Suspected BITTER APT Continues Targeting Government of China and Chinese Organizations

The Anomali Threat Research Team discovered a phishing site impersonating a login page for the Ministry of Foreign Affairs of the People's Republic of China email service. When visitors attempt to login to the fraudulent page, they are presented with a pop-up verification message asking users to close their windows and continue browsing. Further analysis of the threat actor's infrastructure uncovered a broader phishing campaign targeting other government sites and state-owned enterprises in China. One of the domains uncovered during the investigation was identified by the Chinese security vendor "CERT 360" as being part of the "BITTER APT" campaign in May 2019. Anomali has identified further attempts by the actor to target the government. Based on the Let's Encrypt certificate issuance date, we believe this campaign to be active from May 2019. We expect to see BITTER APT continuing to target the government of China by employing spoofed login pages designed to steal user credentials and obtain access to privileged account information.

Initial Discovery

Anomali researchers identified a website designed to look like the Ministry of Foreign Affairs email login page. Further investigation revealed approximately 40 additional sites, all of which appear to be targeting the government of China and other organisations in China. All of the sites use Domain Validation (DV) certificates issued by "Let's Encrypt". The subdomains appear to have similar naming conventions, primarily targeting online mail logins and containing a verification or account validation theme.

Phishing Site Details

The screenshot below is the initial site that was discovered and investigated. The sites hosted on the domain "btappclientsvc[.]net" was registered on May 30, 2019.

Figure 1 - Phishing site targeting Ministry of Foreign Affairs

The phishing site has been designed specifically to pose as the login page for the Ministry of Foreign Affairs (mail.mfa.gov.cn), it is possible the original page was cloned. Similar to the sites below, and in line with the subdomains identified in this campaign. The phishing sites appear to be designed to steal the Ministry of Foreign Affairs (MFA) email credentials. Once users input their credentials they are greeted with the message in Figure 2.

Figure 2 - Message after user/victim logs into the site

Figure 3 - Phishing site targeting the China National Aero-Technology Import & Export Corporation (CATIC)

Figure 3 shows the spoof site designed to look like the China National Aero-Technology Import and Export Corporation (CATIC). This organisation is a state-owned organisation that deals with aviation products and supports the military and commercial industries.

Figure 4 - Phishing site targeting the National Development and Reform Commission (NDRC)

The National Development and Reform Commission's (NDRC) primary objective is to formulate and implement strategies of national economic and social development.

Figure 5 - Phishing site targeting the Ministry of Commerce of the People's Republic of China (MOFCOM)

The phishing site, displayed in figure 5, is being distributed through the use of URL shortener "TinyURL". The URL "tinyurl[.]com/y4nvpj56" redirects to the URL webmail.mofcom.gov.cn.accountverify.validation8u2904.jsbchkufd546.nxjkgdgfhh345s.fghese4.ncdjkbfkjh244e.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd75894t5.njfg87543.k
The Ministry of Commerce of the People's Republic of China is responsible for cabinet-level policies on foreign trade. This includes import and export decisions, market competition, and trade negotiations.

Threat Infrastructure Analysis

During our analysis, we identified six domains and over 40 subdomains impersonating the following:

- Four People's Republic of China (PRC) government agencies
- Six state-owned enterprises
- One Hong Kong-based auction house
- Two email service providers (NetEase Inc. and Gmail)

Of note, each subdomain impersonation contains a similar naming structure, which could be indicative of the same threat actor or group involved in this latest phishing campaign. The following highlights the naming similarities:

- A random sequence of letters and numbers
- Ending with the malicious domain name
- One or two additional "l" characters added to the word "mail" e.g. "maill" or "mailll"
- The use of the target's legitimate domain name
- Variations of the words "accountvalidation" and "verify"

The below sections provide further details on each of the malicious domains:

Domain 1 - btappclientsvc[.]net

The domain btappclientsvc[.]net was registered on May 30, 2019 with Registrar Internet Domain Service BS Corp. to a Registrant Organization named IceNetworks Ltd.. Privacy protection service was used for the registration to keep the registrant details private. Based on the Start of Authority (SOA) record, this domain is associated with email address reports@orangewebsite[.]com, which in turn is associated with Icelandic web hosting, VPS and dedicated server provider named OrangeWebsite.

