Uncovering Suspicious Download Pages Linked to App Installer Abuse

Table of Contents

Executive Report

Threat actors have been abusing App Installer, a Windows 10 feature that makes installing applications more convenient. The abuse could lead to ransomware distribution and was likely carried out by financially motivated actors Storm-0569, Storm-1113, Sangria Tempest, and Storm-1674. These malicious actors imitated the landing pages of popular software, such as Zoom, Microsoft OneDrive, Microsoft SharePoint, and Microsoft Teams, to lure target victims into downloading malicious installers.

While Microsoft immediately responded by disabling the ms-appinstaller protocol handler by default, WhoisXML API researchers decided to look for traces of the attack in the DNS.

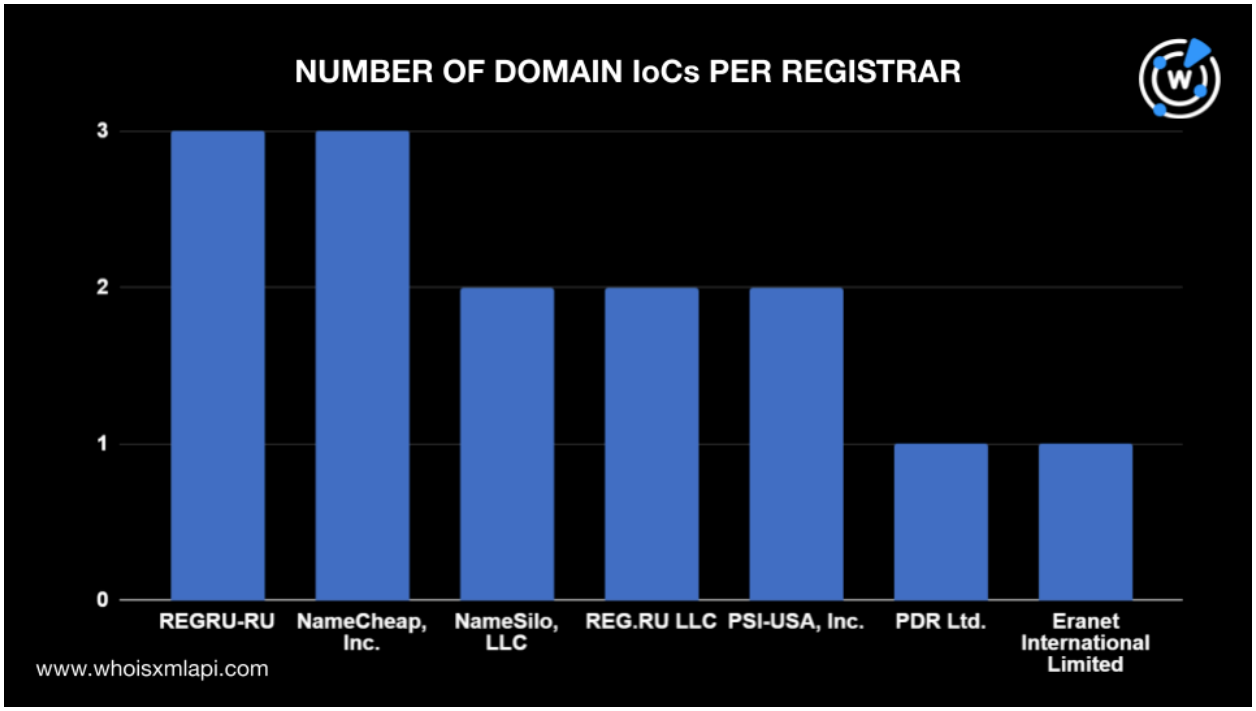
With that in mind, our research team expanded the IoC lists Microsoft published comprising 18 subdomains and 14 domains tagged as IoCs (three of which were extracted from the subdomains). The investigation led to the discovery of:

- Four email-connected domains
- 16 IP addresses
- 127 IP-connected domains
- 401 string-connected domains
- 596 string-connected subdomains

