 Mozilla temporarily disabled their Firefox Send service due to abuse by malware. Hornetsecurity's Security Lab explains how malware was abusing the Firefox Send service. To this end, a malspam campaign distributing a variant of the Ursnif malware is analyzed. The campaign used the Firefox Send service to host its malicious downloader and send victims these malicious Firefox Send links. Such abuse prompted Mozilla to disabled the Firefox Send service, because the service is currently lacking a feature to report abuse. Meaning even if researchers found these malicious links they could not be reported to Mozilla for takedown. However, our analysis further reveals that malware already abuses other services, hence, disabling Firefox Send – even though it was the right decision – has no impact on malware campaigns.

Background

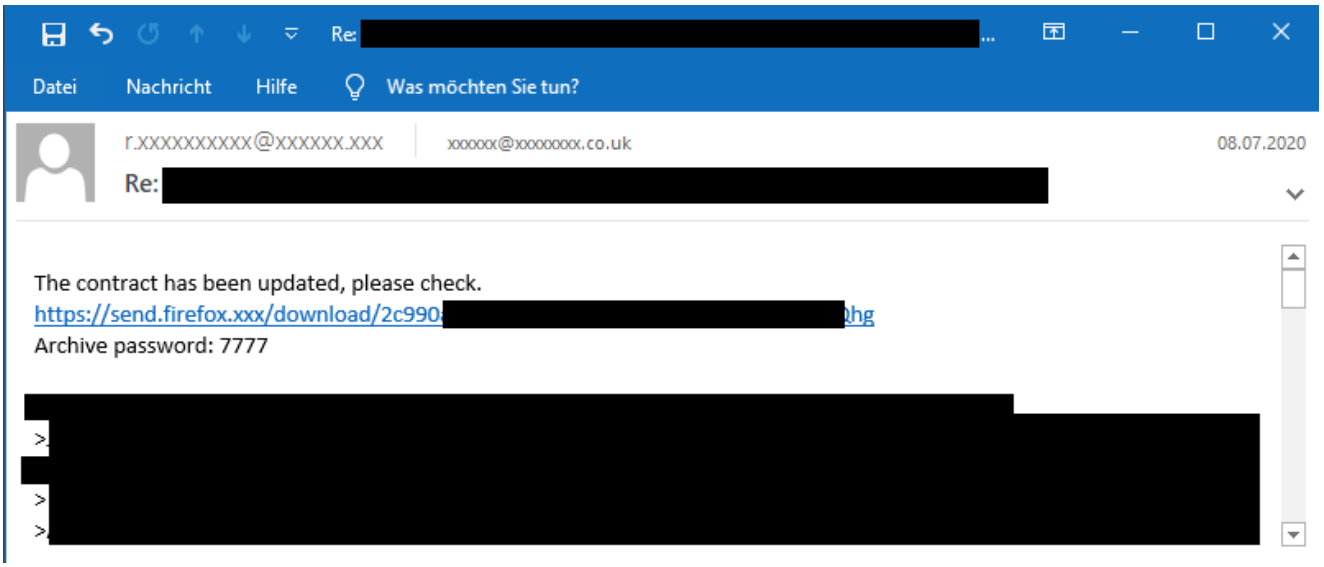
On 2020-07-07 Mozilla temporarily disabled their Firefox Send service due to abuse by malware. This was mainly done because the service does not offer a method to report abuse. Mozilla will likely enable the service again once they finish "work on product improvements" as stated on the message currently displayed when trying to reach the Firefox Send service's webpage:



To explain why Mozilla temporarily disabled their Firefox Send service, Hornetsecurity's Security Lab will analyze one malspam campaign distributing an Ursnif malware variant.