The domain is hosted on Iceland-based IP address 82.221.129[.]17 and assigned to the organization, Advania Island ehf (AS50613).

During the past twelve months this IP was observed hosting phishing websites masquerading as organisations in various sectors including:

- Finance (Barclays, Credit Suisse, Keytrade Bank)
- Payment processing (PayPal)
- Cryptocurrency (Bittrex)

The server hosting the domain btappclientsvc[.]net has a Let's Encrypt-issued SSL/TLS certificate (SN: 308431922980607599428388630560406258271383) installed with a validity period of 90 days from July 30, 2019 to October 28, 2019. Based on the certificate's Subject Alternative Name (SAN), there were four distinct subdomains created to impersonate two People's Republic of China (PRC) government agencies and one state-owned defense company:

- China National Aero-Technology Import & Export Corporation (CATIC), a defense industry state-owned enterprise
- Ministry of Foreign Affairs of the People's Republic of China (MFA)
- The National Development and Reform Commission, People's Republic of China (NDRC), a macroeconomic management agency under the State Council

The figure below represents the fraudulent subdomains created to impersonate the PRC organizations and leveraged to mount a phishing campaign:

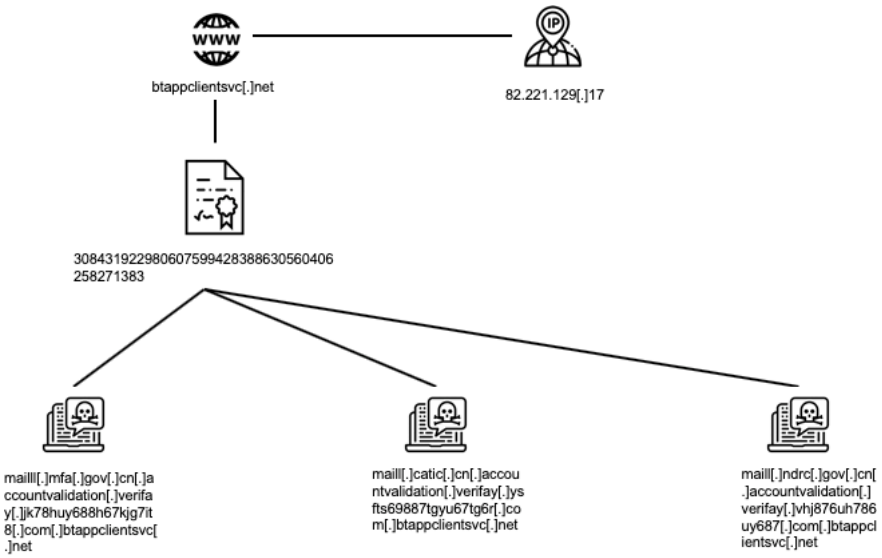

Figure 6 - The three main targets for the domain created May 30th 2019 (CATIC, MFA & NDRC)

Domain 2 - v3solutions4all[.]com

Similar to the first domain, v3solutions4all[.]com was also registered with Registrar Internet Domain Service BS Corp. on December 28, 2018 and is associated with Registrant Organization Icenetworks Ltd. Again, the SOA record reveals the use of the same Icelandic web hosting provider OrangeWebsite and email address reports@orangewebsite[.]com.

The domain v3solutions4all[.]com resolves to Iceland-based IP address 82.221.129[.]19 (AS50613 - Advania Island ehf). This domain and IP address has been previously associated with the BITTER APT and targeting government agencies in China with phishing attacks, based on reporting from 360-CERT.

