PerSwaysion Threat Actor Updates Their Techniques and Infrastructure

2022-01-18
By Alec Dhuse

The PerSwaysion phishing campaign is back. The threat actor behind PerSwaysion is now using a more direct phishing method and updated techniques from previous campaigns, aimed at stealing credentials for Microsoft 365.

A Quick History of PerSwaysion

In April of 2020 the Group-IB Threat Intelligence team published an investigation of a series of phishing attacks they dubbed the PerSwaysion Campaign. This campaign targeted high-level executives with attacks going back to at least August 2019. Group-IB concluded these attacks were likely perpetrated by a Vietnamese-based threat actor. You can read their write-up here: https://blog.group-ib.com/perswaysion

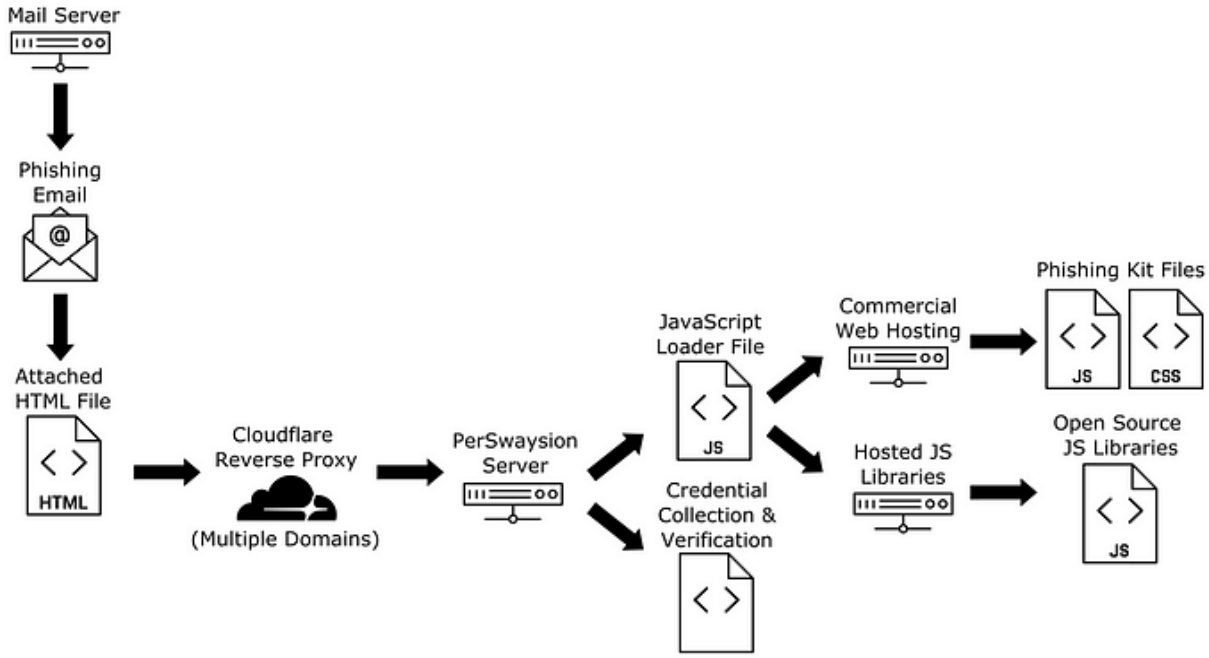
More than a year later, in November of 2021, SeclarityIO published an in-depth analysis of PerSwaysion's phishing kit code and its infrastructure. Their write-up can be accessed here: https://www.seclarity.io/resources/blog/the-art-of-perswaysion-phishing-kit/

This article will focus on the changes in techniques and the current infrastructure used in the latest phishing campaigns we've observed.

Attack Chain

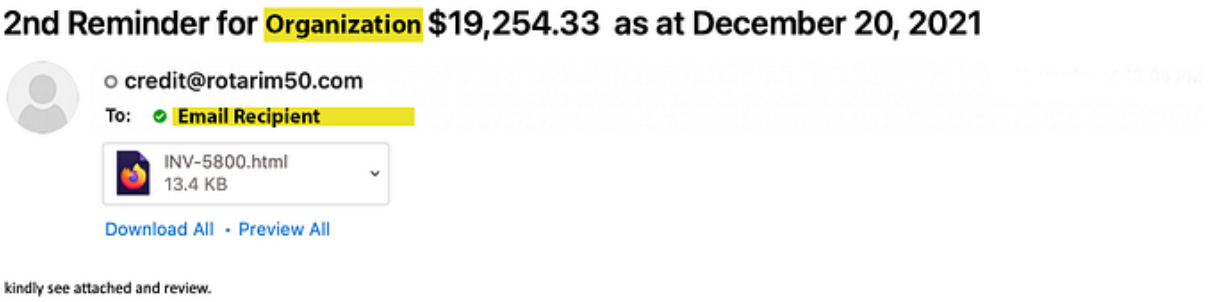
In the past, PerSwaysion phishing pages were hosted on file sharing websites or hosting sites that had a trial or free version. This was based on the assumption that the phishing campaign would be completed before the phishing page was taken down or the trial period expired.

