Cofense Intelligence™ Strategic Analysis

Phishing Campaigns Abusing Web3 Platforms Increases 482% in 2022

The term “Web3” refers to a set of technologies intended to decentralize common internet and computing activity. Proponents of decentralization tout the ability to host content without the need for large technology companies. In short, anybody can publish any content, avoiding technical problems like server management as well as legal problems or censorship. Unfortunately, these features make the technologies attractive to threat actors seeking easy, robust hosting for malicious content. Analyzing credential phishing campaigns that reached inboxes during the first three quarters of 2022, we found massive growth in the abuse of Web3 platforms for phishing during the first three quarters of 2022. In this report, we explain the utility of Web3 platforms for phishing threat actors and analyze the growth and other trends in malicious Web3 usage.

Why Web3 Is Good for Phishing Threat Actors

Threat actors are regularly abusing several similar Web3 platforms. Each platform has two essential characteristics that make them useful to phishing threat actors:

- Anyone can host content within the platforms simply by running the relevant software. No central servers are involved. Instead, content is collaboratively hosted by the platforms’ users. From a threat actor’s perspective, the users unwittingly provide free, anonymous, no-questions-asked hosting.
- No company or governing organization moderates hosted content. While some measures are available to limit access to malicious content, it’s impossible to prevent it from being hosted within the platforms or to remove it once it has been hosted. The lack of oversight gives malicious content a longer lifespan, saving threat actors the trouble of finding new hosting.

Generally, the platforms are designed to make content hosting more available to individuals, evade censorship, and guarantee access to published content. But these features also make the platforms attractive for threat actors seeking to host malicious content.

Each platform is designed with different underlying technologies and use cases in mind, yielding differences in the ways threat actors can abuse them. For more details on the platforms and protocols involved, see Appendix A.

© Copyright 2022 Cofense™. Confidential. All rights reserved.

Malicious Use of Web3 Exploded in Q2, Still Increasing Steadily

Web3 platforms are an increasingly common method of hosting malicious content for phishing campaigns, as Figure 1 shows. Although a few malware campaigns have recently started to use Web3 platforms to host their payloads, credential phishing constitutes nearly all of the abuse so far. Our analysis in this report covers credential phishing emails found in users' inboxes during Q1 to Q3 2022. Web3-hosted content was involved in 1.5% of credential phishing campaigns reaching inboxes in Q1. During Q2, that figure more than quintupled, accounting for an 8.0% share of campaigns reaching inboxes. In Q3, the share increased to 8.8%, with the number of campaigns abusing Web3 platforms being 482% of the number observed in Q1.