The server hosting the domain v3solutions4all[.]com has installed a Let's Encrypt-issued SSL/TLS certificate (SN: 284039852848324733535582218696705431782795) with a validity period of 90 days from April 29, 2019 to July 28, 2019. Based on the certificate's Subject Alternative Name (SAN), there were nine distinct subdomains created to impersonate one PRC government agency and two state-owned defense companies:

- Ministry of Foreign Affairs of the People's Republic of China (MFA)
- China National Aero-Technology Import & Export Corporation (CATIC)
- China National Electronics Import & Export Corporation (CEIEC), a state-owned enterprise, directed by the Central Government of China to implement international cooperation in critical areas of national security and economic development

The below represents the fraudulent subdomains created to impersonate PRC organizations and leveraged to mount a phishing campaign:

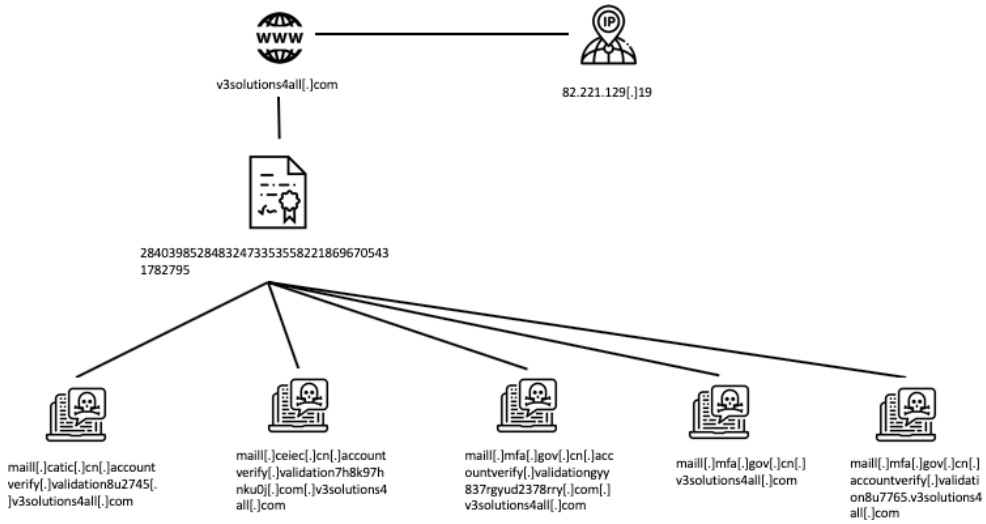

Figure 7 - The three main targets for the domain created December 28th 2018 (CATIC, CEIEC and MFA)

Domain 3 - winmanagerservice[.]org

The domain winmanagerservice[.]org was registered on February 20, 2019 with Registrar OnlineNIC Inc. and is associated with Registrant Organization International Widespread Services Limited. The domain name is likely a reference to Windows Service Manager, which is a single point of administration for managing various aspects of Windows service; however, it is unclear as to the significance behind the chosen name.

The domain is hosted on 94.156.175[.]61 (AS206776 - Histate Global Corp.), located in Sofia, Bulgaria, and is also the host for 105 suspicious-looking domains. Based on the domain's SOA record, it was associated with Gmail account techslogonserver{at}gmail[.]com from February 22, 2019 to May 13, 2019. This email is associated with one registrar from 2016 who has an address in India (see Appendix A). The domain's name server (NS) record identified it is assigned to name servers dns11.warez-host.com and dns12.warez-host.com, which are also servers used for suspicious and malicious sites.