In their most recent campaigns, this threat actor has switched from using a hosted phishing site to an HTML file attached to a phishing email. The attached file then loads a series of support files to display a copy of Microsoft 365's login page. See below for the diagram of the attack chain.



PerSwaysion Attack Chain

Phishing Email — The Lure



Screenshot of a PerSwaysion phishing email.

The latest emails were observed being sent from Amazon's Simple Email Service, with each email passing both Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) protections.

The domains **gemlacksresults[.]net** and **rotarim50[.]com** were being used as sender domains. Both sender domains are registered through sav.com, and were used less than 30 days after having been registered.

The previous run of phishing emails was observed sending using stolen Google Mail accounts.

The HTML Attachment

The payload of the phishing email is an HTML attachment. The content of this file is obfuscated using multiple layers of JavaScript functions. Presumably, this is to evade some email filtering systems as well as to prevent causal analysis of the payload. Despite this, Microsoft's Exchange Online Advanced Threat Protection detects these attachments as malicious.

The first layer of obfuscation is Base 64 encoded text that is decoded using built-in browser functions. The decoded text is then written to the Document Object Model (DOM). This is a common technique observed in phishing emails with HTML attachments. This is generally seen with the Base 64 decoding nested inside the document write function like this:
document.write(atob("[Base 64 Text]"));

The next layer of obfuscation uses a modified JavaScript minifier and packer function originally developed by Dean Edwards. This modified version includes additional array lookup and replacement, with the lookup array containing character-shifted cipher values.

Despite all the layers of obfuscation, the attached HTML page is a simple wrapper that adds anti-debugging JavaScript statements and a single link to an external JavaScript file. This external JavaScript file loads additional resources to display the phishing page to the victim (for ease of reference, we will be calling this file the JavaScript loader file).

The JavaScript loader file is hosted at **hXXps://valdia.quatiappcn[.]pw/[hex digits].js** Older campaigns have been observed using **hXXps://kifot.wancdnapp[.]page/[hex digits].js** as the host for this file. In all the campaigns we have observed, there are multiple JavaScript loader files hosted here, with each file having a unique filename consisting of hexadecimal numbers.

The loader file will in turn load the additional library files used in the phishing kit. Each unique loader file loads the same library files except for one file that is unique to each loader filename. That unique file has a filename with 32 hexadecimal characters and a .js extension. It contains a hard-coded string that appears to be Base 64 encoded text, but does not decode into anything recognizable. This may indicate that the contents are encrypted or that it is an API key used on the PerSwaysion server to differentiate between campaigns or users.

The JavaScript loader file loads these phishing kit resource files:

hXXps://rikapcndmmooz.firebaseapp.com/njtyzxntbfsdvxxz/themes/css/7f01272697919812996411ac56c3d204nbr1639582853.css

hXXps://rikapcndmmooz.firebaseapp.com/njtyzxntbfsdvxxz/themes/css/069a654bc4a1e6e66a713098353bb534nbr1639582853.css

hXXps://rikapcndmmooz.firebaseapp.com/njtyzxntbfsdvxxz/themes/7f01272697919812996411ac56c3d204nbr1639582853.js

hXXps://rikapcndmmooz.firebaseapp.com/njtyzxntbfsdvxxz/themes/ab50d0179cfb0f7e29d68bebaaa0e399.js

hXXps://rikapcndmmooz.firebaseapp.com/njtyzxntbfsdvxxz/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301639582846.js

As well as these open-source JavaScript libraries:

hXXps://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js

hXXps://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js

hXXps://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js

hXXps://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js

hXXps://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js

hXXps://unpkg.com/axios@0.16.1/dist/axios.min.js

hXXps://unpkg.com/lodash@4.17.4/lodash.min.js

hXXps://unpkg.com/vue@2.6.11/dist/vue.min.js

hXXps://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js

Older campaigns hosted the files on a different Google Firebase domain:

hXXps://rikcndapplala.web.app/zxhjkmnjdbfxzvdzx/themes/css/5ec43dada25c716f7880b0b8e6ff5e61nbr1633368005.css

hXXps://rikcndapplala.web.app/zxhjkmnjdbfxzvdzx/themes/css/26ee67cd59cf7ee7f6ca4f6e3a4695f9nbr1633368005.css

hXXps://rikcndapplala.web.app/zxhjkmnjdbfxzvdzx/themes/5ec43dada25c716f7880b0b8e6ff5e61nbr1633368005.js

hXXps://rikcndapplala.web.app/zxhjkmnjdbfxzvdzx/themes/a144f6f5e581d7026db3c04ffe1ab2da.js

