


Thomas Buzza
@p-byer


Roberto Rodriguez
@cphrmrdrdy

BLUE TEAM ARSENAL TRAINING

PYTHON AND GENERATIVE AI FOR THREAT INTELLIGENCE

BlackHat Europe: 4 Days - December 9-12

 [Link in Bio](#)



24,945 followers

1,039 Posts

View Profile

+ Follow


The image is a screenshot of a LinkedIn post by Thomas Roccia. A large white sign-in overlay is positioned in the upper half of the image. The overlay contains the text "Sign in to view more content", "Create your free account or sign in to continue your search", and two buttons: "Continue with Google" (with the Google logo) and "Sign in". Below these buttons, it says "or" and "New to LinkedIn? Join now". At the bottom of the overlay, there is a disclaimer: "By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy."

Below the overlay, a diagram titled "Decoded C2 from ICOs" is visible. It shows a list of domains and services, including "msstorageazure(.com)/analysis", "officestoragebox(.com)/api/biosync", "visualstudiofactory(.com)/groupcore", "azuredeploystore(.com)/cloud/images", "msstorageboxes(.com)/xbox", "officeaddons(.com)/quality", "sourceslabs(.com)/status", "zacharryblogs(.com)/xmlquery", "pbxcloudservices(.com)/network", "pbxphonenetwork(.com)/phone", "akamaitechcloudservices(.com)/v2/fileapi", "azureonlinestorage(.com)/google/storage", "msedgepackageinfo(.com)/ms-webview", "glcloudservice(.com)/v1/status", "pbxsources(.com)/queue", and "www.3cx(.com)/blog/event-trainings/".

The diagram illustrates a workflow: 1. "Downloads ICO containing the C2 Base64 encoded and AES + GCM encrypted." (with a URL: "https://raw.githubusercontent.com/iconstorages/images/main/icon[1-15].ico"). 2. "Retrieve a JSON that contains a payload encoded in base64." (with a JSON snippet: "{"url":"","description":"","meta":"vyoAAL4D<truncated>"}"). 3. "Install an information-stealer payload." (with a magnifying glass icon over a document).

The post's engagement metrics show 4,414 likes and 110 comments. The author's name, "Thomas Roccia", is visible, along with his title, "Author, Speaker, Senior Security Researcher at Microsoft". The post is dated "1y" (1 year ago). The author's Twitter handle, "@FR0GGER_THOMAS ROCCIA", is also displayed.

Page 1 of 2

 LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job 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](#).

Florian Roth

VP R&D at Nextron Systems

1y

Awesome graph 🌟

Like ·

Reply

13 Reactions

Robert MacMillan

1y

Great summary... The samples on [Vx Underground](#) also had one with a valid signature using a Microsoft certificate with thumbprint 914A09C2E02C696AF394048BCB8D95449BCD5B9E (Serial number 33000003DFFB6AE3F427ECB6A30000000003DF). There was also one with no signature.

Also worth noting, two of the sections with no characteristics (permissions) are seen in Expiro malware samples - could be a variant of that older stuff...

Like ·

Reply

1 Reaction

Fabrice D.

Conseiller en a

Hi Thomas, r

Thanks

Like ·

Reply

1 Reaction

Neumann Li

DFIR professio

Love all you

Like ·

Reply

1 Reaction

Mike Herrin

Business Tech

I was gonna

Like ·

Reply

1 Reaction

Louie E.

Multi-Clou

Thomas, I lik

Thanks

Like ·

Reply

1 Reaction

Aaron Birnbaum

Chief Security Officer @ Seron Security | vCISO | TRaViS ASM Founder | Cybersecurity Whisperer | ...

1y

Thanks for sharing the analysis.

Like ·

Reply

1 Reaction

See more comments

To view or add a comment, [sign in](#)



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](#).