The server hosting the domain winmanagerservice[.]org has installed a Let's Encrypt-issued SSL/TLS certificate (SN: 262081132907426754038710300383315550862850) with a validity period of 90 days from April 23, 2019 to July 22, 2019. Based on the certificate's Subject Alternative Name (SAN), there were nine distinct subdomains created to impersonate five unique PRC organizations:

- Ministry of Foreign Affairs of the People's Republic of China (MFA)
- China National Aero-Technology Import & Export Corporation (CATIC)
- NetEase services: 126.com and 163.com
- Poly Auction Hong Kong Ltd., an auction house located in Hong Kong

The below graphic represents the fraudulent subdomains and leveraged to mount a phishing campaign:

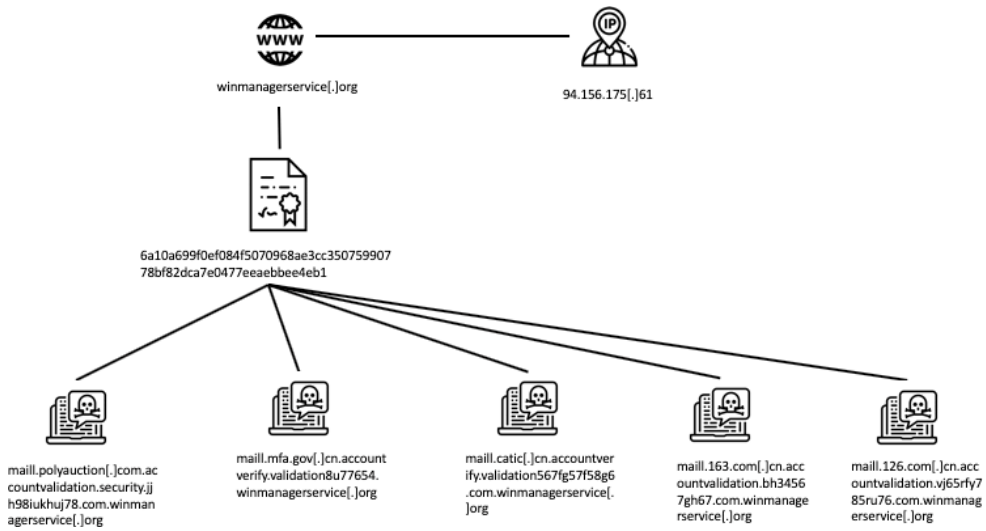

Figure 8. The main targets for domain created February 20th 2019 (Polyauction house, MFA, CATIC, 163 and 126)

Domain 4 - winmanagerservice[.]net

The domain winmanagerservice[.]net was registered on November 20, 2018 with Registrar NetEarth One Inc. using GDPR masking to conceal the registrant's information. At the time of this report, the domain did not resolve to an IP address, however, it is assigned to two name servers: ns1.bitcoin-dns[.]com and ns2.bitcoin-dns[.]com. This server also functions as the name servers for a variety of malicious activities such as phishing, malware hosting and distribution, and carding shops. An interesting subdomain created by the threat actor or group impersonates the State-owned Assets Supervision and Administration Commission of the State Council (SASAC):

maill[.]sasac[.]gov[.]cn[.]accountverify.validation8u6453.jsbch876452.nxjkgdg096574.fghe5392.ncdjkbfkj873e65.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd8766532.njfg

At the time of analysis, we were unable to retrieve a SASAC-themed phishing page but did find a historical screenshot taken on November 20, 2018 of an open directory hosted at <hxxp://www[.]winmanagerservice[.]net/> that contained a single CGI-bin folder.


Index of /

Name	Last modified	Size	Description
cgi-bin	20-Nov-2018 11:45	-	

Proudly Served by LiteSpeed Web Server at www.winmanagerservice.net Port 80

Figure 9 - Screenshot of malicious domain winmanagerservice[.]net from 2018

A historical IP address resolution search of winmanagerservice[.]net identified it resolved to United States-based IP address 162.222.215[.]96 (AS54020 - Admo.net LLC) from November 20, 2018 until February 22, 2019. This same search uncovered a historical Sender Policy Framework (SPF) record that specified United States-based IP address 162.222.215[.]2 (AS 8100 QuadraNet Enterprises LLC) as authorized to send email traffic on behalf of winmanagerservice[.]net from December 10, 2018 to February 22, 2019.

