The Makings of ADHUBLLKA According to the DNS

Table of Contents

Executive Report

It's not uncommon for cybercriminals to tweak an existing piece of malware and then call it a new creation. We've seen that happen even in malware's earliest days. It's actually happening more and more these days, especially with the rise of the malware-as-a-service (MaaS) business model.

Netenrich recently published an in-depth analysis of one such malware they've dubbed "ADHUBLLKA," which has been linked and likened to at least three older malware—CryptoLocker, LimeRAT, and GlobeImposter. The researchers identified 47 indicators of compromise (IoCs)—11 domains, 32 IP addresses, and four email addresses—so far.

Using the IoCs as jump-off points, the WhoisXML API research team performed a DNS deep dive that uncovered:

- An additional registrant email address from an IoC's current WHOIS record
- An additional IP resolution that turned out to be malicious based on a malware check
- 230 domains hosted on the seemingly dedicated IP addresses identified as IoCs, 18 of which have already been tagged as malicious based on a bulk malware check
- 200 domains starting with the string **yip.** akin to the sole non-Tor-hosted IoC

Behind the ADHUBLLKA IoC Infrastructure

We began our investigation with a further analysis of the published ADHUBLLKA IoCs. First, we performed a WHOIS lookup for the only domain that wasn't hosted on the Tor network—yip[.]su. That led to the discovery of an unredacted registrant email address—root@iplogger[.]com. We also learned that the IoC was administered by RUCENTER-SU and created on 17 January 2017.

Next, we subjected the 32 IP addresses identified as IoCs to a bulk IP geolocation lookup that led to these discoveries:

- Only two of the 32 IP addresses—162[.]159[.]129[.]233 and 40[.]126[.]32[.]133—had active resolutions.
- The IP address 162[.]159[.]129[.]233, under the administration of Cloudflare, Inc., originated from the U.S. while 40[.]126[.]32[.]133, under Microsoft Corporation, pointed to the Netherlands as its origin.

Finally, we conducted a bulk email verification lookup for the four email addresses identified as IoCs. Here's a summary of our findings.

- Three of the email addresses—pr0team@protonmail[.]com, filessupport@onionmail[.]org, and rick5@xmpp[.]jp—didn't have an active Simple Mail Transfer Protocol (SMTP) connection while filessupport@cock[.]li was classified as "bad."
- pr0team@protonmail[.]com was created via a free email service.
- filessupport@cock[.]li was dubbed a disposable email address.