Analysis

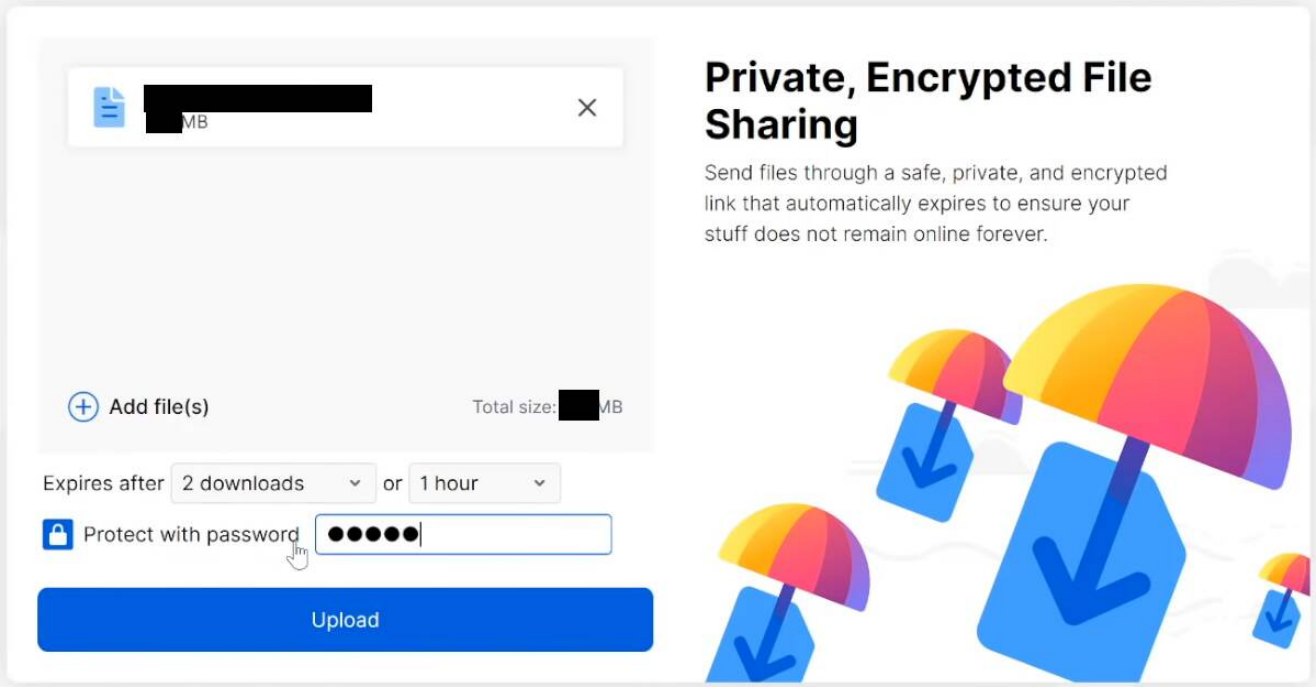
The campaign uses a mixture of link and attachment malspam distributing a VBScript file that downloads the Ursnif malware. The campaign leverages email conversation thread hijacking, i.e., the actors behind the attack will send their malware as a reply to their victims' existing email conversations. One example email using the Firefox Send service to host the malicious payload looks as follows:



The redacted parts contain a stolen email conversation thread that the campaign is replying to with its malicious link and a short message. The messages typically will state that a document has been updated and can be downloaded from the Firefox Send link. How good the malicious message fits into the hijacked email conversation thread seems to depend on chance, i.e., the message will refer to updated documents regardless what the conversation thread was really about.

The Firefox Send link will lead to a VBScript file. The VBScript file downloads an Ursnif variant most likely developed from another Ursnif variant called ISFB for which the source code is available publicly.

Then on 2020-07-07 Mozilla decided to temporarily disable Firefox Send, because the service does not feature a mechanism to report abuse. That means the download links can not be reported to Mozilla by security researchers. An abuse report feature is important to have for an online service, especially since the privacy focused nature of Firefox Send provides many opportunities for abuse. For example, the links can be password protected. The number of downloads, as well as, how long the download will be available, can be restricted:

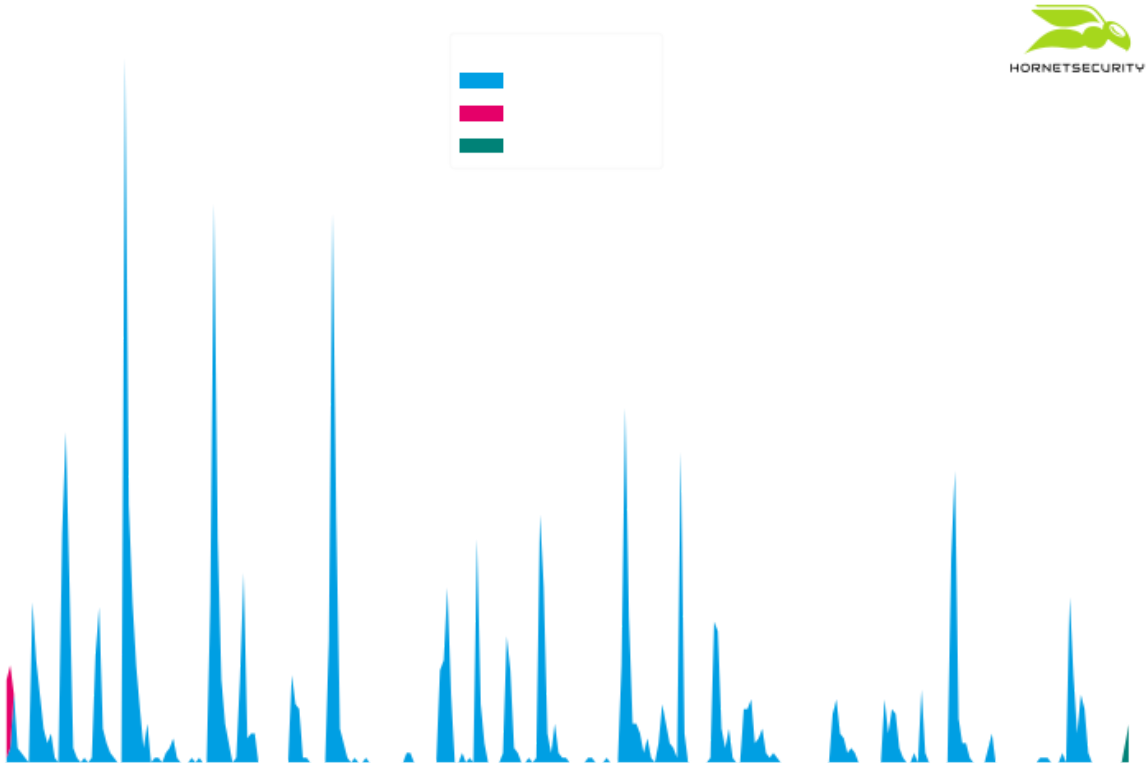


This means an attacker can limit the amount of downloads to one for his victims. In case of a successful compromise an incident response team can not download the original malware payload anymore to reconstruct the infection. If the malware deletes its files after infection it will be hard to trace such an attack.

