

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](#).

Agree & Join LinkedIn

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

[Skip to main content](#)
[LinkedIn](#)

- [Articles](#)
- [People](#)
- [Learning](#)
- [Jobs](#)
- [Games](#)
- [Get the app](#)

[Join now](#) [Sign in](#)

Thomas Roccia's Post



 [View profile for Thomas Roccia, graphic](#)
[Thomas Roccia](#)

Author, Speaker, Senior Security Researcher at Microsoft

1y



- [Report this post](#)


 If you are looking for a comprehensive overview of the current [#3CX](#) supply chain attack, I created a diagram that shows the attack flow for the Windows version!  I'll update as soon as the analysis progresses. [#cybersecurity](#) [#infosec](#) [#supplychainattack](#) [#3CXpocalypse](#)

-  No alternative text description for this image

   [4,414 110 Comments](#)

[Like Comment](#)

- [Copy](#)
- [LinkedIn](#)
- [Facebook](#)
- [Twitter](#)


 [Thomas Roccia](#)
[Thomas Roccia](#)

Author, Speaker, Senior Security Researcher at Microsoft

1y



- [Report this comment](#)

 FYI what we call a ‘stealer’ is not really a stealer. It mainly grabs some information from the infected machines to filter the targets and installs a potential other stage

[Like](#)

[Reply](#)

[13 Reactions](#) 14 Reactions

 [Perfecto Antonio](#)

[Perfecto Antonio](#)

Cyber Security Incident Response Specialist | CSIRT | Blue Team | SCITUM

1y



- [Report this comment](#)

Hi Thomas, great overview, excuse me What software did you use to create the diagram?

[Like](#)

[Reply](#)

[3 Reactions](#) 4 Reactions

 [Florian Roth](#)

[Florian Roth](#)

VP R&D at Nextron Systems

1y



- [Report this comment](#)

Awesome graph ✨

[Like](#)

[Reply](#)

[13 Reactions](#) 14 Reactions

 [Robert MacMillan](#)

[Robert MacMillan](#)

1y



- [Report this comment](#)

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](#)

[5 Reactions](#) 6 Reactions

 [Fabrice D.](#)

[Fabrice D.](#)

Conseiller en architecture Cybersécurité • Analyste en Cybersécurité • Endpoint security, protection des données, et sécurité Infonuagique • Certifié SC-100, SC-200, SC-400 & ISO 27005

1y



- [Report this comment](#)

Hi Thomas, really nice works here thanks. Do we know how they exfiltrate? Thanks

[Like](#)

[Reply](#)

[3 Reactions](#) 4 Reactions

 [Neumann Lim](#)

[Neumann Lim](#)

DFIR professional | SANS Advisory Board | Co-Founder of Malware Village | vCISO | DEFCON/BSides/GrayHatCon/CCTX/HTCIA speaker


1y



- [Report this comment](#)

Love all your diagrams fr0gger

[Like](#)

[Reply](#)
[2 Reactions](#) 3 Reactions
 [Mike Herrington](#)
[Mike Herrington](#)


Business Technology and Cyber Security Advisor

1y



- [Report this comment](#)

I was gonna do a blog post about the threat. Can I use this and attribute it to you?

[Like](#)
[Reply](#)
[1 Reaction](#) 2 Reactions
 [Lcuiê E.](#)
[Lcuiê E.](#)


☁ Multi-Cloud Computing ☺ DevSecOps 🔒 Infrastructure 🏢 Database 📦 Educator 🧑 🏠

1y



- [Report this comment](#)

[Thomas](#), I like the work you put into this. Makes it so much easy to understand. Thanks

[Like](#)
[Reply](#)
[1 Reaction](#) 2 Reactions
 [Aaron Birnbaum](#)
[Aaron Birnbaum](#)

Chief Security Officer @ Seron Security | vCISO | TRaViS ASM Founder | Cybersecurity Whisperer | CISSP | MBA Thoughts, opinions, rants, etc. are my own and are in no way affiliated with any employer/partner/contractor.

1y



- [Report this comment](#)

Thanks for sharing the analysis.

[Like](#)
[Reply](#)
[1 Reaction](#) 2 Reactions

[See more comments](#)

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

 Thomas Roccia

- [1,039 Posts](#)

[View Profile Follow](#)

Explore topics

- [Sales](#)
- [Marketing](#)
- [IT Services](#)
- [Business Administration](#)
- [HR Management](#)
- [Engineering](#)
- [Soft Skills](#)
- [See All](#)

- LinkedIn © 2024
- [About](#)
- [Accessibility](#)
- [User Agreement](#)
- [Privacy Policy](#)
- [Cookie Policy](#)
- [Copyright Policy](#)
- [Brand Policy](#)
- [Guest Controls](#)
- [Community Guidelines](#)

- - العربية (Arabic)
 - বাংলা (Bangla)
 - Čeština (Czech)
 - Dansk (Danish)
 - Deutsch (German)
 - Ελληνικά (Greek)
 - **English (English)**
 - Español (Spanish)
 - فارسی (Persian)
 - Suomi (Finnish)
 - Français (French)
 - हिंदी (Hindi)

- Magyar (Hungarian)
- Bahasa Indonesia (Indonesian)
- Italiano (Italian)
- עברית (Hebrew)
- 日本語 (Japanese)
- 한국어 (Korean)
- मराठी (Marathi)
- Bahasa Malaysia (Malay)
- Nederlands (Dutch)
- Norsk (Norwegian)
- ਪੰਜਾਬੀ (Punjabi)
- Polski (Polish)
- Português (Portuguese)
- Română (Romanian)
- Русский (Russian)
- Svenska (Swedish)
- తెలుగు (Telugu)
- ภาษาไทย (Thai)
- Tagalog (Tagalog)
- Türkçe (Turkish)
- Українська (Ukrainian)
- Tiếng Việt (Vietnamese)
- 简体中文 (Chinese (Simplified))
- 正體中文 (Chinese (Traditional))

Language



Sign in to view more content

Create your free account or sign in to continue your search

Sign in



Welcome back

Email or phone

Password

Show

[Forgot password?](#)

or

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

New to LinkedIn? [Join now](#)

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

Never miss a beat on the app

Don't have the app? Get it in the Microsoft Store.

[Open the app](#) 