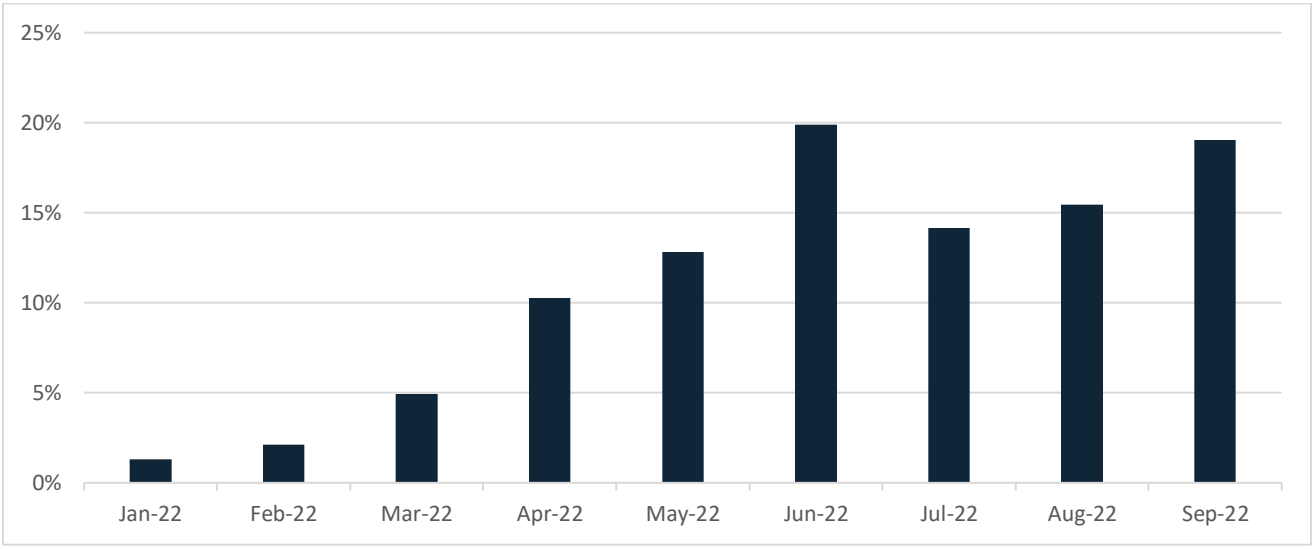

Figure 1: Emails found in commercial inboxes that included Web3-hosted malicious content. The graph shows each month's share of the total number of emails from Q1 to Q3 of 2022.

Several services allow for easy use of Web3 technologies, including the generation of gateway URLs that can be accessed with a web browser. The URL's domain reflects which service was used to create it. Fleek (fleek.co) was the most popular service for threat actors, accounting for almost half of the URLs in the campaigns we analyzed.

© Copyright 2022 Cofense™. Confidential. All rights reserved.

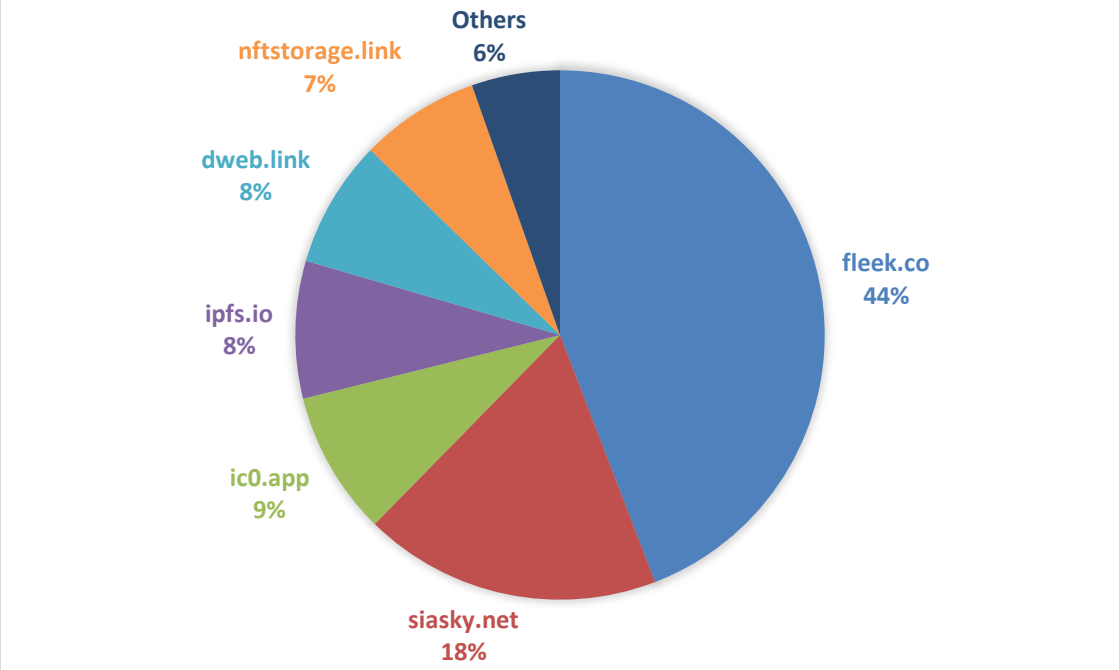

Figure 2: Share of URLs from each Web3-related service in credential phishing emails, Q1 to Q3 of 2022.