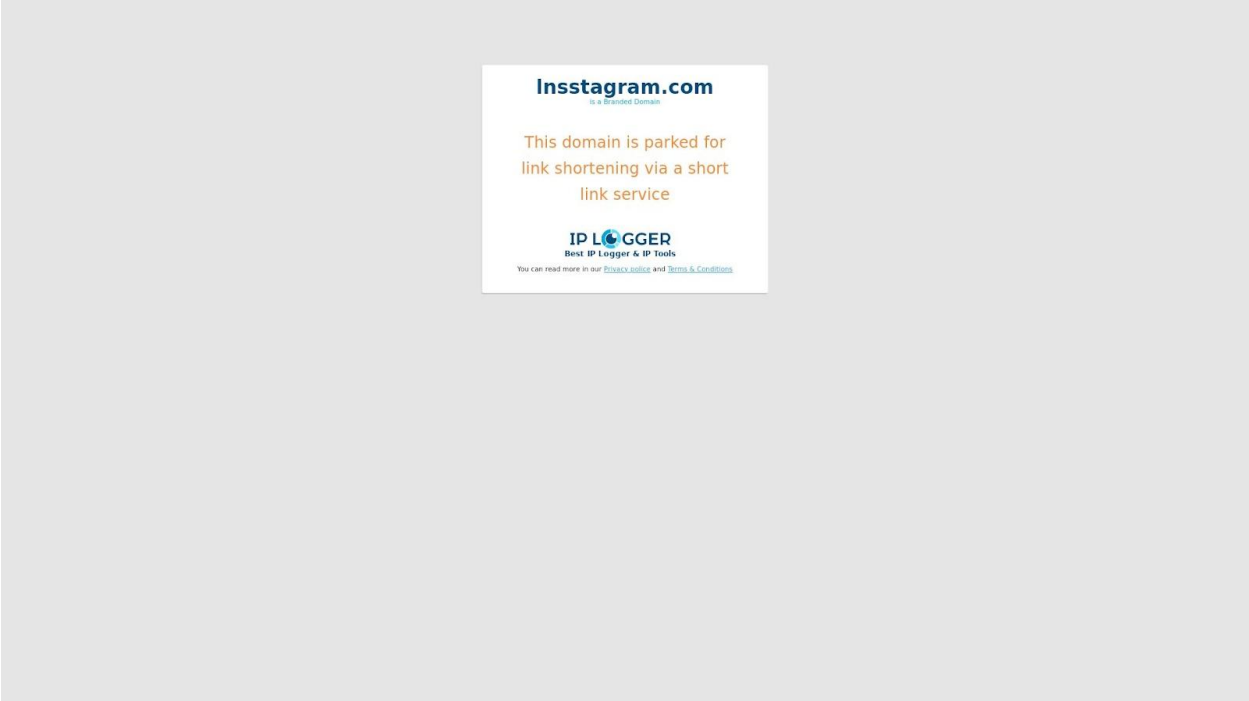
ADHUBLLKA IoC DNS Revelations

As it is our goal to make the Internet safer for all users, we sought to find artifacts potentially connected to ADHUBLLKA. We started by looking for the IP address yip[.]su resolved to. Our DNS lookup gave 148[.]251[.]234[.]93 as a result. The IP address, which turned out to be malicious according to a malware check, originated from Germany and was administered by Hetzner Online GmbH based on an IP geolocation lookup.

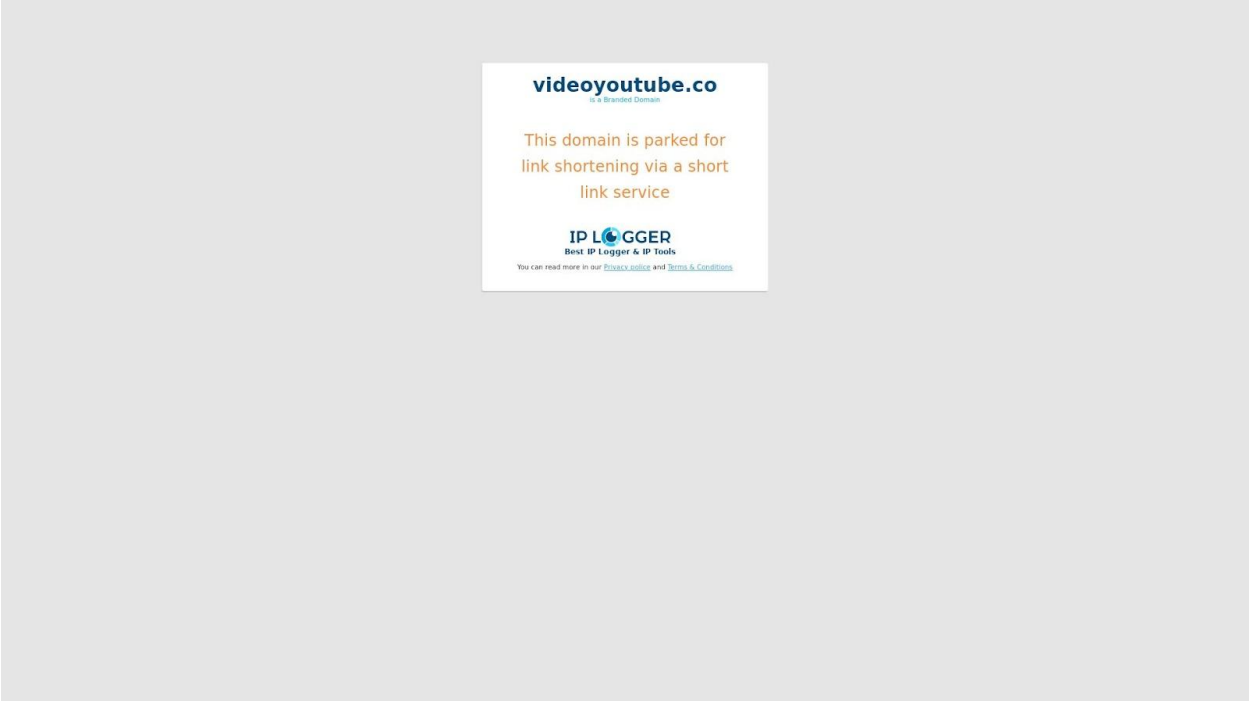
Next, we performed reverse IP lookups for the 33 IP addresses—32 identified as IoCs and one additional IP resolution—and found that 15 were seemingly dedicated. Together, they hosted 230 domains, 18 of which turned out to be malicious based on a bulk malware check.