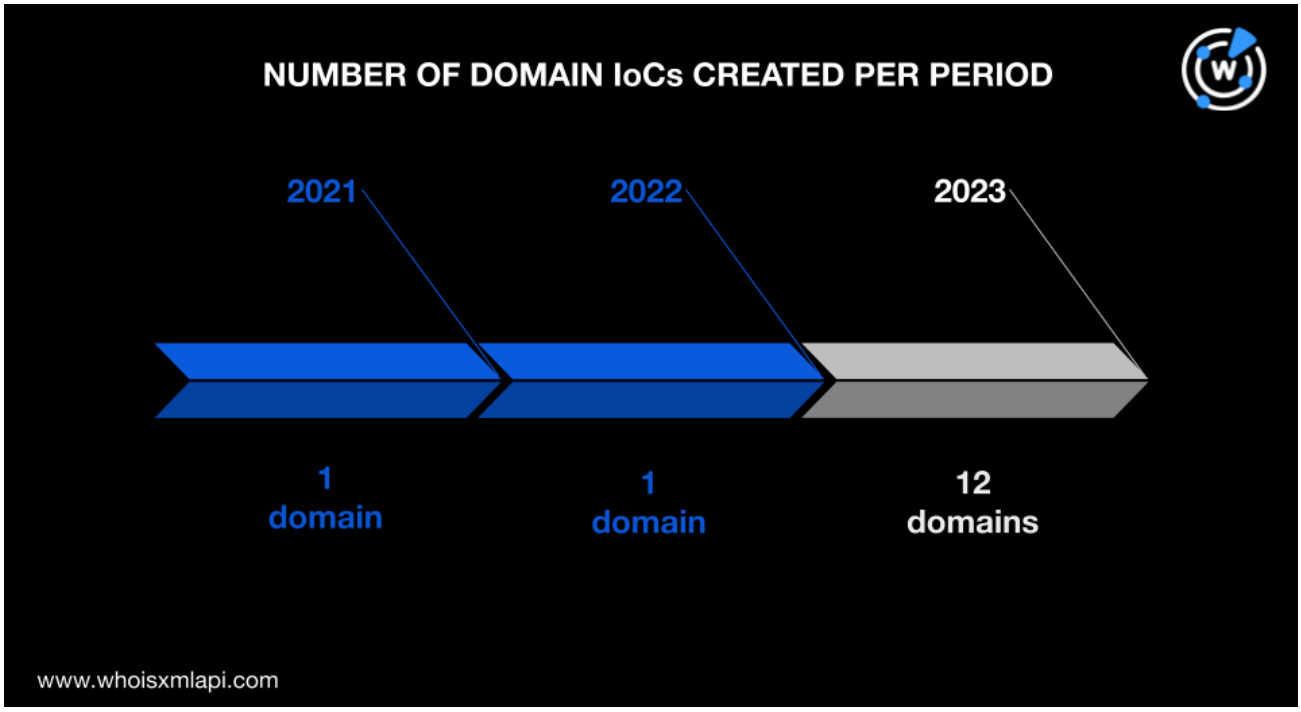
Infrastructure Analysis of the App Installer Abuse IoCs

To begin understanding the attack infrastructure, we did a bulk WHOIS lookup for the 14 domains tagged as IoCs, three of which were extracted from the 18 subdomains found on the IoC lists. Their WHOIS records revealed that:

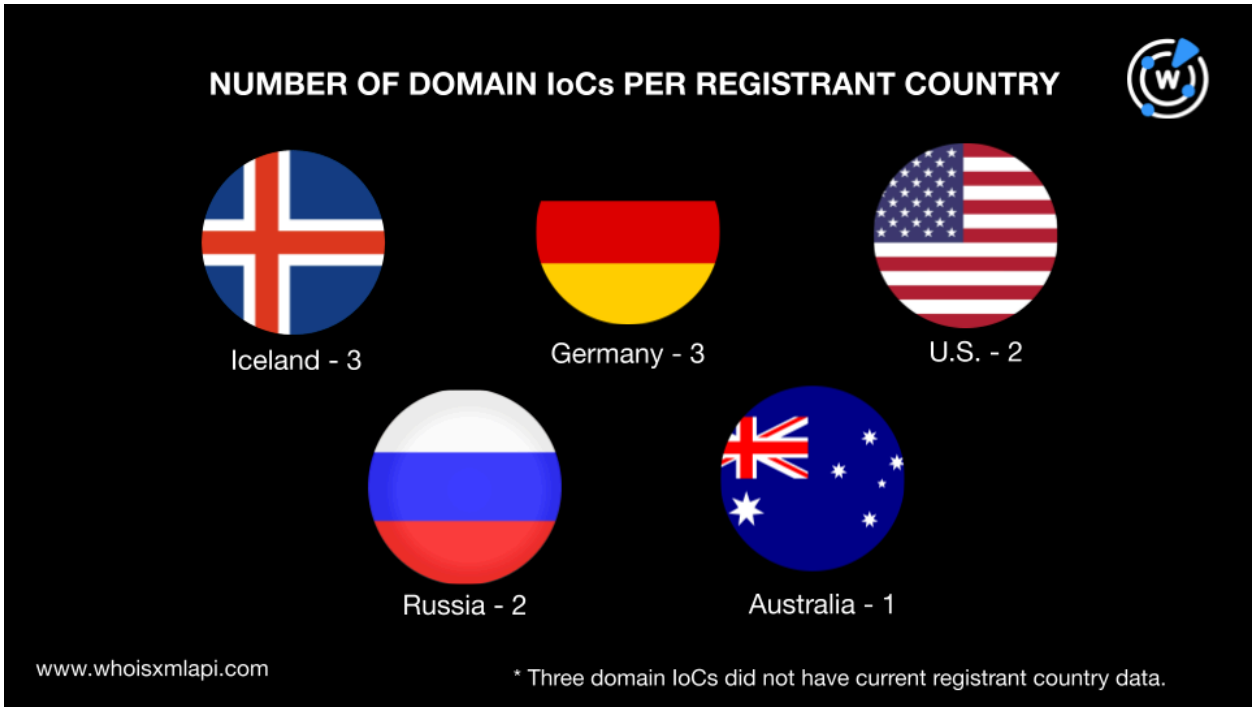
- They were administered by seven different registrars. REGRU-RU and NameCheap, Inc. accounted for three domains each; NameSilo LLC; REG.RU LLC; and PSI-USA, Inc. for two domains each; and PDR Ltd. and Eranet International Limited for one domain each.



