Phishing Campaigns Abusing IPFS

Date: February 2023
Category: Advisory

CTM360 has recently identified a growing number of phishing cases using IPFS (InterPlanetary File System). IPFS is a decentralized system for storing and accessing files, and it has gained popularity due to its potential to improve the efficiency and security of file sharing. However, like any new technology, it also comes with its own set of risks and challenges.

Due to its decentralized nature, threat actors use IPFS to host fake websites, as the files are stored on multiple nodes, rather than on a central server. **This makes it challenging to take down the fake website since no central authority can be contacted to remove the website**. Furthermore, IPFS websites can be accessed through a content identifier (CID) *(a unique string of letters and numbers)* which is a label used to point towards the content in IPFS rather than a traditional URL, which can make it more difficult for victims to recognize a phishing attempt.

When a file is uploaded to IPFS, it is split into smaller parts and distributed across different nodes. Each part has a separate hash, which helps the network identify different parts of the file on different nodes. In order to retrieve the files, the hash is entered into the browser. Once identified, the IPFS requests all the parts of the file through a P2P connection. Even if the file is deleted from one node, it can still be accessible on other nodes. IPFS URLs often follow this format:

- hxxps://ipfs[.]io/ipfs/{46 random character string}#{user email address}
- hxxps://ipfs[.]io/ipfs/{46 random character string}?(filename|key)={random character string}
- hxxps://ipfs[.]io/ipfs/{46 random character string}?filename={file name}\.html &emailtoken={email address}

The content stored within the IPFS network can be accessed using IPFS nodes called ‘gateways’ which act as a bridge between the HTTP protocol used by all the web browsers and the IPFS network. The gateways can be set up by anyone using various publicly available tools. The most popular gateways used are the **ipfs.io** ,**Fleek**, **Dweb.link**. Other publicly available IPFS gateways can be found in Appendix.

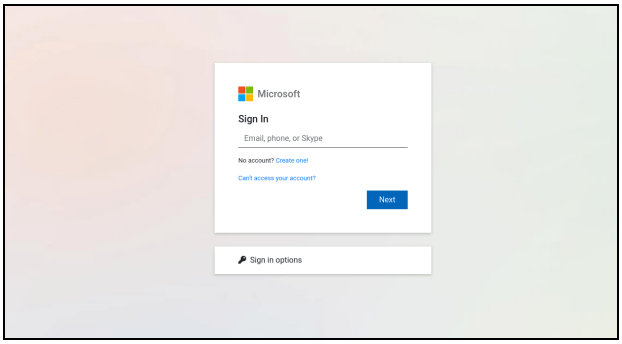
Various Phishing cases observed on IPFS

Below are some phishing cases observed using IPFS services:

Sharing IPFS links through emails

Phishing attacks are carried out by attackers using social engineering techniques to lure the victim into clicking a link or file embedded in the email. The email contains an IPFS link or an embedded HTML file that looks like a legitimate site, such as Microsoft or DHL.

URL Observed:
hxxps[:]//**ipfs[.]io**/ipfs/bafybeibgsqc62urteqhu2l3bq3mql5j2sceysff6wyf5kgqvl7ixiq3icm/ef[.]html

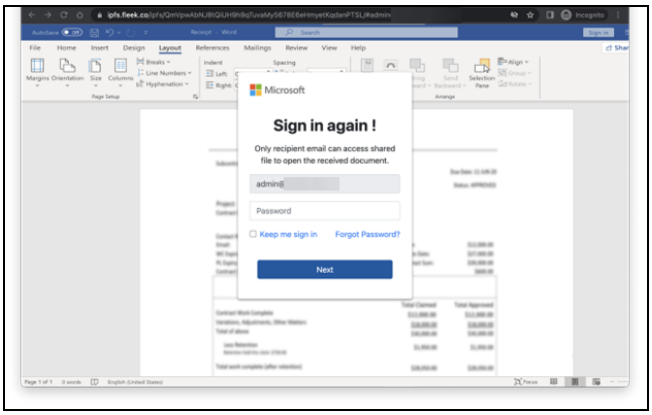


Generic phishing page hosted on IPFS

HTML File hosted on IPFS

In another case, CTM360 has witnessed threat actors utilizing HTML files in their phishing attacks. The HTML file redirects the victims in turn to the destination URL hosted in the IPFS network for stealing their credentials. Upon opening the file, the user is redirected to a document page asking for login credentials.

URL Observed
hxxps://ipfs[.]fleek[.]co/ipfs/QmVpwAbNJ8tQUH9h9qTuvaMy5678E6eHmyetKqdanPTSL/#adminiev



HTML file hosted on IPFS

IPFS hosted phishing exploiting Google Translate service

Scammers have also implemented a technique where the Google Translate service is being abused. Google Translate lets you translate entire websites simply by passing it a link and selecting the source and target languages. Therefore, it can pose a fake “good” reputation for the websites due to the abuse of Google's official domain, and hence, getting it fraudcasted on safe browsing is also challenging since it is associated with a genuine Google service.

Phishing URL:
hxxps[:]//z4db4kcmazkuxame2l2iy42m7yf5b2mysb7lqepzngrhk33a-ipfs-dweb-link[.]translate[.]goog/ML[.]html?victim@victim.com+&_x_tr_hp=bafybeifjos&_x_tr_sl=auto&_x_tr_tl=en-GB&_x_tr_hl=en-GB

Conclusion

By integrating the idea of decentralized cloud services with IPFS, phishing tactics have advanced significantly. This malicious usage of IPFS is expected to rise further, highlighting the importance of being cautious. Organizations need to provide regular training and awareness programs that will educate employees and their customers on new phishing techniques, how to spot and report different phishing cases. Further, blocking identified phishing URL patterns could also mitigate some risks.

Appendix

Below is a list of public IPFS gateways accessible across the internet without a central governing authority:

Video.oneloveipfs.com
Jorropo.net
4everland.io
Gateway.ipfs.io
Gateway.pinata.cloud
Storry.tv
Ipfs.eth.aragon.network
Dweb.link
W3s.link
Ipfs.litnet.work

Ipfs.io
Cloudflare-ipfs.com
Via0.com
Ipfs.kaleido.art
Ipfs.joaoleitao.org
Ipfs.best-practice.se
Nftstorage.link
Ipfs.runfission.com
C4rex.co
Ipfs.ink
Cf-ipfs.com
Hardbin.com
Ipfs.jpu.jp
Ipfs.fleek.co

Disclaimer

For more information:

Email: monitor@ctm360.com Tel: (+973) 77 360 360