Domain 5 - cdaxpropsvc[.]net

The domain cdaxpropsvc[.]net was registered with Registrar OnlineNIC Inc. on March 21, 2019. It is associated with a UAE-based Registrant IWS Ltd of Registrant Organization International Widespread Services Limited using Registrant Email info{at}iws[.]co. A reverse Whois lookup of this registrant email uncovered 122 domains created using this address dating back to June 08, 2014 and as recent as of August 1, 2019.

The domain is hosted on 94.156.175[.]61, located in Sofia, Bulgaria, and is also the host for 105 suspicious-looking domains. Based on the domain's SOA record, it is associated with Gmail account techslogonserver{at}gmail[.]com since March 22, 2019 and assigned to name servers dns11.warez-host.com and dns12.warez-host.com.

According to historical SSL/TLS certificates for the server hosting the domain cdaxpropsvc[.]net, we found 12 subdomain impersonations targeting four defense sector state-owned enterprises and free email service providers, NetEase and Gmail. At the time of analysis, the subdomains did not host a website; however, based on the threat actor or group's targeting patterns, it is highly likely that they were created to host faux login phishing pages designed to steal user's credentials.

- China National Aero-Technology Import & Export Corporation (CATIC)
- China Great Wall Industry Corporation (CGWIC), the sole commercial organization authorized by the government of China to provide commercial launch services, satellite systems and to carry out space technology cooperation
- China National Nuclear Corporation (CNNC), a state-owned enterprise that generates and distributes nuclear power products and operates nuclear environmental engineering construction, nuclear military development, and other businesses
- China Zhongyuan Engineering Corp (CZEC), a contractor and contracting international and domestic projects

- NetEase, Inc. service 163.com
- Gmail

The below represents the fraudulent subdomains created to impersonate these organizations and leveraged to mount a phishing campaign:

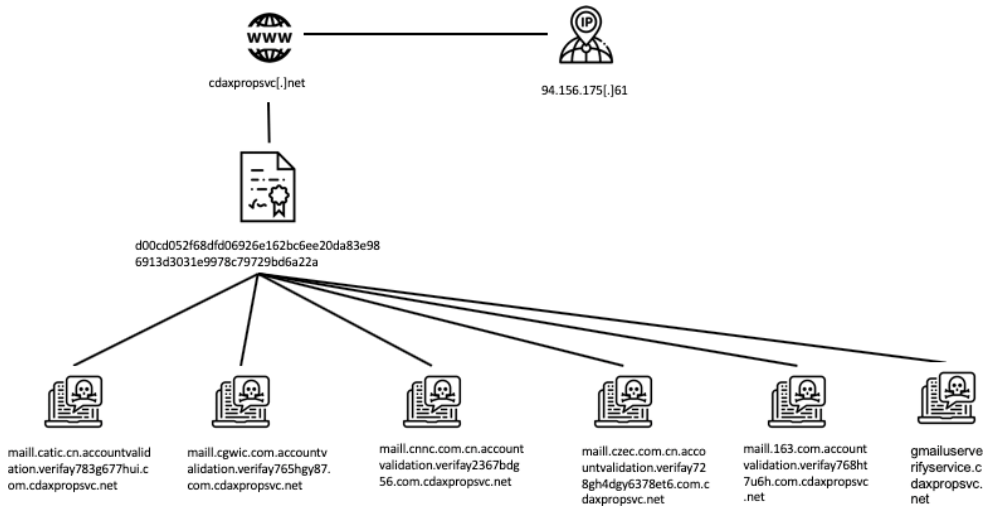

Figure 10 - The main targets for domain created March 21st 2019 (CATIC, CGWIC, CNNC, CZEC, 163 and Gmail)

Domain 6 - wangluojiumingjingli[.]org

When investigating the IP address 82.221.129[.]18 and the domain wangluojiumingjingli[.]org, we found 2 subdomain impersonations targeting government organisations in China: The Ministry of Commerce of the People's Republic of China (MOFCOM) and the Aviation Industry Corporation of China (AVIC). At the time of analysis, the aviation subdomain did not host a website; however, based on the threat actor or group's targeting patterns, it is highly likely that they were created to host faux login phishing pages designed to steal user's credentials.There was a screenshot of the spoof site targeting the Ministry of Commerce showing a faux email login page.