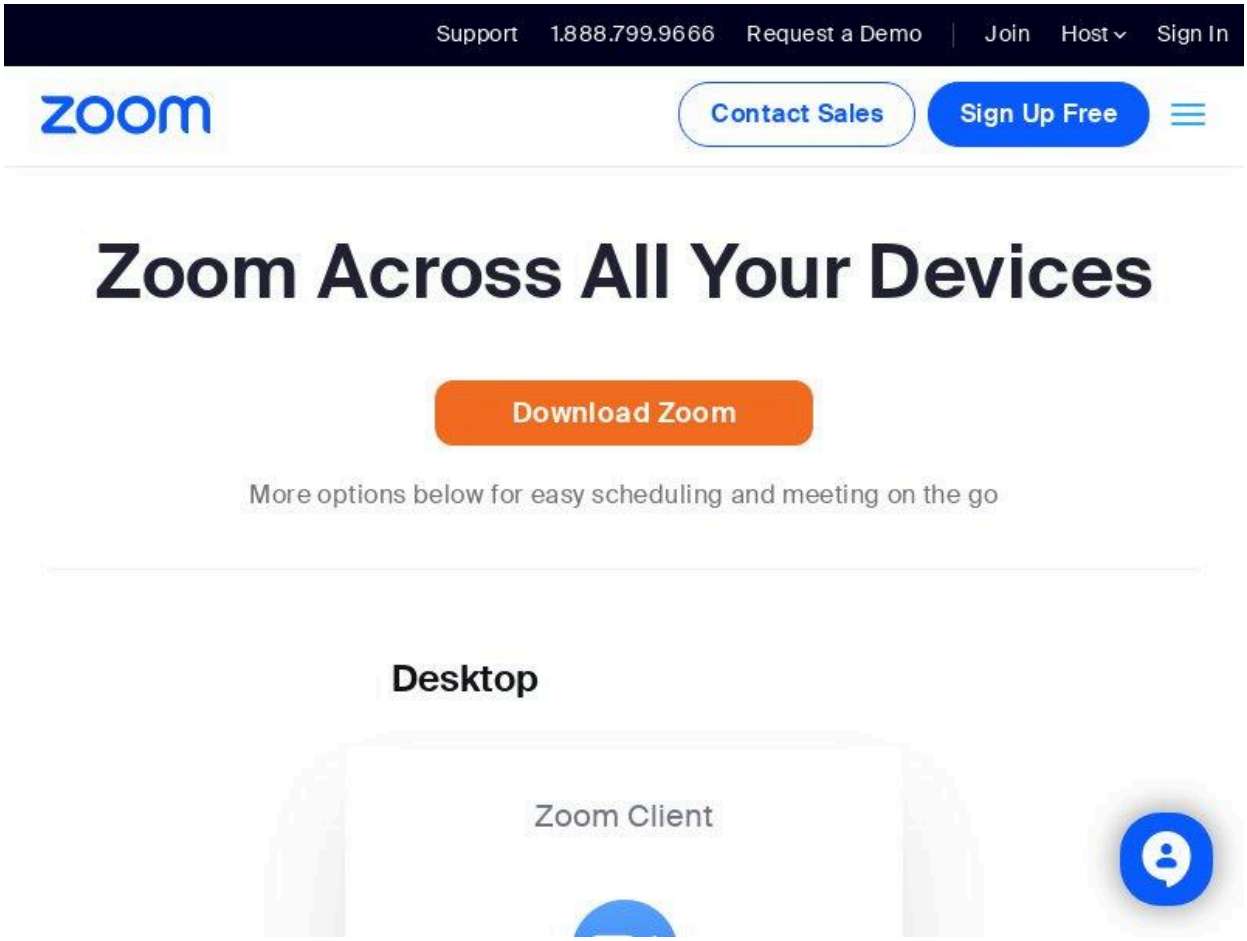
- Most of the domains, 12 to be exact, were created in 2023, while one domain was registered in 2022 and another in 2021.



