NotCarbanak Mystery - Source Code Leak

Published: 2018-07-11 · Archived: 2026-04-05 14:46:25 UTC

I got a tip a very short time ago in our slack group about possible Carbanak source code leak. A quick google search proven this is indeed a possibility.

hxxp://mal4all.com/showthread.php?tid=494&action=lastpost

Here is the source code in a zip file.

Please make sure you use proper security steps such as sandbox and isolated environment. The origin of this zip files is unknown and was not inspected for booby traps etc.

This file was uploaded for research and defense purpose only. If you plan to use this for malicious reasons you suck.

Pass: f1Up$zD%QY*p5@!&

If you are creating any signatures such as Yara and Snort please share back with the community.

Happy Researching

My team at Minerva have organized the information into a single blog post:

> Initial analysis and insights about the enhanced #Buhtrap source code #leak (not #carbanak) https://t.co/b4hCMmc5fp
>
> — Minerva Labs (@MinervaLabs) July 12, 2018

Some on-going updates posted during the initial investigation:

> the #carbanak leak seems to have full AD dump of several banks such as:
> Kazan-based Energobank pic.twitter.com/NpHKdGd35G
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> And of course, Enums visible machines in current or any specified domain
> pic.twitter.com/KD0bFGCSD1
>
> — Bryan (@bry_campbell) July 11, 2018

> Somebody leaked the Carbanak source code last week
>
> I've been talking with several security researchers who are currently trying to verify the code's authenticity and they believe it to be the real thing, albeit they're not 100% sure just yet

> pic.twitter.com/8sAUHPEgnv
>
> — Catalin Cimpanu (@campuscodi) July 11, 2018

> Here's a video of the arrest: https://t.co/vzKhroTYFt
>
> — Catalin Cimpanu (@campuscodi) July 11, 2018
