■侵入の痕跡（Indicators of Compromise、IoC）

IP address

- 87[.]236[.]16[.]235

URL

- hxxps://www.verified-instagramsupport[.]ml/business/contact/

Phishing and scam URLs related to the IP address linked to the attacks:

- hxxp://1-delom.ru/wp-admin/images/Webmail.htm
- hxxp://1nstagram-supp0rt.cf/
- hxxp://adsmoney.pw/
- hxxp://ae-cosmet.ru/
- hxxp://automatic-profit.ru/
- hxxp://avito3.ru/3ds021/
- hxxp://axel39.ru/
- hxxp://bankrotstvo-kursk.ru/
- hxxp://best-rif.online/
- hxxp://bestshop-foryou.online/
- hxxp://black-friday.kz/
- hxxp://bluebadgehelpteams.com/
- hxxp://bluebadgeslnstagram.cf/
- hxxp://bolliani.online/
- hxxp://bonus706.online/
- hxxp://boxberry.ru-orderid.ru/
- hxxp://buian.com/tpjauwp/KTEQ_0103_03062020.zip

- hxxp://buian.com/tpjauwp/KTEQ_34244056_03062020.zip
- hxxp://buian.com/tpjauwp/KTEQ_8560_03062020.zip
- hxxp://busfor-payment.online/
- hxxp://businesslinesupport.com/
- hxxp://cdek.ru-orderid.ru/
- hxxp://centerbuh96.ru/
- hxxp://clientesdkb.com/
- hxxp://copyrightissue.tk/confirm
- hxxp://copyright-Instagramhelpsuport.tk/
- hxxp://copyrightverify-instagram.com/
- hxxp://coronavirus-propusk.ru/
- hxxp://cozdat.website/
- hxxp://developer007.ru/fatalyti.rar
- hxxp://duffleywov.host/
- hxxp://e-devletturkiyeaidatsistemimgovtr.com/
- hxxp://ensymax.com/
- hxxp://excheats.online/
- hxxp://fb-covidsupport.ml/
- hxxp://fblnstagrambluebadgehelp.ml/
- hxxp://florencia-spb.ru/
- hxxp://form-Instagramverificationbadges.com/
- hxxp://forum445.online/
- hxxp://full-design.online/
- hxxp://funseeds.site/
- hxxp://gasimpro.space/
- hxxp://gastro-line.online/
- hxxp://gitara-plus.ru/
- hxxp://helpers-verified.com/
- hxxp://helplnstagramverifiedbadges.ml/
- hxxp://hspillow.online/
- hxxp://hydragid.space/
- hxxp://igbluebadgeverification.cf/
- hxxp://instagram.help--services.cf/
- hxxp://instagrambadgeverified.ml/
- hxxp://instagramcopryhgthelpp.ml/

- hxxp://instagramforcopyrights.com/
- hxxp://instagramsupportdesk.com/
- hxxp://katerinakrovateva.online/
- hxxp://kazhetkoi.site/
- hxxp://listvennica-mos.online/
- hxxp://liv-rus.ru/
- hxxp://lnstagramcopyrightappeal.cf/support/3547839323473811
- hxxp://lnstagramcopyrightappeal.cf/support/3547839323473811/2020/04/09
- hxxp://lnstagramcopyright-bluebadgeverification.net/
- hxxp://lnstagramcopyrightinfohelps.ml/
- hxxp://lnstagramhelp2569874.tk/
- hxxp://lnstagramhelpscopyrightssupports.ml/
- hxxp://lnstagram-helpservice-team.com/
- hxxp://lnstagramverifyform.ml/
- hxxp://lnstagramverifymanagment.com/
- hxxp://mail-maskcentr.ru/
- hxxp://maskskin.site/
- hxxp://meta42.ru/
- hxxp://miningplatform.space/
- hxxp://napalmshop73.online/
- hxxp://natalia-shibalkina.online/
- hxxp://otoplenie-svarka-murmansk.online/
- hxxp://pays.pm/2064a0b6/
- hxxp://pays.pm/3db012/
- hxxp://pays.pm/3db013/
- hxxp://pays.pm/3db014/
- hxxp://pays.pm/3db015/
- hxxp://pays.pm/3db016/
- hxxp://pays.pm/3db017/
- hxxp://pays.pm/3dS016/
- hxxp://pays.pm/3dS017/
- hxxp://pays.pm/3ds020/
- hxxp://pays.pm/3ds022/
- hxxp://pays.pm/3re022/
- hxxp://pays.pm/5361806/