- Their registrations were spread across five countries. Three domains each were registered in Iceland and Germany, two each in the U.S. and Russia, and one in Australia. Three domains did not have current registrant country data.



We then subjected the domain IoCs to a screenshot analysis. We found that some continued to host live content, including the websites below that show the Zoom and Microsoft landing pages.



Screenshot of the page hosted on domain IoC info-zoomapp[.]com

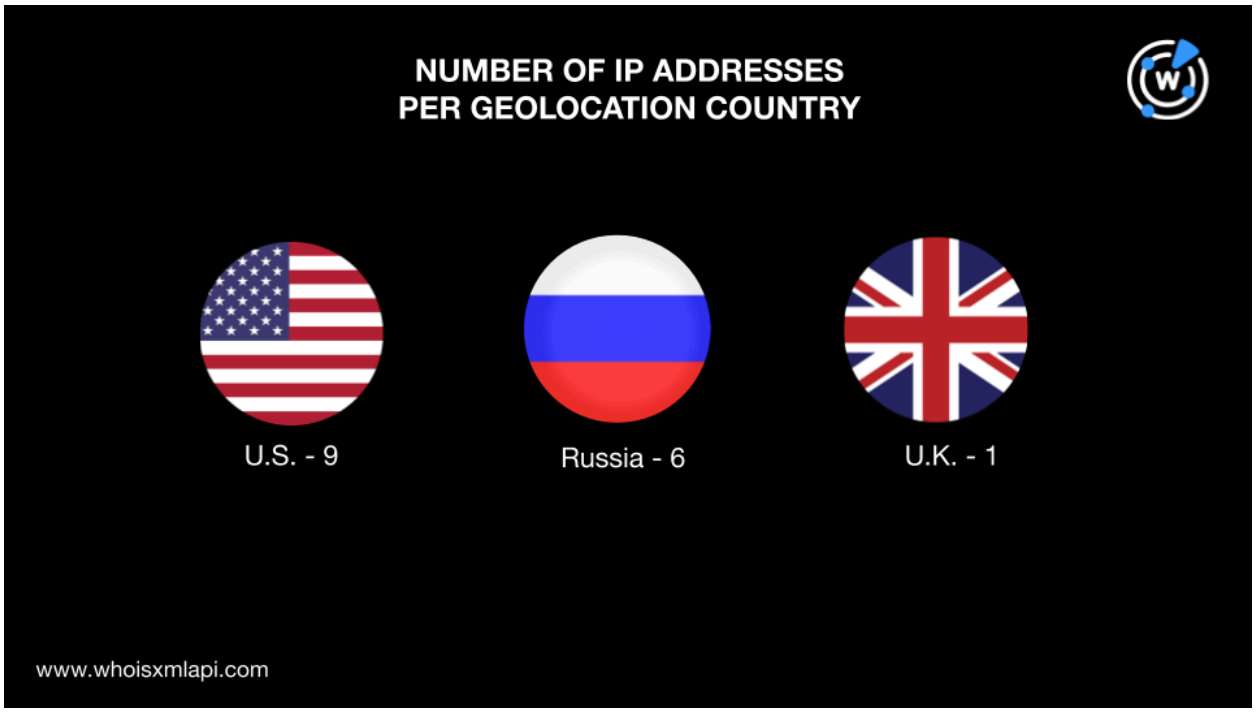
Uncovering DNS Connections Related to the App Installer Abuse IoCs

As our next step, we traced the DNS footprints of the malicious domains and subdomains used in the campaigns.

