GreenSpot APT Targets NetEase 163.com Users with Fake Download Pages & Spoofed Domains

Published: 2025-02-04 · Archived: 2026-04-05 18:33:39 UTC

TABLE OF CONTENTS

Named by Antiy Labs in 2018, the GreenSpot Advanced Persistent Threat (APT) group is believed to operate from Taiwan and has been active since at least 2007. Known for data theft operations, the group targets government, academic, and military-related entities primarily in China through phishing campaigns.

163.com, a free email service operated by NetEase-one of China's largest IT companies-has become a frequent target for GreenSpot, with the primary objective of stealing login credentials.

Hunt.io researchers observed domains registered within hours of each other, designed to mimic legitimate 163.com services. One such domain hosts a malicious login page, while further analysis of similar domains revealed fake download pages aimed at capturing usernames and passwords. **Patterns in hosting providers, the impersonation of NetEase services, and domain naming conventions-combined with overlaps in public reporting-strongly suggest that this phishing infrastructure is linked to the group**.

Although this recent campaign is confined to a specific region, it reminds us that even free email services can be targeted by advanced threat actors.

Infrastructure Analysis

Our research began with two domains registered within hours of each other via the reseller SugarHosts. Acquiring domains through a reseller minimizes the risk of direct interaction with major registrars, thereby reducing links back to the group. These domains serve as part of the threat actor's malicious infrastructure, both resolving to 139.162.62[.]21 :

- mail[.]ll63[.]net (using the letter "L")
- mail.eco163[.]com

```
Domain Name: ECO163.COM
Registry Domain ID: 2941934076_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2025-01-01T13:25:10Z
Creation Date: 2024-12-13T05:35:53Z
Registrar Registration Expiration Date: 2025-12-13T05:35:53Z
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68949396850
Reseller: SugarHosts https://www.sugarhosts.com
Domain Status: clientTransferProhibited - http://www.icann.org/
epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Taiwan
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: TW
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact via https://www.1api.net/send-message/eco163.com/registrant
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
```

Figure 1: Screenshot of Whois results for eco163[.]com

```
Domain Name: LL63.NET
Registry Domain ID: 2941940395_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2025-01-01T13:25:11Z
Creation Date: 2024-12-13T07:02:53Z
Registrar Registration Expiration Date: 2025-12-13T07:02:53Z
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68949396850
Reseller: SugarHosts https://www.sugarhosts.com
Domain Status: clientTransferProhibited - http://www.icann.org/
epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Taiwan
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: TW
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact via https://www.1api.net/send-message/ll63.net/registrant
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
```

Figure 2: Whois results for ll63[.]net

Querying the IP in Hunt shows the server is hosted on the Akamai Connected Cloud network in Singapore, with ports 22 and 80 open. Of note, port 80 responds with a non-standard HTTP status code of **588**. While this code is

not recognized by IANA, Alibaba Cloud uses it for "Exceeded_Quota" errors-suggesting either a custom response or proprietary configuration is in use.