Screenshot lookups showed that all of the malicious domains continued to host live content.

Two of the domain names were interesting since they contained brand names, specifically Instagram, albeit misspelled (Insstagram[.]com), and YouTube (videoyoutube[.]co). WHOIS record comparisons with the brands' official domains, however, revealed that the malicious properties weren't publicly attributable to the tech giants. Both domains were seemingly parked via the short link service IP Logger.



Screenshot of Insstagram[.]com

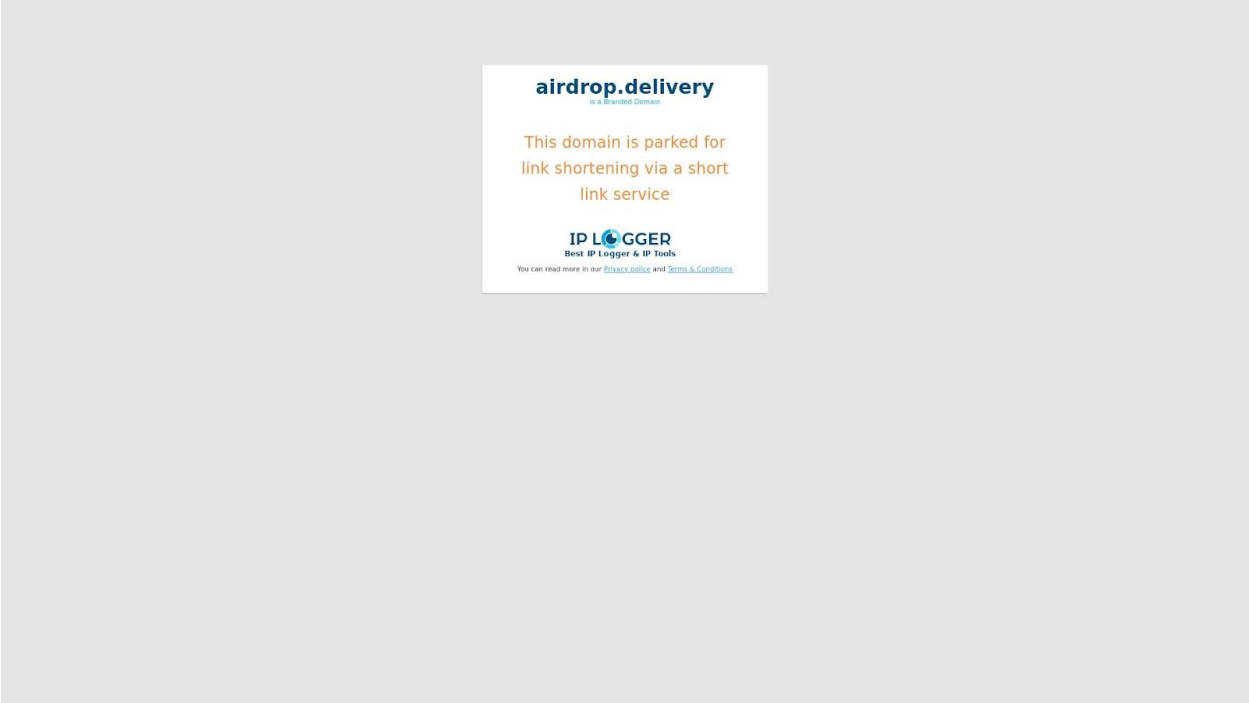


Screenshot of videoyoutube[.]co

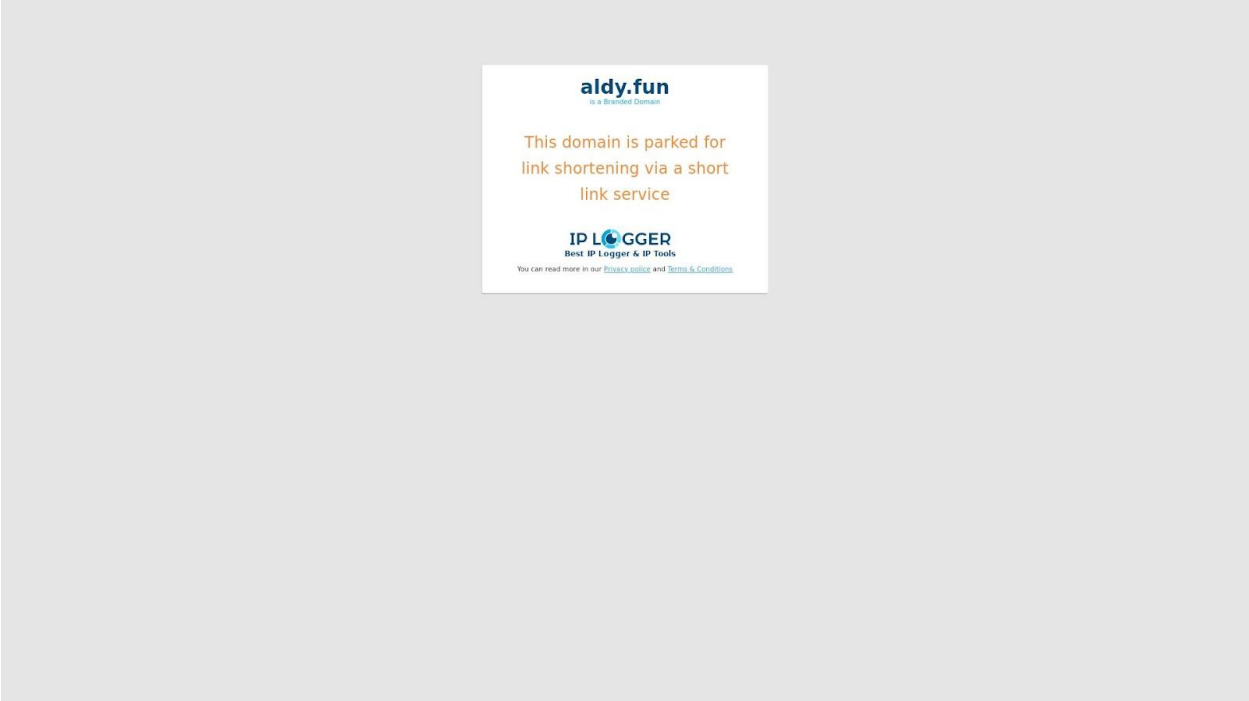
We also found that four of the malicious domains contained the string **iplogger**. We could not, however, explicitly determine if they were owned by the company since the WHOIS record

details of iplogger[.]org (its official domain name) is redacted. However, all four domains sported the company's brand name and logo. They also had the same content as, or redirected to, its official website.