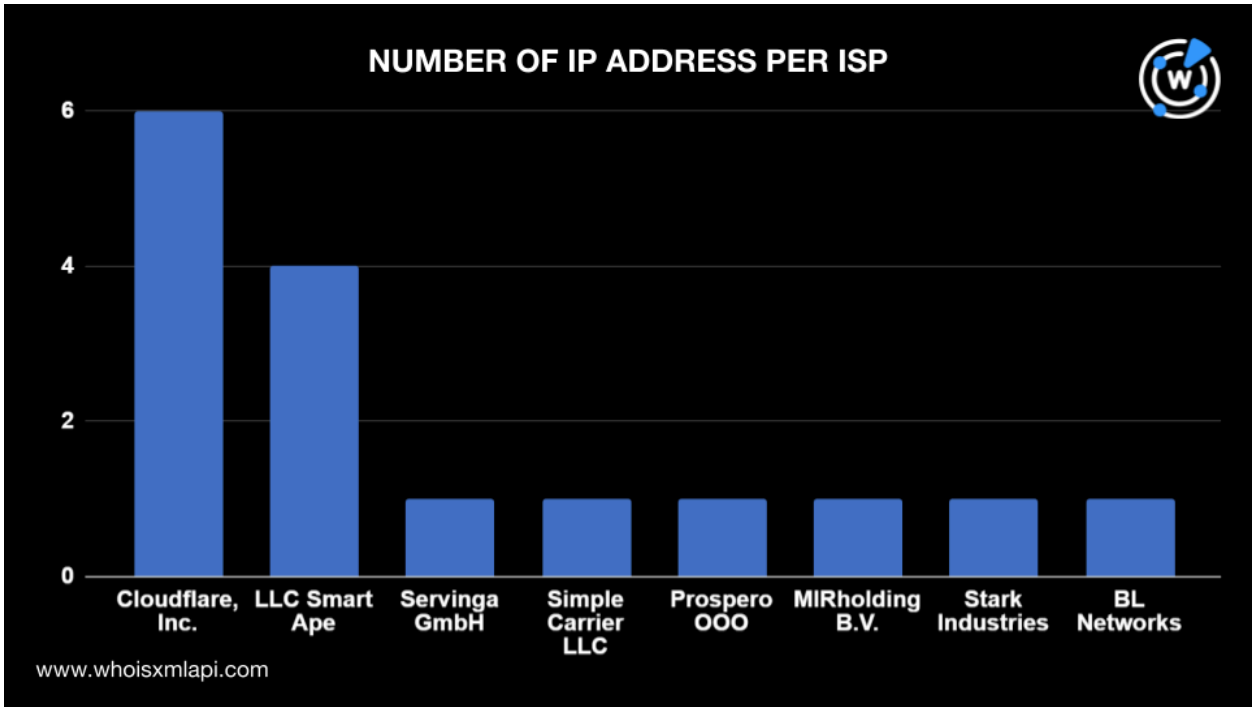
WHOIS History API searches for the domain IoCs led to the discovery of 12 email addresses in their historical WHOIS records, five of which were public. Running these public email addresses on Reverse WHOIS API allowed us to determine that they appeared in the current WHOIS records of 8,434 domains. However, one email address was likely owned by a domainer since it was used to register 8,429 domains. After removing the domains the domainer possibly owns and the IoCs, we were left with four email-connected domains.

We then performed DNS lookups for the IoCs and obtained 16 IP addresses to which the 14 domains and 18 subdomains tagged as IoCs resolved. Subjecting these IP addresses to IP geolocation lookups, we found that:

- They were geolocated in only three countries—nine originated from the U.S., six from Russia, and one from the U.K.



- They were managed by eight ISPs—Cloudflare, Inc. administered six IP addresses; LLC Smart Ape, four; and Serving GmbH, Simple Carrier LLC, Prospero OOO, MIRholding B.V., Stark Industries, and BL Networks, one each.



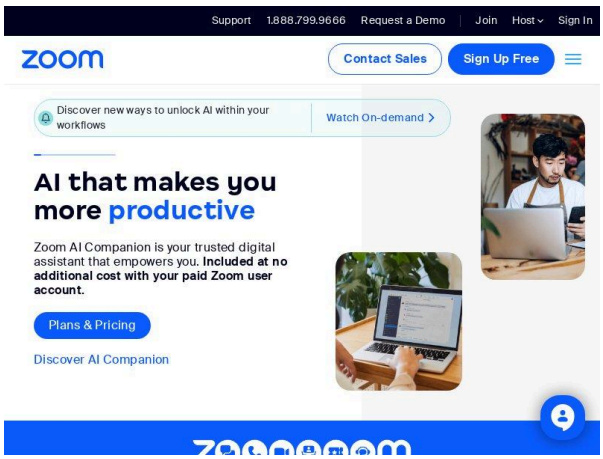
- Threat Intelligence API also revealed that nine of the 16 IP addresses were associated with various threats. A few examples are shown in the table below.