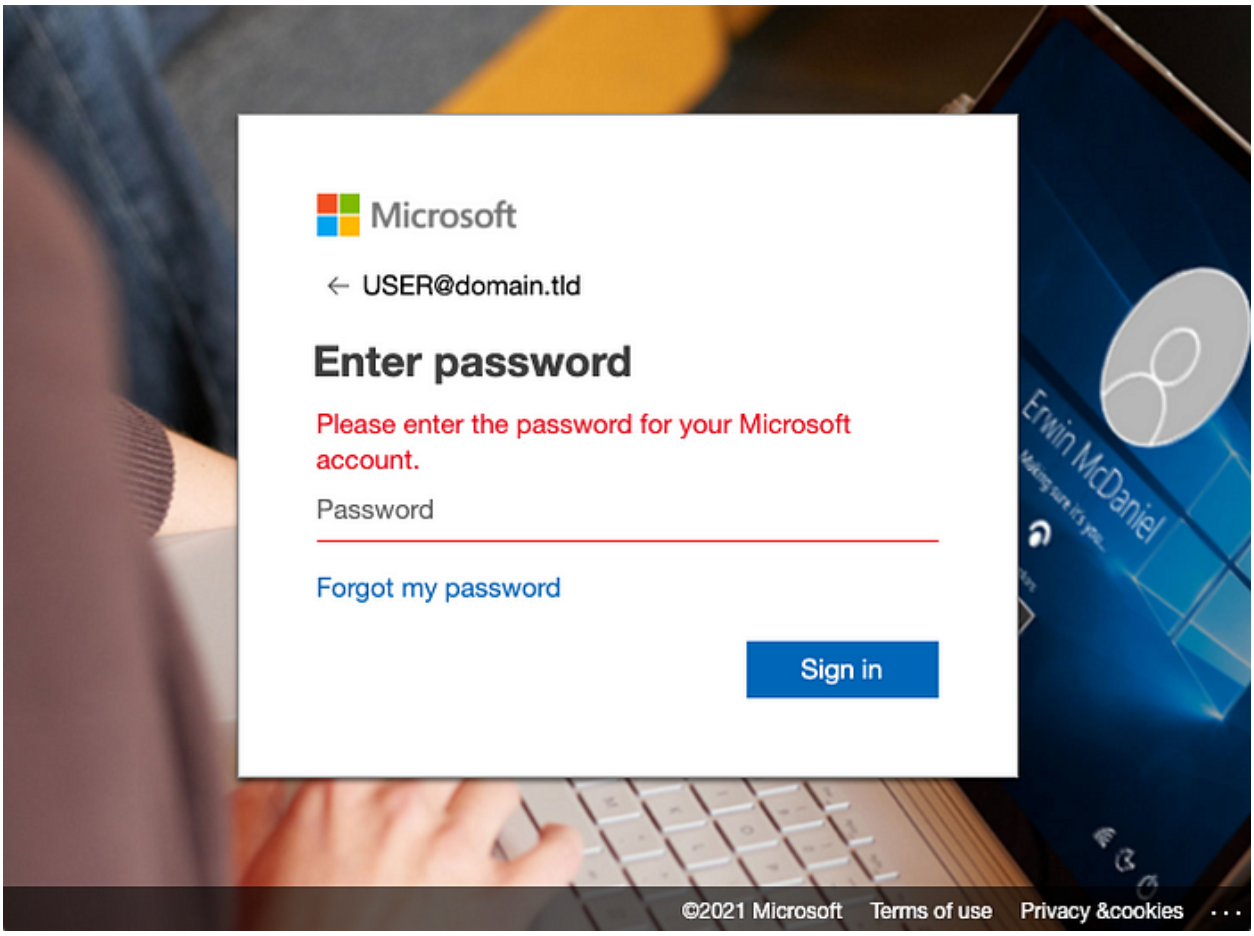
The domains hosting the JavaScript file loader files seem to have been short lived, with different domains being used over the months of the investigation. Each of the observed domains is using Cloudflare to mask the actual server IP address.

However, the IP address we observed performing credential verification serves up the same files as the Cloudflare protected domains. This is a strong indicator that the server hosting the

JavaScript loaded files is the same one doing credential verification. Furthermore, the same JavaScript loader files are still accessible even after the domain name changes, which further indicates that a single server is being used to serve up the loader files, capture credentials and then verify those credentials. Credential capture and verification is discussed later in this article.