The second most common service, Skynet Labs (siasky.net), announced recently that it is shutting down, effective November 15, 2022. Skynet Labs URLs have not declined meaningfully in October, but the shutdown will almost certainly affect the distribution of Web3 URLs in November and beyond.

How Web3 URLs Are Used in Phishing Emails

As in our past analyses of domains used in credential phishing emails, we divide malicious URLs into two stages. Stage 1 URLs are embedded into the email itself, but rarely go directly to the credential phishing page. Stage 2 URLs include any that are involved after the user has opened the link embedded in the email.

Only 21% of Web3 URLs are used in Stage 1. Since Web3 platforms lack content censorship by design, organizations are more likely to block emails linking to them. Threat actors continue to prefer abusing well-known services like Adobe, Google, and Microsoft, which organizations are essentially unable to block.

© Copyright 2022 Cofense™. Confidential. All rights reserved.

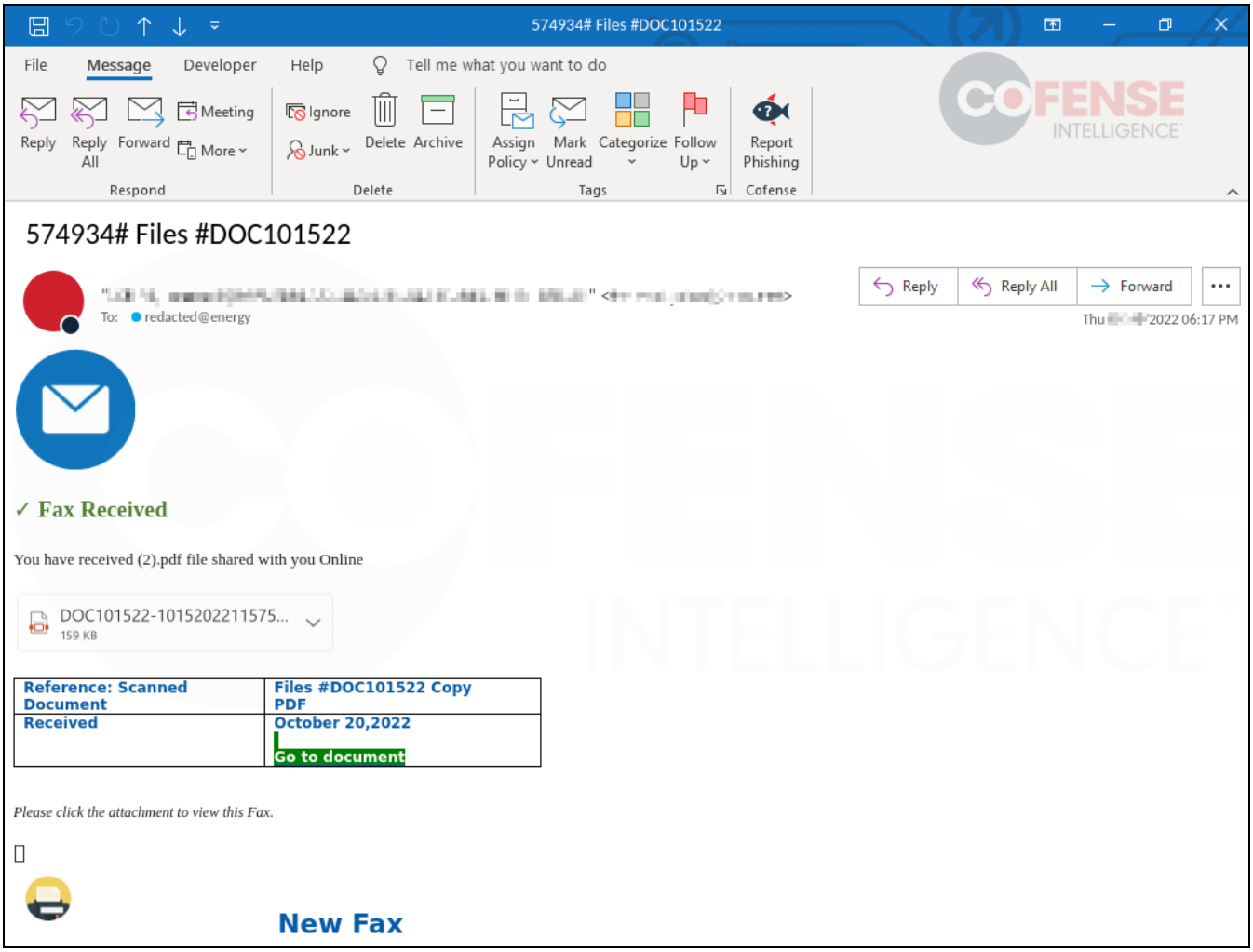

Figure 3: A fax-themed email linking to a fraudulent page hosted on the Microsoft Customer Voice service.

© Copyright 2022 Cofense™. Confidential. All rights reserved.

Figure 4: The fraudulent page linked in the email from Figure 3. It leads to a phishing page hosted on Skynet.

By contrast, Web3-hosted content is well suited to threat actors' needs in subsequent stages of the phishing campaign. Broadly speaking, content published on Web3 platforms is permanent. Moreover, Web3 publication removes the need for creating or stealing accounts, compromising websites, or registering new domains to host a credential phishing page. Threat actors can continuously publish new phishing pages to stay ahead of countermeasures.

© Copyright 2022 Cofense™. Confidential. All rights reserved.

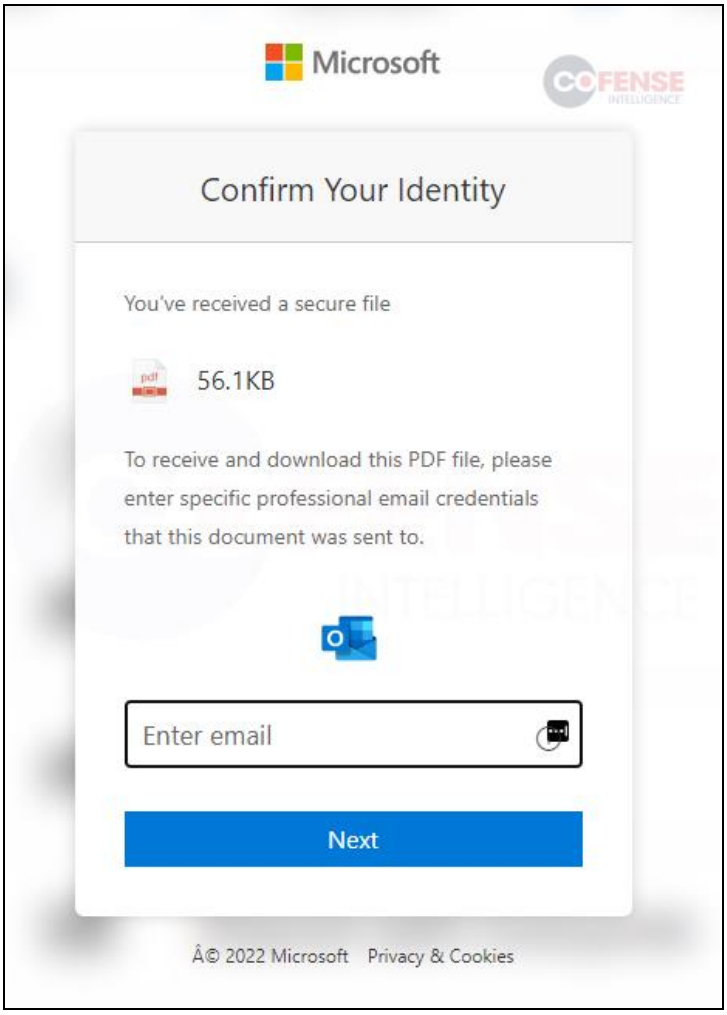

Figure 5: The Skynet-hosted phishing page linked by the campaign in Figure 3.