In addition, the pages hosted on 10 other malicious domains also sported the shortened link service provider's logo. Examples are shown below.



Screenshot of airdrop[.]delivery



Screenshot of aldy[.]fun

To check if other possibly connected artifacts were present in the DNS, we looked for domains containing the same text string as the only IoC that wasn't hosted on the Tor network—yip[.]su. Our Domains & Subdomains Discovery search allowed us to uncover 200 such domains.

ADHUBLLKA IoC Ties to CryptoLocker, LimeRAT, and GlobeImposter

The Netenrich analysis revealed ADHUBLLKA connections to at least three malware—the ransomware CryptoLocker, the remote access Trojan (RAT) LimeRAT, and another ransomware GlobeImposter. We thus sought to see if they had DNS ties, too.

We obtained seven IP addresses identified as CryptoLocker, LimeRAT, and GlobeImposterIoCs. A bulk IP geolocation lookup comparison showed that only the LimeRAT IoC 20[.]199[.]13[.]167 had something in common with the ADHUBLLKA IoC 40[.]126[.]32[.]133, that is, they shared the same ISP—Hetzner Online GmbH).

—

Our ADHUBLLKA IoC list expansion analysis led to close to 500 artifacts that could be related to the threat, in addition to another IP address that could further link the newly discovered ransomware to LimeRAT. Also, we noted the presence of several malicious domains containing

the string **iplogger** and the use of the domain iplogger[.]com in the email address used to register the IoC yip[.]su.

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 and IoCs

ADHUBLLKA IoCs Identified by Netenrich

- mrv44idagzu47oktcipn6tlll6nzapi6pk3u7ehsucl4hpxon45dl4yd[.]onion
- mmeeiix2ejdwkmseycljetmpiwebdvgjts75c63camjofn2cjdoulzqd[.]onion
- mmcbkgua72og66w4jz3qcxkkhefax754pg6iknmtfujvkt2j65ffraad[.]onion
- helpqvrg3cc5mvb3[.]onion
- helpinfh6vj47ift[.]onion
- decrmbgpvh6kvmti[.]onion
- alcx6zctcmhmn3kx[.]onion
- 7rzpyw3hflwe2c7h[.]onion
- 54fjmcwsszltlixn[.]onion
- 24cduc2htewrcv37[.]onion
- yip[.]su
- 194[.]85[.]61[.]76
- 109[.]70[.]26[.]37
- 8[.]209[.]75[.]209
- 47[.]91[.]93[.]231
- 47[.]75[.]127[.]193
- 5[.]101[.]49[.]142
- 91[.]239[.]235[.]200
- 20[.]80[.]129[.]13
- 23[.]35[.]69[.]10
- 23[.]35[.]69[.]32
- 23[.]35[.]69[.]35
- 23[.]35[.]69[.]42
- 23[.]35[.]69[.]48
- 23[.]35[.]69[.]66
- 162[.]0[.]235[.]197
- 13[.]107[.]4[.]50
- 162[.]159[.]129[.]233
- 162[.]159[.]130[.]233
- 162[.]159[.]133[.]233
- 162[.]159[.]134[.]233
- 162[.]159[.]135[.]233
- 20[.]99[.]184[.]37
- 192[.]229[.]211[.]108
- 104[.]18[.]14[.]101
- 23[.]216[.]147[.]61
- 23[.]216[.]147[.]64
- 13[.]107[.]4[.]52
- 20[.]190[.]160[.]17
- 20[.]190[.]160[.]20
- 20[.]190[.]160[.]22
- 20[.]99[.]132[.]105
- 40[.]126[.]32[.]133
- Pr0team@protonmail[.]com
- filessupport@onionmail[.]org

- filessupport@cock[.]li
- rick5@xmpp[.]jp

Email Address Used to Register the IoC yip[.]su

- root@iplogger[.]com

Additional IP Resolution

- 148[.]251[.]234[.]93

Sample IP-Connected Domains (Limited to Dedicated Hosts)