- hxxp://pizzaentertainnment.com/
- hxxp://podarok67.online/
- hxxp://podarok677.space/
- hxxp://poverka-rf.com/
- hxxp://prombelt.com/
- hxxp://pron4u.2cuptea.site/
- hxxp://pro-structure.ru/fgp83hz3v1yy/de/firmenkunden
- hxxp://provesetor.ml/7dbbe80602f3fb3fbbb8f9bb03ff8802/index.php?cmd=login
- hxxp://riphyon.com/
- hxxp://sberbank-08-dr.ru/
- hxxp://school91distant.ru/
- hxxp://secured2recover.ml/
- hxxp://secured2recover.tk/
- hxxp://seofeed.ru/
- hxxp://shpweb.online/
- hxxp://socialmediabluebadge.com/
- hxxp://stopcoronavirusu.ru/
- hxxp://superzhaloba.online/
- hxxp://supportlnstagram.tk/
- hxxp://supportverifyinstagram.tk/
- hxxp://tehnomir-vostok.ru/
- hxxp://tryenglish.ru/
- hxxp://uaz-51.online/
- hxxp://verified-instagramsupport.ml/
- hxxp://verify-badge.com/557
- hxxp://verify-badge.com/pjj
- hxxp://verify-badge.com/pjx
- hxxp://verify-badge.com/sitemap.html
- hxxp://verify-blue-teak-instagram.gq/
- hxxp://vvdnhiksd.site/
- hxxp://www.boxberry.ru-orderid.ru/index.php
- hxxp://www.facebooklivesupport.cf/
- hxxp://www.instagramlivecommunity.com/
- hxxp://www.instagramsupportdesk.com/
- hxxp://xn-----6kcbgkka5afshedentcbdb1chnldg8zmcm.xn--p1ai/

- hxxp://xn--80abddyaur.xn--p1ai/
- hxxp://xn----htbbbbonju6adjdd2m.xn--p1ai/
- hxxp://xolod-ok.ru/
- hxxp://you-partner.site/
- hxxps://1nstagram-supp0rt.cf/
- hxxps://akilidestekbasvuru.online/uygulamaid542154800095246
- hxxps://authhimersxiaa8j.ga/us8920922/usaat/uS0909/captcha
- hxxps://authhimersxiaa8j.ga/us8920922/usaat/uS0909/captcha/run/contact.html?6175746868696d65727378696161386a2e67616175746868696d65727378696161386a2e67616175746868696d65727378696161386a2e67616175746868696d65727378696161386a2e6761
- hxxps://bluebadgehelpteams.com/form.php
- hxxps://business-Instagram-confirm.ml/
- hxxps://consultmill.ru/kvartira/propiska/v-municipalnuyu.html
- hxxps://copyrightlivesupport.cf/
- hxxps://ebayappl.com/ebayapp.zip
- hxxps://ebayappl.com/EbayApp.zip
- hxxps://e-devletturkiyeaidatsistemimgovtr.com/
- hxxps://fblnstagrambluebadgehelp.ml/
- hxxps://form-Instagramverificationbadges.com/
- hxxps://form-Instagramverifiedbadge.ml/
- hxxps://help-about.cf/info/848350608641984=VerifyAccount.php?nick=bhills_4964@mailinator.com
- hxxps://helpers-verified.com/
- hxxps://helpInstagramverifiedbadges.ml/
- hxxps://hydraruzxpnew4aaf.space/
- hxxps://igbluebadgeverification.cf/
- hxxps://instagram.help--services.cf/
- hxxps://instagram-copyrightreview.com/
- hxxps://instagram-helpcenter-com.ml/
- hxxps://instagramlivecommunity.com/
- hxxps://instagramlivecommunity.com/form.php
- hxxps://instagramverifiedcopyright.tk/
- hxxps://j-ulia.ru/
- hxxps://livesupportInstagram.ml/
- hxxps://Instagramcopyrightinfohelps.ml/

- hxxps://lnstagram-copyrights-center.com/
- hxxps://lnstagram-helpcontact.ml/
- hxxps://lnstagramoffice.com/
- hxxps://lnstagramssupportcenter.com/username.php
- hxxps://lnstagram-suspended-account-center.cf/
- hxxps://lnstagramverifymanagment.com/
- hxxps://mivago.ru/intense-j13-40-den-kolgotki/
- hxxps://pays.pm/43161893
- hxxps://percunas.com.ua/pribor/shkafy-raspredelitelnye-kru-rn-6-rt-vnt
- hxxps://poleznii-site.ru/meditsina/vitaminy/kollagen-dlya-sustavov-svyazok-i-suhozhiliy-otzyvykak-prinimat-kak-vybrat.html
- hxxps://reolink-russia.ru/
- hxxps://secure2recover.ml/
- hxxps://socarenergoresource.ru/
- hxxps://socialmediabluebadge.com/
- hxxps://socialmediabluebadge.com/form.php
- hxxps://supportcenterinstagram.ml/
- hxxps://supportverifyinstagram.tk/
- hxxps://uoperatora.ru/yota/knopka-besplatnogo-dostupa-yoty-kak-prodlit-internetavtonazhatie.html
- hxxps://verifycopyright-instagram.com/
- hxxps://vgolove.net/licenzionnyj-klyuch-iobit-uninstaller-pro-8-kod-aktivacii-2019-2020/
- hxxps://vgolove.net/wp-content/uploads/soft/Reg.Org_8.52_serial.zip
- hxxps://vvdnhiksd.site/
- hxxps://www.copyrightforsupportinsta.cf/
- hxxps://www.secure2recover.cf/
- hxxps://www.secure2recover.tk/

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com