NotCarbanak Mystery - Source Code Leak


malware-research.org/carbanak-source-code-leaked/

GelosSnake July 11, 2018

11 Jul 2018
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:

> I wouldn't put a solid carbanak tag on it just yet :) it sure has similarities...
>
> — Denis O'Brien (@Malwageddon) July 11, 2018

> after deeper look into Ratopak we should say - it is not original Buhtrap but Pegasus. Pegasus and Buhtrap have very similar TTP. So, Ratopak is the right shot here.
>
> — codelancer (@codelancer) July 11, 2018

> Comodo signed binaries from this #carbanak leak (CN="\"Allegro\" LLC", O="\"Allegro\" LLC", STREET="Nagatinsky 2ND, 2,2", L=Moscow, ST=Moscow, OID.2.5.4.17=115487, C=RU) leads to this attack on Russian banks:https://t.co/LTbCr8CVu6https://t.co/gmcw2xk76H
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> At least some parts of the source code leak fit to Buhtrap/Ratopak (f4ae5579930f20ccc41d1f8b1e417e87) code as described here: https://t.co/zkcv05OaEC #carbanak #buhtrap #ratopak pic.twitter.com/rqQrzIxFJF
>
> — Daniel Plohmann (@push_pnx) July 11, 2018

> Ok just clarifying this is leak is not #Carbanak leak as the source zip states. Its leak from #RatoPak group.
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> Probably why this group was called Pegasus before the leak: pic.twitter.com/nySAMXek6o
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> This potential #Carbanak code is very well documented. Example from the lateral movement section. pic.twitter.com/DD8e5cFI5V
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> Funny, comment: decryption of svchost will trigger @kaspersky KIS emulator. pic.twitter.com/gQ5P4DtlSb
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> Interesting information related to banking fraud on the potential #carbanak leak. pic.twitter.com/kzZxi0hWzq
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> 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

> Also the #carbanak leak seems to have a step by step guide to use/hack swift. Can anyone experience with #swift confirm this? pic.twitter.com/9N3zgJvNCM
>
> — 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

> Are you wondering why the leaked #carbanak zip files are named after @groupib ? Well they are the firs to discover #carbanak which was named Anunak by them. Also been actively working against the hacker group for many years. pic.twitter.com/UobwEj0SWK
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> Some of the leaked files are corresponding to banks hacked by #Corkow group. Really interesting: https://t.co/OHeGTg7f2E
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> This #RatoPak / (not) #Carbanak leak investigation and discussions really shows once again how difficult attribution can be and why security researchers should collaborate as much as possible. Long night a head of us (:
>
> — Omri Moyal (@GelosSnake) July 11, 2018

> Nice admin panel you've got there :) its #notcarbanak but #ratopak according to @GelosSnake and @codelancer pic.twitter.com/yUjbygZ9Yf
>
> — rik (@rikvduijn) July 11, 2018

> Confirmed Link: '#Pegasus' shares some code lib struct with #Buhtrap and appears to be an improved/altered version of the leaked Buhtrap main 'lib' (machineid, mem, etc.) 🤔 h/t @push_pnx for lead
>
> Exact Code Overlap:
>
> buhtrap/11. DLL Side-Loading+panel/.../libs/ -> pegasus/inc/ pic.twitter.com/NIvcD7ecLO
>
> — Vitali Kremez (@VK_Intel) July 11, 2018

> List of bank possibly hacked and found in the leak:
> AK BARS Bank
> IBSP Bank
> acropol
> genbank
> icbru
> interprombank
> metallinvestbank
> minbank
> nevskybank
> nipbank
>
> — Omri Moyal (@GelosSnake) July 11, 2018