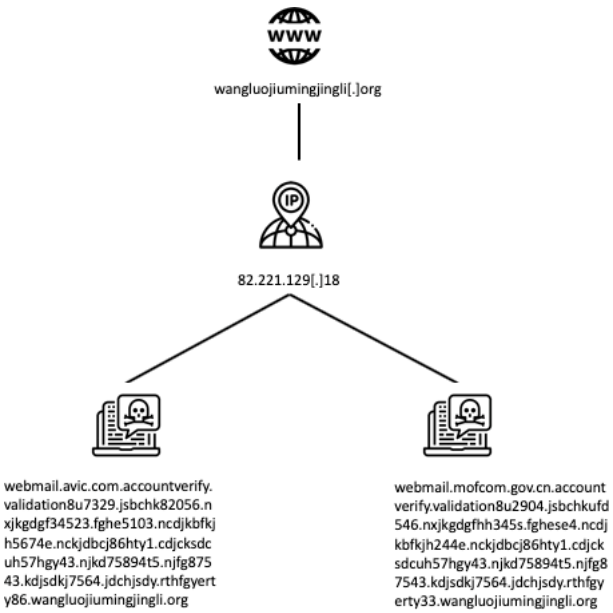

Figure 11 - The main targets for domain created April 2019 (MOFCOM and AVIC)

Three of the domains were hosted on the same hosting provider; orangewebsite.com. This hosting provider is based in Iceland and has particularly strong protocols for digital privacy and little to no internet censorship. The hosting provider also accepts Bitcoins as a payment method, which is likely to be the reason it is attractive to use for malicious purposes.

Summary

As part of its ongoing research initiatives, the Anomali Threat Research Team has discovered a new phishing attack leveraging spoof sites that seem to be designed to steal email credentials from the target victims within the government of the People's Republic of China. By stealing email credentials, and accessing internal email content, it would be possible to gain insight into what decisions are being made within the target organisation and could lead to the theft of sensitive information. Although it is difficult to pinpoint the exact motivation of the attacker, it is highly likely this campaign is to pursue some form of espionage. The victims of these campaigns are the members of staff for the organisations being targeted. Most of the organisations being phished in these campaigns relate to economic trade, defence, aviation and foreign relations. This suggests that the attackers are likely to be an actor or group operating under a mandate to understand what China's goals and decisions are likely to be internationally. "CERT 360" has reported on related indicators being attributed to BITTER APT; a South Asian country (suspected Indian APT in open source reporting). BITTER APT campaigns are primarily targeting China, Pakistan and Saudi Arabia historically.

References

- 360CERT. (24 May 2019). Suspected BITTER organization's recent analysis of targeted attacks against China and Pakistan. Retrieved on 02 August 2019
- Censys.io. (31 July 2019). TLS Certificate for btappclientsvc[.]net. Retrieved on 02 August 2019
- Censys.io. (29 April 2019). TLS Certificate for v3solutions4all[.]com. Retrieved on 02 August 2019
- Censys.io. (23 April 2019). TLS Certificate for winmanagerservice[.]org. Retrieved on 02 August 2019
- Censys.io. (22 July 2019). TLS Certificate for cdaxpropsvc[.]net. Retrieved on 02 August 2019
- Censys.io. (22 May 2019). TLS Certificate for cdaxpropsvc[.]net. Retrieved on 02 August 2019
- URLScan.io. (31 July 2019). Domain search on btappclientsvc[.]net. Retrieved on 02 August 2019
- URLScan.io. (08 January 2019). Domain search on v3solutions4all[.]com. Retrieved on 02 August 2019
- URLScan.io. (23 April 2019). Domain search on winmanagerservice[.]org. Retrieved on 02 August 2019
- URLScan.io. (12 June 2019). Open directory for www[.]gmailuserverifyservice.cdaxpropsvc[.]net. Retrieved on 02 August 2019