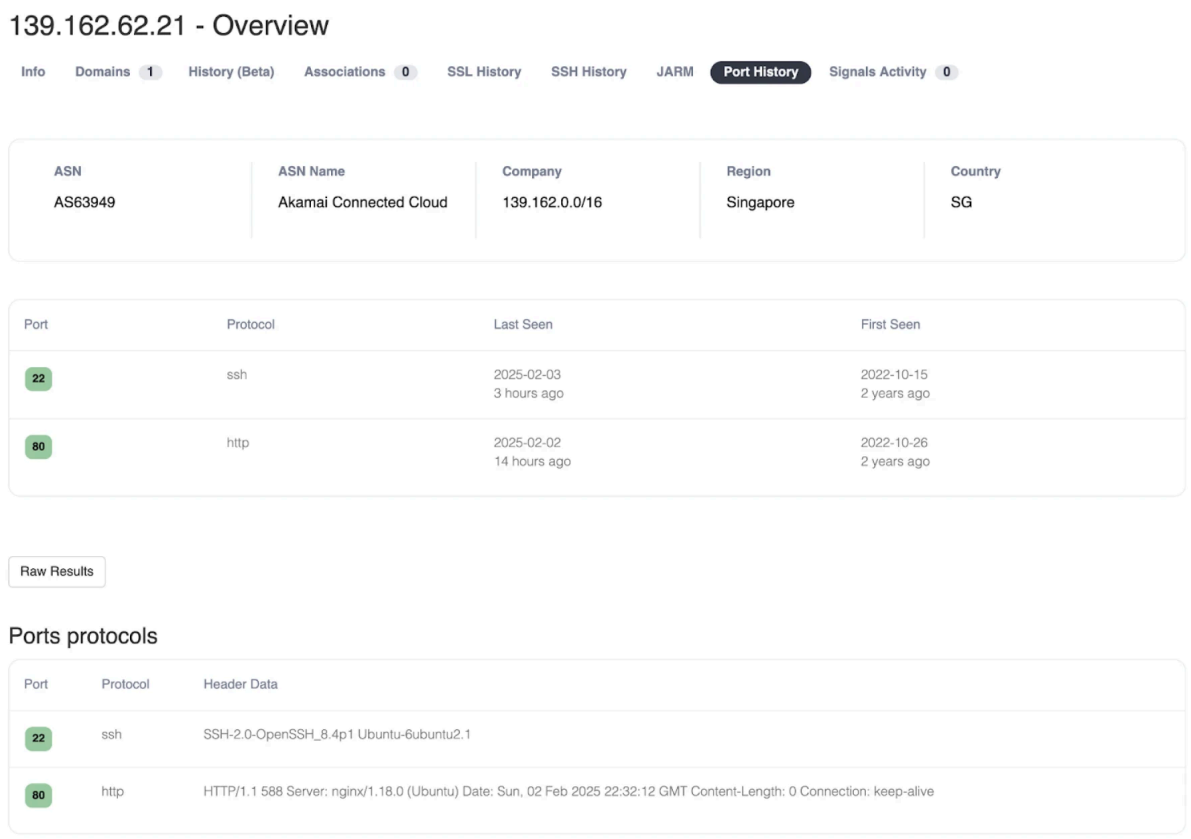

Figure 3: Port history overview for the suspicious IP in Hunt.

The domains are crafted to impersonate the 163.com mail service. While mail[.]ll63[.]net displays a blank web page, mail[.]eco163[.]com presents a login page closely mirroring the legitimate login interface.

Figure 4: Spoofed domain at mail[.]eco163[.]com hosting suspicious login page.

Figure 5: Legitimate login page at mail[.]163[.]com

Upon submitting user credentials, JavaScript code is executed on the 163nailaiba.php page, which dynamically constructs a redirection link based on the URL's domain and displays a 404 page. The script is configured to detect specific domains, including:

- vip[.]163[.]com
- vip[.]126[.]com
- vip[.]188[.]com
- mail[.]yeah[.]net

If one of the above domains is not detected, the user is redirected to the legitimate email login page. Although we have not observed any evidence of credentials being exfiltrated at this time, the script could easily be modified to redirect users to another domain under their control.

Malicious Download Service

Expanding our search for domains using Hunt's "New Hostnames Found on SSL Certs" feed, we identified several suspicious web pages posing as large attachment download services for 163[.]com. These pages-likely distributed via phishing emails-initiate a countdown timer upon visit, pressuring users to enter their credentials to access the document. We found that even after the time expired, the decoy files, none of which are detected as malicious remain available for download.