IP ADDRESSES	ASSOCIATED THREAT TYPES
185[.]196[.]8[.]246	Attack Command-and-control (C2) Malware
91[.]215[.]85[.]199	Attack Malware Spam
172[.]67[.]147[.]29	Generic Phishing
172[.]67[.]209[.]46	Generic Malware Phishing

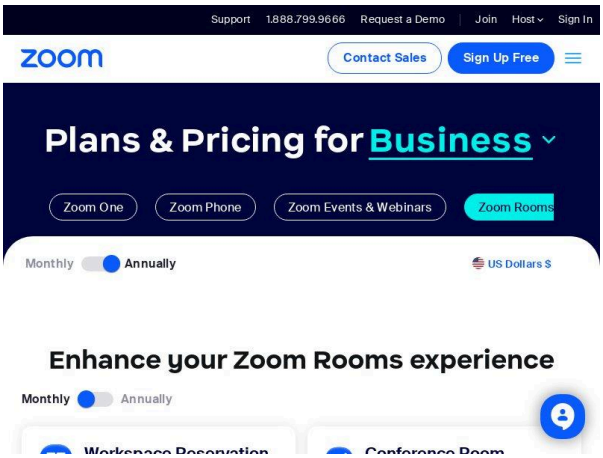
We also subjected the 16 IP addresses to reverse IP lookups, which showed that nine were potentially dedicated. They led to 127 IP-connected domains after removing duplicates, the IoCs, and the email-connected domains.

We also performed a screenshot analysis for the IP-connected domains, which revealed that many hosted installation pages like the malicious resources involved in the App Installer abuse as of this writing.

Screenshot of the page hosted on IP-connected domain bitvarden-info[.]com



Screenshot of the page hosted on IP-connected domain biryaneehouse[.]com



Screenshot of the page hosted on IP-connected domain cotattoo[.]com

Screenshot of the page hosted on IP-connected domain rextowingcarolinas[.]com

Finally, we looked for string-connected domains using Domains & Subdomains Discovery. We used the following search parameters and text strings leading to the discovery of 401 domains.

- Starts with **scheta.**
- Starts with **tnetworks**
- Starts with **1204** and ends with **.ru**
- Starts with **gertefin**
- Starts with **septcn**
- Contains **-zoomapp**

- Starts with **storageplace**
- Starts with **sun1.**
- Starts with **tech-department**
- Starts with **kellyservices-**
- Starts with **ithr.**
- Starts with **meetlng**
- Starts with **webmicrosoft** and contains **system.**

Meanwhile, subdomain searches using the text strings that appeared among the subdomain IoCs unveiled 596 string-connected subdomains for these parameters:

- Starts with **nixonpeabody**
- Starts with **amgreetings**
- Starts with **cbre.**
- Starts with **hubergroup**
- Starts with **formeld**
- Starts with **kelly** and contains **services** and **hr**
- Starts with **mckinsey** and contains **hr**
- Contains **support-my.**
- Starts with **zoonn**
- Starts with **amydeks**
- Starts with **abobe.**
- Starts with **amydesk**

A screenshot analysis for the string-connected resources showed that several hosted suspicious content, including a page that was flagged for phishing as of this writing.

Screenshot of the page hosted on string-connected domain zoonn[.]meetlng[.]cn[.]com

—

We started the investigation with 18 subdomains and 14 domains (three of which were extracted from the subdomains) tagged as IoCs for the App Installer abuse that could potentially lead to ransomware installation. It led us to discover more than 1,100 connected artifacts comprising four email-connected domains, 16 IP addresses, 127 IP-connected domains, 401 string-connected domains, and 596 string-connected subdomains.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Email-Connected Domains

- vmlian[.]top
- foodlian[.]top

Sample IP Addresses

- 188[.]127[.]224[.]193
- 188[.]127[.]254[.]229
- 188[.]127[.]235[.]18
- 91[.]219[.]150[.]24
- 80[.]77[.]23[.]210
- 185[.]196[.]8[.]246
- 91[.]215[.]85[.]199
- 193[.]233[.]22[.]126

