

New Bait Used in Instagram Profile Hacking Scheme

- Appendix

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://bluebadgesInstagram.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-Instagramhelpsupport.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://fbInstagrambluebadgehelp.ml/
- hxxp://florescia-spb.ru/
- hxxp://form-Instagramverificationbadges.com/
- hxxp://forum445.online/
- hxxp://full-design.online/
- hxxp://funseeds.site/

- <http://gasimpro.space/>
- <http://gastro-line.online/>
- <http://gitara-plus.ru/>
- <http://helpers-verified.com/>
- <http://helpInstagramverifiedbadges.ml/>
- <http://hspillow.online/>
- <http://hydragid.space/>
- <http://igbluebadgeverification.cf/>
- <http://instagram.help--services.cf/>
- <http://instagrambadgeverified.ml/>
- <http://instagramcopyrighthelp.ml/>
- <http://instagramforcopyrights.com/>
- <http://instagramsupportdesk.com/>
- <http://katerinakrovateva.online/>
- <http://kazhetkoi.site/>
- <http://listvennica-mos.online/>
- <http://liv-rus.ru/>
- <http://Instagramcopyrightappeal.cf/support/3547839323473811>
- <http://Instagramcopyrightappeal.cf/support/3547839323473811/2020/04/09>
- <http://Instagramcopyright-bluebadgeverification.net/>
- <http://Instagramcopyrightinfohelps.ml/>
- <http://Instagramhelp2569874.tk/>
- <http://Instagramhelpscopyrightssupports.ml/>
- <http://Instagram-helpservice-team.com/>
- <http://Instagramverifyform.ml/>
- <http://Instagramverifymanagment.com/>
- <http://mail-maskcentr.ru/>
- <http://maskskin.site/>
- <http://meta42.ru/>
- <http://miningplatform.space/>
- <http://napalmshop73.online/>
- <http://natalia-shibalkina.online/>
- <http://otoplenie-svarka-murmansk.online/>
- <http://pays.pm/2064a0b6/>
- <http://pays.pm/3db012/>
- <http://pays.pm/3db013/>
- <http://pays.pm/3db014/>
- <http://pays.pm/3db015/>
- <http://pays.pm/3db016/>
- <http://pays.pm/3db017/>
- <http://pays.pm/3dS016/>
- <http://pays.pm/3dS017/>
- <http://pays.pm/3ds020/>
- <http://pays.pm/3ds022/>
- <http://pays.pm/3re022/>
- <http://pays.pm/5361806/>

- <http://pizzaentertainment.com/>
- <http://podarok67.online/>
- <http://podarok677.space/>
- <http://poverka-rf.com/>
- <http://prombelt.com/>
- <http://pron4u.2cuptea.site/>
- <http://pro-structure.ru/fgp83hz3v1yy/de/firmenkunden>
- <http://provesetor.ml/7dbbe80602f3fb3fbbb8f9bb03ff8802/index.php?cmd=login>
- <http://riphyon.com/>
- <http://sberbank-08-dr.ru/>
- <http://school91distant.ru/>
- <http://secured2recover.ml/>
- <http://secured2recover.tk/>
- <http://seofeed.ru/>
- <http://shpweb.online/>
- <http://socialmediabluebadge.com/>
- <http://stopcoronavirusu.ru/>
- <http://superzhaloba.online/>
- <http://supportInstagram.tk/>
- <http://supportverifyinstagram.tk/>
- <http://tehnomir-vostok.ru/>
- <http://tryenglish.ru/>
- <http://uaz-51.online/>
- <http://verified-instagramsupport.ml/>
- <http://verify-badge.com/557>
- <http://verify-badge.com/pjj>
- <http://verify-badge.com/pjx>
- <http://verify-badge.com/sitemap.html>
- <http://verify-blue-teak-instagram.gq/>
- <http://vvdnhiksd.site/>
- <http://www.boxberry.ru-orderid.ru/index.php>
- <http://www.facebooklivesupport.cf/>
- <http://www.instagramlivecommunity.com/>
- <http://www.instagramsupportdesk.com/>
- <http://xn-----6kcbgkka5afshedentcbdb1chnldg8zmcm.xn--p1ai/>
- <http://xn--80abddyaur.xn--p1ai/>
- <http://xn----htbbbonju6adjdd2m.xn--p1ai/>
- <http://xolod-ok.ru/>
- <http://you-partner.site/>
- <http://1instagram-supp0rt.cf/>
- <http://akilidestekbasvuru.online/uygulamaid542154800095246>
- <http://authhimersxiaa8j.ga/us8920922/usaat/uS0909/captcha>
- <http://authhimersxiaa8j.ga/us8920922/usaat/uS0909/captcha/run/contact.html?6175746868696d65727378696161386a2e67616175746868696d65727378696161386a2e67616175746868696d65727378696161386a2e6761>
- <http://bluebadgehelptteams.com/form.php>