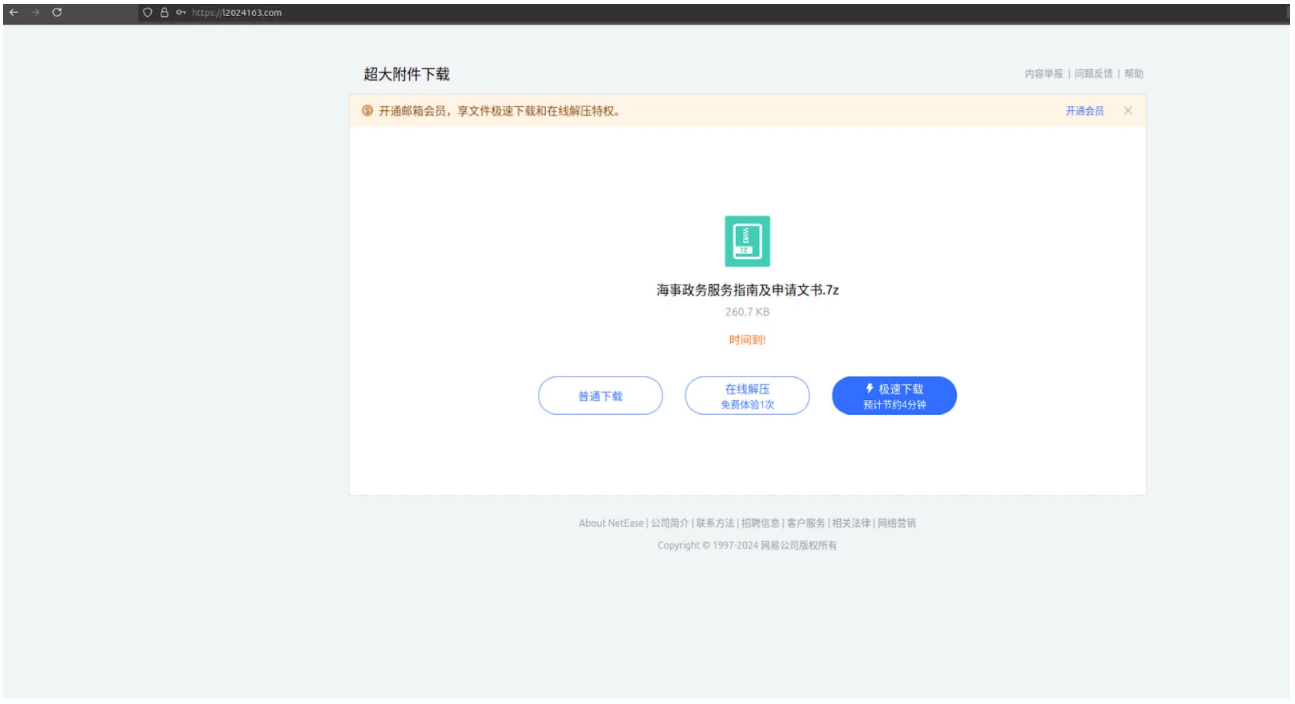

Figure 6: Example "large attachment download" page serving benign files.

The file names, translated from Chinese, include:

- "Guide to Maritime Administrative Services and Application Documents.7z"
- "Highlights of Inspections.docx"
- "Summary of the Situation of Persons Applying for Allocation of Adjusted Apartment Housing.xlsx"

In addition to domains featuring "163" in their names, the hosted page is titled "网易邮箱超大附件下载" (translated as "Download Large Attachments for Netease Mailbox"). **Using this title as part of our search query, we uncovered a small cluster of servers employing a mix of self-signed TLS certificates with the common name "localhost" and Let's Encrypt certificates using the domain as the common name**. It appears that the "localhost" certificates are deployed when servers are inactive, switching to Let's Encrypt during active attack periods.

Potential victims are prompted to enter their 163[.]com username and password to download the file. The first try triggers an error message-likely an attempt to confirm password accuracy. A POST request to login.js is sent on the second attempt, which captures the entered credentials, saving them via a PHP script named "saveData.php." A simple confirmation message, "The data was successfully saved to a file," is displayed upon accessing the script directly.