- wus2s1c-displaycatalog[.]frontdoor[.]bigcatalog[.]commerce[.]microsoft[.]com
- autologon[.]microsoftazuread-sso[.]com
- dub2[.]current[.]a[.]prd[.]aadg[.]akadns[.]net
- www[.]a[.]ak[.]prd[.]aadg[.]akadns[.]net
- www[.]current[.]a[.]prd[.]aadg[.]akadns[.]net
- www[.]tm[.]a[.]prd[.]aadg[.]akadns[.]net
- www[.]tm[.]a[.]prd[.]aadg[.]trafficmanager[.]net
- www[.]tm[.]ak[.]prd[.]aadg[.]akadns[.]net
- www[.]tm[.]ak[.]prd[.]aadg[.]trafficmanager[.]net
- www[.]tm[.]v4[.]a[.]prd[.]aadg[.]akadns[.]net
- www[.]tm[.]v4[.]a[.]prd[.]aadg[.]trafficmanager[.]net
- aurus[.]co[.]th
- plusmax-world[.]com
- 5361411[.]kiev[.]ua
- activit[.]com[.]ua
- agres[.]space
- anripharmglobal[.]com
- apnas-natural[.]com
- arthurs-berdyansk[.]com
- atlas37[.]com
- auramc[.]com
- autoprotector[.]com[.]ua
- avtotrans[.]kr[.]ua
- baby-birthday[.]kiev[.]ua
- babycenter[.]com[.]ua
- babysad[.]kiev[.]ua
- bagel[.]com[.]ua
- borschfest[.]com
- bubbleice[.]com[.]ua
- budcontainer[.]if[.]ua
- budcontainer[.]lviv[.]ua
- cam-z[.]org
- cantexnika[.]kiev[.]ua
- centerlife[.]od[.]ua
- chandi[.]com[.]ua
- chandi[.]kiev[.]ua
- colostrum[.]org[.]ua
- crp-robot[.]com[.]ua
- diridestyle[.]com
- drogerie[.]trade
- dziga[.]com[.]ua
- elikom[.]com
- elroma[.]studio
- fakel-berdyansk[.]com
- fialan[.]info
- fialan[.]net

- fialan[.]org
- flazhok[.]com
- folgoizol[.]com
- foodcenter[.]com[.]ua

Sample Malicious IP-Connected Domains

- autologon[.]microsoftazuread-sso[.]com
- gns-arts[.]com
- pidkova[.]biz
- airdrop[.]delivery
- aldy[.]fun
- cnlyfan[.]com
- diablo4alpha[.]com
- diskonline[.]net
- iplogger[.]cn

Sample String-Connected Domains

- yip[.]science
- yip[.]ca
- yip[.]kim
- yip[.]org[.]in
- yip[.]no
- yip[.]bet
- yip[.]org
- yip[.]network
- yip[.]fi
- yip[.]fj[.]cn
- yip[.]id
- yip[.]realestate
- yip[.]at
- yip[.]jcloud-ver-jpc[.]ik-server[.]com
- yip[.]cl
- yip[.]tech
- yip[.]dog
- yip[.]fashion
- yip[.]sh[.]cn
- yip[.]christmas
- yip[.]fyi
- yip[.]yoga
- yip[.]cz
- yip[.]mo-siemens[.]io
- yip[.]photos
- yip[.]zone
- yip[.]mba
- yip[.]or[.]id
- yip[.]icu
- yip[.]net[.]cn
- yip[.]band
- yip[.]nl
- yip[.]ai
- yip[.]nu
- yip[.]kr
- yip[.]vc
- yip[.]services
- yip[.]realtor
- yip[.]sh
- yip[.]pe
- yip[.]co[.]uk
- yip[.]live
- yip[.]site
- yip[.]link
- yip[.]fit
- yip[.]co[.]th
- yip[.]lu
- yip[.]ru
- yip[.]com[.]au
- yip[.]tw