Sample IP-Connected Domains

- 500token[.]ru
- 001531[.]com
- 009987[.]com
- edd2ed2[.]online
- tservicessss[.]store
- accesutqymyiq[.]com
- meetlng[.]group
- admiai[.]com
- amjsecurityservices[.]com
- austinsmilecenter[.]com
- australiatvic[.]com
- autodesk-promo[.]com
- belaladel[.]com
- bestrealtorsindallas[.]com
- biblealways[.]com
- bibleandsouls[.]com
- bibleasoul[.]com
- biltwerdem-info[.]com
- birgletrossgolf[.]com
- biryaneehouse[.]com
- bitvarden-info[.]com
- bottletorque[.]com
- bouncebackbabyfat[.]com
- bouncebeast[.]com
- bugglesworth[.]com
- bundles2go[.]com
- buscorestaurante[.]com
- cannothide[.]com
- carepettips[.]com
- carnitasdelivery[.]com
- cartknoxxs[.]com
- challengermenu[.]com
- chicaespectaculos[.]com
- cotattoo[.]com
- creativedesignint[.]com
- cryptofindy[.]com
- crystalgemsfruit[.]com
- csritindia[.]com
- cualoland[.]com
- easyquickdinners[.]com
- enhanceexercise[.]com
- filmandfilmmaking[.]com
- fromge[.]com
- garypearlphotography[.]com
- gdaygym[.]com
- gdaygyms[.]com
- gdayreviews[.]com
- getmailgetpaid[.]com
- globalqualityparts[.]com
- globalwholesaleremanufacturing[.]com

Sample String-Connected Domains

- scheta[.]info
- scheta[.]net
- scheta[.]moscow
- scheta[.]ru
- scheta[.]online
- scheta[.]com
- tnetworkperu[.]com
- tnetwork[.]cn
- tnetworkusa[.]com
- tnetworkmarketing[.]com
- tnetworks[.]com[.]au
- tnetworks[.]com[.]tr
- tnetwork[.]jp
- tnetwork[.]com[.]au
- tnetwork[.]cz
- tnetworkers[.]com
- tnetworkinc[.]com
- tnetworkservices[.]com
- tnetworksindo[.]com
- tnetwork[.]io[.]vn
- tnetwork[.]se
- tnetworkelsalvador[.]vg
- tnetworkdc[.]ws
- tnetworkworld[.]com
- tnetworkgroup[.]com
- tnetworks[.]df[.]gov[.]br
- tnetworksinc[.]com
- tnetwork[.]nl
- tnetworkinginc[.]ca
- tnetwork[.]co[.]kr
- tnetworkbd[.]net
- tnetwork[.]it
- tnetwork[.]co[.]jp
- tnetwork[.]de
- tnetwork[.]in
- tnetworks[.]xyz
- tnetwork[.]ca
- tnetworks[.]eu
- tnetworkyfl[.]top
- tnetworks[.]net
- tnetworkuk[.]info
- tnetworkasia[.]com
- tnetworkcn[.]com
- tnetwork[.]xyz
- tnetwork[.]com
- tnetworkmc[.]com
- tnetworksoftware[.]com
- tnetwork-system[.]online
- tnetworka[.]com
- tnetwork[.]dk

Sample String-Connected Subdomains

- nixonpeabody[.]careers[.]micronapps[.]com
- nixonpeabody-website[.]cmservicesltd[.]com
- nixonpeabody[.]vps[.]powersharkmbr[.]com
- nixonpeabody[.]introhive[.]com
- nixonpeabody[.]vmlstage[.]com
- nixonpeabody[.]zoom[.]us
- nixonpeabody[.]com[.]outerstats[.]com
- nixonpeabody[.]app[.]kirasystems[.]com
- nixonpeabody2[.]adobeconnect[.]com
- nixonpeabody[.]highq[.]com[.]origin[.]highq[.]com
- nixonpeabody[.]com[.]clearwebstats[.]com