Although Web3 platforms may be a good hosting solution for threat actors, they cannot perform data exfiltration on their own. None of the Web3 technologies can receive input from a user and send it to an exfiltration service. Instead, threat actors still rely on embedded forms or JavaScript code, so that the victim's browser sends captured login credentials to endpoints under threat actor control.

Outlook

Web3 technology offers little downside to threat actors at present. In the near future, there is no reason to doubt that Web3 abuse will continue to increase in both credential phishing and malware.

Over the longer term, if Web3 technology gains adoption in the everyday life of users and organizations, the opportunity for abuse will only grow. For example, most browsers currently need gateway services to create URLs for them to access decentralized content using the InterPlanetary File System (IPFS–see Appendix A for more details). Those services can disable a URL if it is reported as malicious. But if browsers receive native IPFS support in the future, then opening an IPFS link will be similar to opening a saved file from the user's hard drive.

© Copyright 2022 Cofense™. Confidential. All rights reserved.

By design, decentralization technology puts all the responsibility for publishing and for consuming content on individual users. For network defenders, that prospect involves a significant amount of risk. Short of outright blocking all Web3 gateway services (for those companies that have no need for legitimate access to such services), keeping users educated and vigilant remains the best feasible preventive measure for the foreseeable future.

Appendix A: Description of Web3 Technologies Used for Phishing

Gateway URLs

Each of the Web3 technologies covered in this report creates a network of many different computers working together to host content or applications. They include protocols that allow users to access the content or applications, but in most cases, those protocols are not currently supported directly by web browsers. To make the services more usable, the protocols also include a way to create "gateway URLs," which allow browsers to open Web3-hosted content or applications as though they were hosted on a traditional server. These are the services threat actors use to send links to the phishing pages they host using Web3 technologies.

Services that provide gateway URLs are operated by a mix of commercial and community organizations. Gateway services can help speed up the adoption of Web3 technology by making it more usable by current browsers. However, they also effectively centralize access to Web3-hosted content because they can choose to disable a gateway URL that points to malicious or illegal content. All the operators of gateways we found in our data have a way for users to report malicious content.

InterPlanetary File System (IPFS)

IPFS is a protocol for decentralized storage and serving of content. An IPFS user wishing to publish a piece of content can choose to make it available from their computer. Initially, other IPFS clients download the content from the original publisher's computer. When they do, they also start to make the content available to more clients. This way, IPFS essentially serves as a content distribution network, ensuring that content remains available–and from one or more nearby hosts, which improves performance.

Protocol Labs, the organization responsible for IPFS development, operates a few gateway URL services for IPFS. Others are operated by commercial entities attempting to utilize and enhance IPFS for their customers. Protocol Labs maintains a list of public IPFS gateways.

Sia / Skynet / Skynet Labs

Sia is a blockchain project that utilizes users' empty disk space to act as part of a distributed file storage platform. It has its own cryptocurrency, Siacoin, which is used to "rent" disk space on computers running the Sia software. Skynet is a technology built on top of Sia intended to be used for web and application hosting. The organization behind it, Skynet Labs, operates a gateway service (siasky.net) that has been popular with threat actors. That gateway service will be shut down in November 2022, but Skynet will still be accessible using other gateway services.

© Copyright 2022 Cofense™. Confidential. All rights reserved.

Internet Computer

The Internet Computer is a general-purpose blockchain designed to run apps, similar the smart contracts of the Ethereum blockchain. Serving content directly to a web browser is a unique ability of apps running on the Internet Computer. Dfinity, the organization that developed the Internet Computer, operates the domain ic0.app, serving a similar purpose as the gateway services mentioned above. Dfinity maintains a code of conduct specifying several prohibited categories of content. If an app is serving malicious content, Dfinity will disable the public URL on the ic0.app domain, leaving the app inaccessible (even though it is still running).

© Copyright 2022 Cofense™. Confidential. All rights reserved.