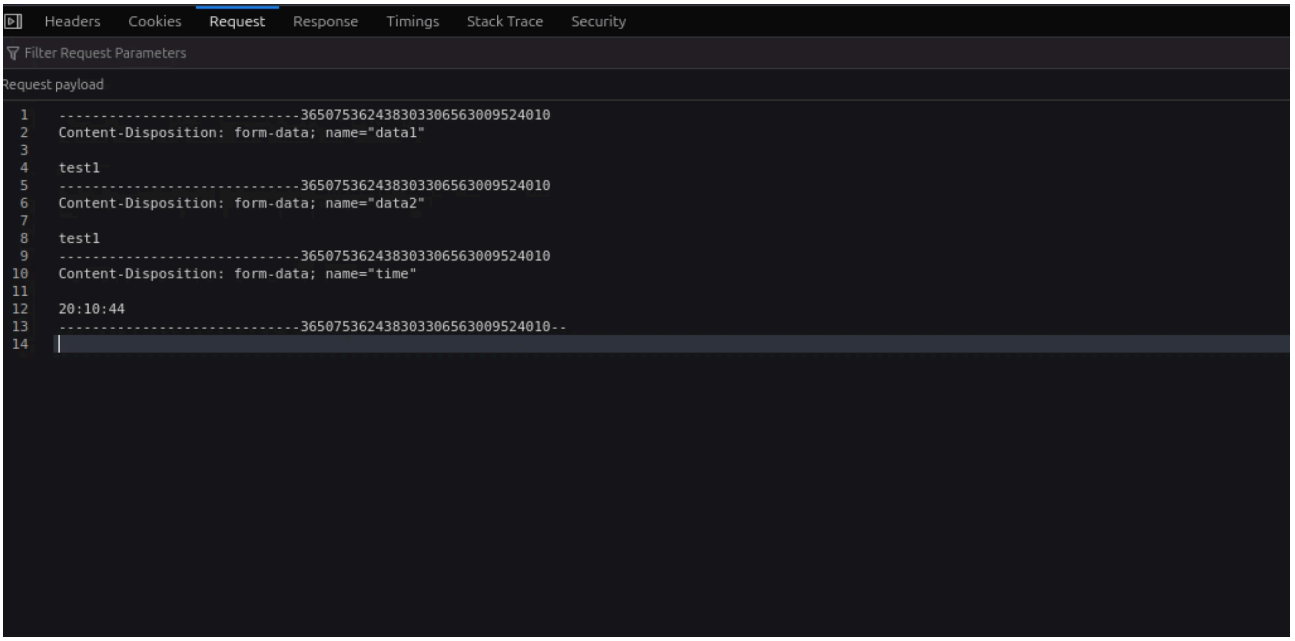

Figure 7: Example of extracted credentials after attempting to access a benign file.

Impact and Relevance

Although this campaign targets 163.com, its implications extend beyond a single service or region. **GreenSpot's techniques-using deceptive domains, manipulated TLS certificates, and counterfeit interfaces-demonstrate a threat actor adept at compromising online platforms**. While free email services are designed for ease of access, they often rely on users to activate enhanced security features like multi-factor authentication. Without these protections, users remain at risk of credential theft, potentially exposing sensitive communications and personal data.

Conclusion

GreenSpot's tactics underscore the sophistication of modern credential theft operations. Our investigation reveals that deceptive domains manipulated TLS certificates, and spoofed login interfaces are used to harvest credentials from 163.com users. Detection efforts should concentrate on identifying irregular domain registrations, certificate anomalies, and unusual HTTP responses.

Organizations and individuals are advised to enable multi-factor authentication, bolster network monitoring, and ensure threat intelligence feeds are current. These proactive measures are essential for mitigating risks from adversaries like GreenSpot.

Network Observables and Indicators of Compromise (IOCs)

IP Address	Domains	Notes
139.162.62[.]21	mail[.]ll63[.]net mail[.]eco163[.]com	Hosted on an open directory at 152.32.138[.]108

IP Address	Domains	Notes
45.76.180[.]253	l2024163[.]com	Malicious download page hosting "Guide to Maritime Administrative Services and Application Documents.7z"
207.148.124[.]130	superset[.]greeninvietnam[.]org[.]vn	Download page hosting "Highlights of Inspections.docx"
198.13.56[.]201	chamber[.]icu	Download page hosting "Summary of the Situation of Persons Applying for Allocation of Adjusted Apartment Housing.xlsx"