Appendix A – Indicators of Compromise

Indicator of Compromise
82.221.129[.]17
82.221.129[.]18
82.221.129[.]19
94.156.175[.]61
btappclientsvc[.]net
winmanagerservice[.]org
winmanagerservice[.]net
v3solutions4all[.]com
cdaxpropsvc[.]net
wangluojiumingjingli[.]org
mail.btappclientsvc.net
maill.catic.cn.accountvalidation.verifay.ysfts69887tgyu67tg6r.com.btappclientsvc.net
maill.ndrc.gov.cn.accountvalidation.verifay.vhj876uh786uy687.com.btappclientsvc.net
mailll.mfa.gov.cn.accountvalidation.verifay.jk78huy688h67kjg7it8.com.btappclientsvc.net
mail.v3solutions4all.com
maill.catic.cn.accountverify.validation8u2745.v3solutions4all.com
maill.ceiec.cn.accountverify.validation7h8k97hnku0j.com.v3solutions4all.com
maill.mfa.gov.cn.accountverify.validationgyy837rgyud2378rry.com.v3solutions4all.com
mail.winmanagerservice.org
maill.126.com.cn.accountvalidation.vj65rfy785ru76.com.winmanagerservice.org

maill.163.com.cn.accountvalidation.bh34567gh67.com.winmanagerservice.org

maill.catic.cn.accountverify.validation567fg57f58g6.com.winmanagerservice.org

maill.mfa.gov.cn.accountverify.validation8u77654.winmanagerservice.org

maill.polyauction.com.accountvalidation.security.jjh98iukhuj78.com.winmanagerservice.org

maill.mfa.gov.cn.accountverify.validation8u77654.winmanagerservice[.]org

webmail.avic.com.accountverify.validation8u7329.jsbchk82056.nxjkgdgf34523.fghe5103.ncdjkbfkjh5674e.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd75894t5.njfg87543.kdjsdkj7564.

webmail.mofcom.gov.cn.accountverify.validation8u2904.jsbchkufd546.nxjkgdgfhh345s.fghese4.ncdjkbfkjh244e.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd75894t5.njfg87543.kdjsdkj
ingjingli.org

maill.sasac.gov.cn.accountverify.validation8u6453.jsbch876452.nxjkgdg096574.fghe5392.ncdjkbfkj873e65.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd8766532.njfg73452.kdjsdkj756

maill.catic.cn.accountvalidation.verifay783g677hui.com.cdaxpropsvc.net

maill.cgwic.com.accountvalidation.verifay765hgy87.com.cdaxpropsvc.net

maill.cnnc.com.cn.accountvalidation.verifay2367bdg56.com.cdaxpropsvc.net

maill.czec.com.cn.accountvalidation.verifay728gh4dgy6378et6.com.cdaxpropsvc.net

maill.163.com.accountvalidation.verifay768ht7u6h.com.cdaxpropsvc.net

325ece940de9fb486ef83b680ad00d385b64e435923d1bbc19cbcf33e220c2a2

6a10a699f0ef084f5070968ae3cc35075990778bf82dca7e0477eeaebbee4eb1

5538badac0221b42f457920802b23ebd8ccf2c64b1fb827cd6458a7f9de2c6de

940a1bd16be51cd264ee7e315841b8aa0b0b86d3392d4d08ca00151f01a5cd28

823f85eb6d3465145bb34e570b870e39001c4ec61f7ca325f88a23edee75654f

f456f2a2802242e1404ef9a586366820c4bd7f7f3b113209d56fc34dee2d75bf

7bc4f48a4345f4a47dabbf686a714d3e4c9af9d9f26e73ca873f54a4f164b732

techslogonserver[a]gmail[.]com

About the Author

Anomali Labs