- <https://business-Instagram-confirm.ml/>
- <https://consultmill.ru/kvartira/propiska/v-municipalnuyu.html>
- <https://copyrightlivesupport.cf/>
- <https://ebayappl.com/ebayapp.zip>
- <https://ebayappl.com/EbayApp.zip>
- <https://e-devletturkiyeaidatsistemimgovtr.com/>
- <https://fbInstagrambluebadgehelp.ml/>
- <https://form-Instagramverificationbadges.com/>
- <https://form-Instagramverifiedbadge.ml/>
- https://help-about.cf/info/848350608641984=Verify-Account.php?nick=bhills_4964@mailinator.com
- <https://helpers-verified.com/>
- <https://helpInstagramverifiedbadges.ml/>
- <https://hydraruzxpnew4aaf.space/>
- <https://igbluebadgeverification.cf/>
- <https://instagram.help--services.cf/>
- <https://instagram-copyrightreview.com/>
- <https://instagram-helpcenter-com.ml/>
- <https://instagramlivecommunity.com/>
- <https://instagramlivecommunity.com/form.php>
- <https://instagramverifiedcopyright.tk/>
- <https://j-ulia.ru/>
- <https://livesupportInstagram.ml/>
- <https://Instagramcopyrightinfohelps.ml/>
- <https://Instagram-copyrights-center.com/>
- <https://Instagram-helpcontact.ml/>
- <https://Instagramoffice.com/>
- <https://Instagramsupportcenter.com/username.php>
- <https://Instagram-suspended-account-center.cf/>
- <https://Instagramverifymanagment.com/>
- <https://mivago.ru/intense-j13-40-den-kolgotki/>
- <https://pays.pm/43161893>
- <https://percnas.com.ua/pribor/shkafy-raspredelitelnye-kru-rn-6-rt-vnt>
- <https://poleznii-site.ru/meditsina/vitaminy/kollagen-dlya-sustavov-svyazok-i-suhozhiliy-otzyvy-kak-prinimat-kak-vybrat.html>
- <https://reolink-russia.ru/>
- <https://secure2recover.ml/>
- <https://socarenergoresource.ru/>
- <https://socialmediabluebadge.com/>
- <https://socialmediabluebadge.com/form.php>
- <https://supportcenterinstagram.ml/>
- <https://supportverifyinstagram.tk/>
- <https://uoperatora.ru/yota/knopka-besplatnogo-dostupa-yoty-kak-prodlit-internet-avtonazhatie.html>
- <https://verifycopyright-instagram.com/>
- <https://vgolove.net/licenzionnyj-klyuch-iobit-uninstaller-pro-8-kod-aktivacii-2019-2020/>

- https://vgolove.net/wp-content/uploads/soft/Reg.Org_8.52_serial.zip
- <https://vvdnhiksd.site/>
- <https://www.copyrightforsupportinsta.cf/>
- <https://www.secure2recover.cf/>
- <https://www.secure2recover.tk/>

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, 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 new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com



©2020 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.