- nixonpeabody[.]highq[.]com[.]cn[.]highq[.]com
- nixonpeabody[.]pixeldance[.]com
- nixonpeabody[.]searchfirm[.]micronapps[.]com
- nixonpeabody[.]highq[.]com
- nixonpeabody-sc102xm0-centralus-si[.]azurewebsites[.]net
- amgreetings[.]printercloud[.]com
- amgreetingscareers-com02i[.]mail[.]protection[.]outlook[.]com
- amgreetings[.]benefithub[.]com
- amgreetings[.]ui[.]quickbase[.]com
- amgreetings[.]walkertracker[.]com
- amgreetings[.]int[.]hubwoo[.]com
- amgreetingscareers-com[.]mail[.]protection[.]outlook[.]com
- amgreetings[.]mywbenefits[.]com
- amgreetings[.]dev[.]worksmartsuite[.]com
- amgreetings[.]jamfcloud[.]com
- amgreetingscareers-com02i[.]mail[.]protection[.]skribble[.]pro
- amgreetings-iphone-wifi[.]h6[.]xiaoeknow[.]com
- cbre[.]com[.]ve[.]us[.]cas[.]ms
- cbre[.]apps[.]dev[.]cf[.]thalesdigital[.]io
- cbre[.]ent[.]allianzim[.]com
- cbre[.]ent[.]syncsketch[.]dev
- cbre[.]campus[.]modelical[.]com
- cbre[.]account[.]recruitership[.]com
- cbre[.]referrals[.]connxusdemo[.]com
- cbre[.]referrals[.]fortnite[.]com
- cbre[.]referrals[.]yelp[.]com
- cbre[.]locator[.]zalora[.]com[.]ph
- cbre[.]myhse[.]wormhole[.]com
- cbre[.]ent[.]frontapp[.]com
- cbre[.]denver[.]brokers[.]business[.]ivirus[.]ru
- cbre[.]co[.]uk[.]mcas[.]ms
- cbre[.]ent[.]vk[.]cc
- cbre[.]at[.]ip4[.]bz
- cbre[.]genmills[.]liebi[.]com
- cbre[.]demo[.]tokopedia[.]com
- cbre[.]sandbox[.]joinmesa[.]com
- cbre[.]com[.]br[.]apescout[.]com
- cbre[.]referrals[.]miro[.]com
- cbre[.]myhse[.]speakap[.]com
- cbre[.]co[.]uk[.]eu2[.]cas[.]ms
- cbre[.]referrals[.]binance[.]com
- cbre[.]stage[.]movecloser[.]pl
- cbre[.]com[.]us[.]cas[.]ms
- cbre[.]ent[.]pulleyapp[.]com
- cbre[.]enterpriseqa[.]shakedeal[.]com
- cbre[.]pl[.]ipaddress[.]com
- cbre[.]co[.]uk[.]eu[.]cas[.]ms
- cbre[.]crmaxe[.]microsites02[.]redbull[.]com
- cbre[.]myhse[.]giftya[.]com
- cbre[.]qa7[.]monigle3[.]net
- cbre[.]referrals[.]spotifyforbrands[.]com
- cbre[.]bree[.]warnerbros[.]com
- cbre[.]ent[.]westhotel[.]web-6[.]hiltonbusinessonline[.]com
- cbre[.]referrals[.]selectminds[.]com
- cbre[.]ent[.]ya[.]ru
- cbre[.]pt[.]cutercounter[.]com
- cbre[.]com[.]tested[.]website
- cbre[.]ch[.]locatee[.]com
- cbre[.]dev[.]kodeks[.]no
- cbre[.]testing[.]myvolusion[.]com
- cbre[.]referrals[.]molinostuckyhilton[.]web-11[.]hiltonbusinessonline[.]com
- cbre[.]testing[.]canva-apps[.]com
- cbre[.]co[.]uk[.]admin-us[.]cas[.]ms
- cbre[.]fi[.]w3cdomain[.]com
- cbre[.]qa2[.]monigle3[.]net

- cbre[.]ent[.]williamhill[.]com
- cbre[.]com[.]tr[.]wenotify[.]net
- cbre[.]referrals[.]ardoq[.]com
- cbre[.]uk[.]yeahtic[.]com
- cbre[.]referrals[.]paydiant[.]com
- cbre[.]vo[.]llnwd[.]net
- cbre[.]ent[.]lucidstaging[.]app
- cbre[.]ent[.]fetlife[.]com
- cbre[.]referrals[.]robinhood[.]com
- cbre[.]genmills[.]litix[.]io
- cbre[.]magiceden[.]workers[.]dev
- cbre[.]referrals[.]williamhill[.]com
- cbre[.]com[.]ve[.]admin-us[.]cas[.]ms
- cbre[.]corprealestate[.]truist-api[.]com
- cbre[.]myhse[.]acc[.]mobilevikings[.]be
- cbre[.]ent[.]invisionapp[.]com
- cbre[.]a1[.]mailplus[.]nl
- cbre[.]saml[.]morganstanley[.]com
- cbre[.]ru[.]whoisbucket[.]com
- cbre[.]genmills[.]facilitiesdesk[.]com
- cbre[.]mirror[.]omnee[.]io
- cbre[.]ent[.]betsson[.]com
- cbre[.]ent[.]airbnbchicago[.]com