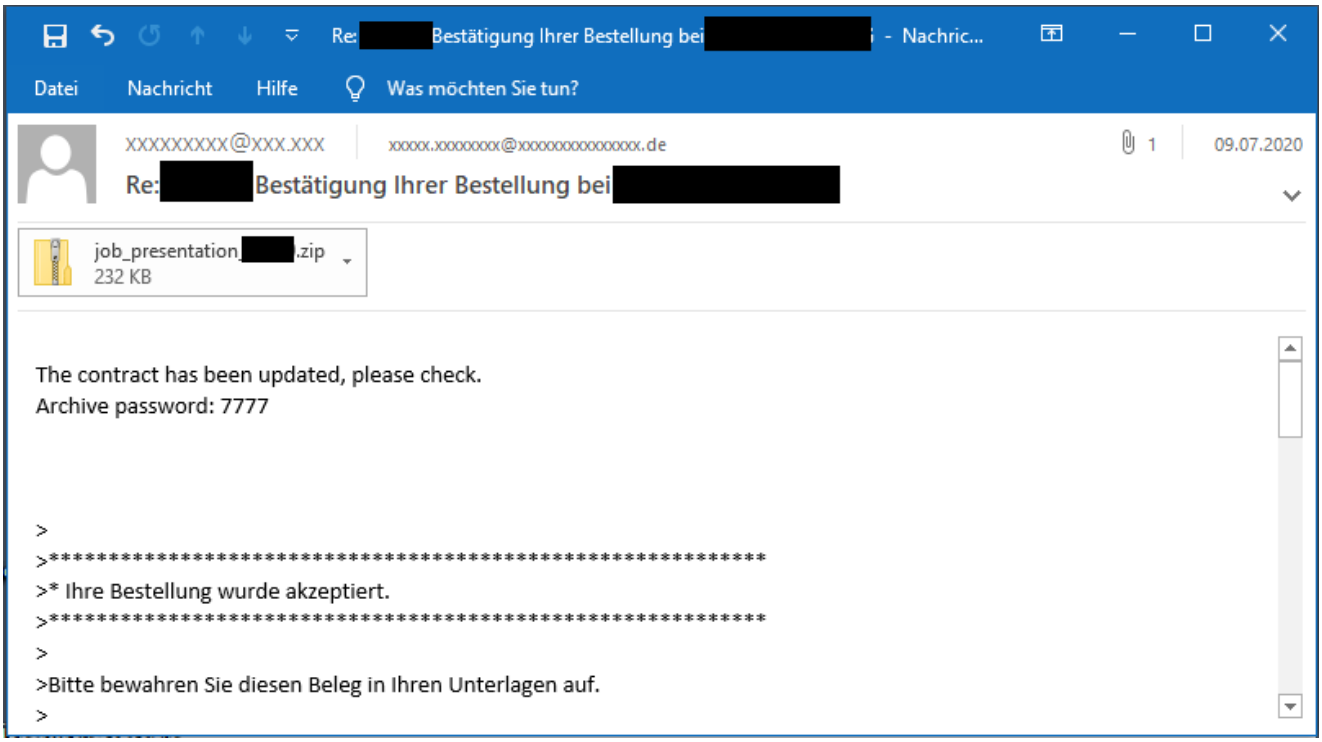
Another problem arises for legitimate use of the service and security software scanning such one-time download links. If security software downloads the file in order to scan it, the real recipient can not download the file anymore as the security software has already used the one available download.

For these reasons the Firefox Send service will highly likely continue to be abused once it returns. The abuse report feature will mainly be useful to report links that allow for multiple downloads and are used over a longer period of time. Reporting one-time download links could aid Mozilla in curbing abuse by detecting patterns in the way the actors behind the abuse interact with their service and then blocking them.

But even if the Firefox Send service should implement better protections against abuse the discussed malspam campaign does not depend on the Firefox Send service at all. The campaign used the Firefox Send service starting from 2020-06-01 (transitioning from using Google Drive links) to the day it was disabled:



However, the campaign has used Google Drive and Dropbox links before using Firefox Send links. It also used encrypted ZIP attachments instead of download links and as soon as the Firefox Send service was disabled it switched to such an encrypted ZIP attachment scheme:



Both Google Drive and Dropbox allow abuse reports, however, they are still abused by malware. This means when Firefox Send returns it will also get abused again.

Conclusion and Countermeasure

While we applaud Mozilla for temporarily disabling the Firefox Send service until an abuse report feature is implemented, the analysis of the discussed malspam campaign indicates that the Firefox Send service is only on of many services abused for malware distribution and adding the abuse report feature will not stop such abuse.

To protect against such attacks, especially the outlined email conversation thread hijacking, users should be cautious when they receive an out-of-order reply from a conversation partner, that tries to entice them to open links or other documents, either attached directly to the email or via a file hosting service, especially when such documents do not fit into the conversation and/or are delivered via an unusual mechanism, e.g., if documents are usually shared via a company internal file sharing solution, users should be especially cautious opening files shared via external services.

Hornetsecurity's Spam Filtering and Malware Protection, with the highest detection rates on the market, already detects and blocks all variations of the outlined emails currently distributing the Ursnif malware variant. Here it is also important that users do not let themselves be fooled by the outlined email conversation thread hijacking. Hornetsecurity's Advanced Threat Protection extends this protection by also detecting yet unknown threats. When using Hornetsecurity's encryption service a third-party service such as Firefox Send to

encrypt sent documents is not necessary. Outgoing emails are automatically encrypted with one of the common encryption technologies (PGP, S/MIME or TLS), depending on the set policy and availability of the corresponding certificates, without any further user intervention.

References

- [1] https://send.firefox.com/
- [2] https://www.zdnet.com/article/mozilla-suspends-firefox-send-service-while-it-addresses-malware-abuse/