malware-ioc/UNC1151 at master · prodaft/malware-ioc · GitHub

github.com/prodaft/malware-ioc/tree/master/UNC1151

prodaft

prodaft/**malware-ioc**

This repository contains indicators of compromise (IOCs) of our various investigations.

3 Contributors | 1 Issue | 105 Stars | 17 Forks

UNC1151 Group Indicators of Compromise (IOC)

These IOCs were released as part of PTI team research. The report link is available here.

UNC1151 Phishing Domains

account-noreply.space
account-passports.top
accounts-facebook.com-pastas.top
accounts-gmail.com-check.online
accounts-gmail.com-login.space
accounts-group.com-pastas.top
accounts-mail.site
accounts-mail.top
accounts-secure.com-firewall.online
accounts-verify.space
accounts.safe-mail.space
accounts.secure-ua.site
accounts.verify-email.space
accountsverify.top
aplikacje.ron-mil.space
bezpieczenstwo-danych.website
bhwbehb.wecwe.com
bigmir.space
bokinteria.pl-kontrola-bezpieczenstwa.space
bokinteria.weryfikacja-konta.pw
com-pastas.top
com-verificate.top
com-verification.online
confirm.acount-pasport.site
confirm.id-bigmir.site
cookie-firewall.com-login.space
dzial-bezpieczenstwa.space
exprentis.com
google.accounts.verify.no-reply.space
google.com-firewall.online
google.verifyprofiles.space
group-rambler.site
grupa-mailowa.weryfikacja-konta.link
i-ua.ml
i.ua-login.top
i.ua-passport.site
i.ua-passport.space
i.ua-passport.top
iat.com.ua
id-mail.site
id-mail.tech
id.verify-mail.space
interia.pl-identyfikacja-uzytkownika.pw
interia.poczta-mailowa.top
interia.weryfikacja-poczty.space
interia.weryfikacja-uzytkownika.site
interii.konto-verify.space
kemda.eu
konto-onet.site
konto-verify.space
konto.weryfikacja-uzytkownika.link
konto.weryfikacja-uzytkownika.online
konto.weryfikacja-uzytkownika.pw
kontrola-bezpieczenstwa.link
kontrola-bezpieczenstwa.walidacja-uzytkownika.pw
kontrola-konta.online
kontrola-mailowa.top
kontrola-poczty.top
krebas.lt
login.creditals-email.space
login.meta-ua.top
login.passport-verify.top
login.verification-email.space
login.verify-mail.space
logowanie.identyfikacja-uzytkownika.link
logowanie.kontrola-poczty.link
mail-accounts.site
mail-accounts.space
mail-profiles.space
mail.mil-gov.space
meta-ua.space
mil-gov.space
mirrohost.space
no-reply.accounts-verify.space
no-reply.space
no-reply.verifyprofiles.space
no-response.site
no-response.website
noreply.accountsverify.top

```
okonto.kontrola-bezpieczenstwa.pw
okonto.kontrola-poczty.pw
passport.i-ua.space
passport.login-verify.top
passport.meta-log.site
passport.meta-ua.top
passport.secure-ua.pw
passport.secure-ua.space
pastas.top
pis.kontrola-bezpieczenstwa.site
plklll.site
poczta-mailowa.top
poczta.bezpieczenstwo-danych.website
poczta.departament-bezpieczenstwa.space
poczta.identyfikacja-uzytkownika.space
poczta.kontrola-bezpieczenstwa.link
poczta.kontrola-bezpieczenstwa.top
poczta.kontrola-konta.online
poczta.kontrola-mailowa.top
poczta.safe-onet.space
poczta.sprawdzanie-zabezpieczen.space
poczta.walidacja-konta.site
poczta.walidacja-uzytkownika.pw
poczta.weryfikacja-okonto.online
poczta.weryfikacja-okonto.site
poczta.wp-firewall.website
pomoc.sprawdzanie-zabezpieczen.space
pomoc.weryfikacja-okonto.online
post.mil-gov.space
post.verify-mail.space
potwierdzenie.konto-onet.site
rambler-account.top
rambler-profile.site
rambler-verify.top
rambler.account-noreply.space
rtrrsfgsfg.site
rwegfwfe.site
sdfavavvvv.site
security.passportlogin.top
service.kontrola-poczty.space
system.walidacja-konta.link
system.walidacja-konta.pw
taysbb.ru
ua-passport.pw
ubsbha.ru
ukr.account-login.top
usluga.kontrola-poczty.top
veirfy-ua.space
verification-email.website
verify.account-login.top
verify.accounts-login.top
verify.accounts-mail.site
verify.accounts-passport.top
verify.acount-passport.site
verify.group-rambler.site
verify.mail-profiles.space
verify.no-replay.space
verify.passport-login.top
verify.passportlogin.top
verify.profiles-login.top
verifyprofiles.space
verifyprofiles.top
walidacja-konta.site
walidacja-poczty.space
walidacja-uzytkownika.space
weryfikacja-konta.link
weryfikacja-konta.space
weryfikacja-okonto.online
weryfikacja-okonto.site
weryfikacja-uzytkownika.link
weryfikacja-uzytkownika.online
weryfikacja-uzytkownika.top
weryfikacja.system-pocztowy.space
wirtualna.grupa-pocztowa.online
wojskowa.akademia-mil.space
```

Phishing Attachments

MD5	SHA1	SHA256
12bd6e9b272a13a70f1e0354b4b33fb5	3b3552f82621a4d67c6b0c955c87b8f8181f4141	57629b46602bf8eaaab8914e1584f0002b59bb1107
9549340bfd3ed44203434b63a270eafa	38cff1fccb6d83730eb0408f2e5bd6a9504c60c7	4c2600843e06db6612a35e93dba74436076cb3c83c
5f7d7b491b98b29dcf8b8ac0239cc660	55f017ca223d71e2c8d67a44ba2afd18d5b1e3b2	d3fd70868556cdb5fccafb2aa1a8bafc5465d61929c7
3c909c3afbfb67d54ac34bff270bfe93	f43520700834d964861d091b345bfe387a510fa2	615fc48c199df4b6424ff880da797735c9002b5014e2
09e19240cbf0faa4f34d71ddf4919eec	54abd425b1d5e87fe833ffcddfef223e3916e68f	5e4ac32767cdfe31e21e577f353d0a19596c1c950f0
2d45004a62e6c3bfbe9357eb92ec2ba5	ba7bb3e52539ca0e07b7806a511557a6e311c9f6	9f420a6f76744a3c2183261488a22a21085fce1b5bb

Command and Control Server

```
kurioworld.cf
kurioworld.gq
```