The Phishing Page

Opening the attached HTML will display a fake Microsoft 365 login page with company branding. This is a change from older versions of the phishing kit, which did not display branding. The sign-in email address is prefilled and matches the recipient of the phishing email. Branding is based on the domain of the email address and is pulled from Microsoft 365 directly.



Example with Microsoft branding

When the phishing page is loaded, several pieces of information are sent to the PerSwaysion server. This information includes the preset victim's email address, the credential type, and the current time and date. This likely serves as a notification that the phishing page is being actively used. This could be the replacement notification system used instead of the email notification mentioned in the SeclarityIO article. In that article, SeclarityIO observed that previous versions of the phishing kit sent notification emails to addresses controlled by this threat actor. Capturing these emails gave security researchers a better understanding of the infrastructure used by this

threat actor. In the latest kit, the direct email notification has been effectively removed by leaving the email field blank.

When a victim enters their credentials, both their email address and password are sent via a POST command to **hXXps://iost.kogodemcnd[.]com/re/[Base 64 Like Text]**, with other observed variants sending data to **hXXps://riki.kogodemcnd[.]com/re/[Base 64 Like Text]**. The Base64-looking text at the end of the URL is hard-coded into one of the phishing JavaScript files, as mentioned above.

The victim's credentials are then validated from **52.156.67[.]141** in real time. This IP corresponds to a server running Ubuntu Linux hosted on Microsoft Azure in the US-West Region. Credential verification has been observed from this IP address since 2021–09–20.

The credential collector domain is using a Cloudflare reverse proxy, with the actual server IP being masked. However, if we try to access the same file path used to POST data on the credential collector domain to the IP we observe verifying credentials, we get the same response. This indicates that **52.156.67[.]141** is the actual credential collection server behind the Cloudflare proxy. As mentioned above, this is the same server hosting the initial JavaScript loader file linked from the HTML attachment.

Victimology

The Group-IB researchers noted that previous campaigns targeted management and executives. In various campaigns taking place in 2021, we observed targeting of senior employees and accounts associated with those employees, such as support staff. We also observed targeting of employees working in human resources and financial departments in the latest campaigns.

In Group-IB's report, they suspected that victims were obtained from browsing or scraping LinkedIn. Of the several hundred victims observed in campaigns this year, 82% had LinkedIn accounts. So while LinkedIn may have been a source in the past, it's clearly not the only source used by this threat actor.

Prevention

As with many types of phishing, obfuscation techniques are very prevalent, more so when HTML attachments are used. If your mail filter allows blocking on regular expression, consider blocking attachments that contain a document write function and a Base 64 encoded string. Here is an example of a regular expression that will match this pattern:
document\.write\s*\(\s*atob\s*\(\s*[\"\']\[a-zA-Z0–9\+\/\=]+[\"\']\s*\)\s*\)

Another suggestion is to block email from domains that have been registered within the last 30 days. This can be a built-in function or can be achieved by creating a block list of newly registered domains.

Conclusion

Phishing and detection is an ever-changing landscape, where threat actors continually change and hone their techniques. Most changes are incremental, allowing threat researchers to attribute new campaigns to known threat actors. By documenting these changes, security professionals can better understand how techniques change over time and use this understanding to better defend their systems and users.

With the newest PerSwaysion campaign, we can see this threat actor using organizational branding to make their phishing pages look more legitimate, as well as using custom sender domains that bypass email sender protections. This increases the likelihood of phishing emails landing in victim mailboxes. This threat actor has also learned from past mistakes by tightening up their operational security and using a new notification system that does not expose their email addresses.

It's likely that future iterations of PerSwaysion will use yet more improved tactics and techniques, making it beneficial for security professionals to keep track of these campaigns and the threat actor behind them.

Indicators

hXXps://valdia.quatiappcn[.]pw/[hex digits].js — JavaScript Loader
hXXps://kifot.wancdnapp[.]page/[hex digits].js — JavaScript Loader
rikapcndmmooz.firebaseapp.com — PhishKit File Hosting
hXXps://iost.kogodemcnd[.]com/re/[base64 text] — Credential Collector
hXXps://riki.kogodemcnd[.]com/re/[base64 text] — Credential Collector
52.156.67[.]141 — Credential Verification
gemlacksresults[.]net — Email Sender Domain
rotarim50[.]com — Email Sender Domain

Additional References

- **https://blog.group-ib.com/perswaysion**
- **https://www.seclarity.io/resources/blog/the-art-of-perswaysion-phishing-kit/**

Tags

- **Cybersecurity**
- **Perswaysion**