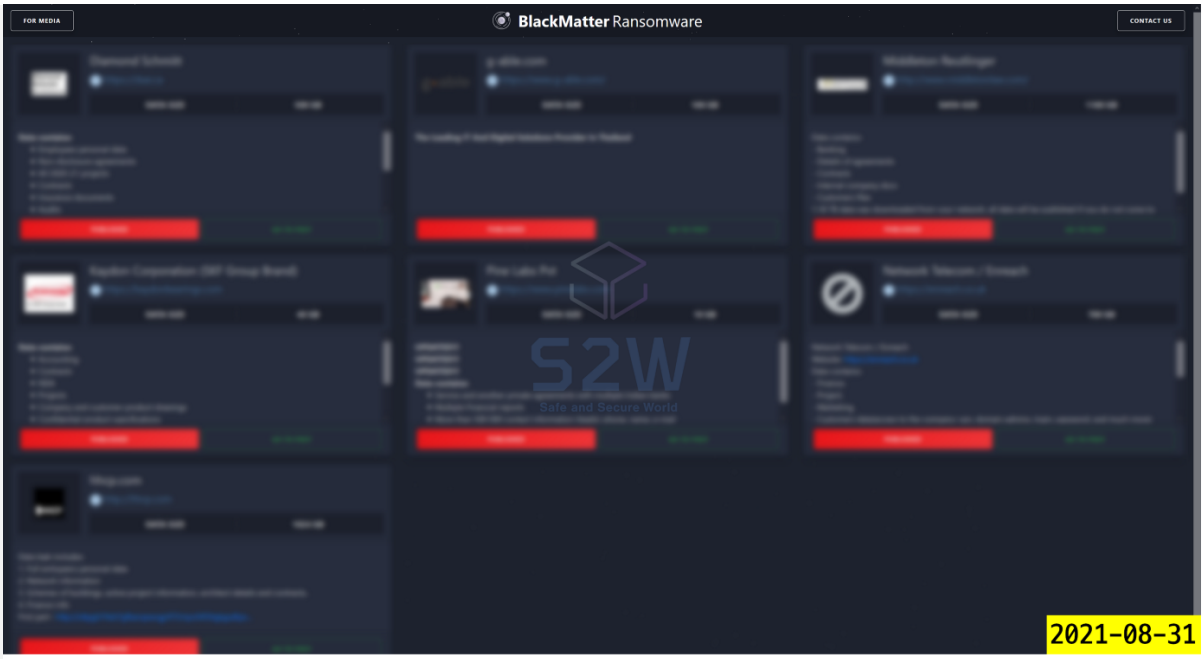
BlackMatter x Babuk : Using the same web server for sharing leaked files

Abstract

BlackMatter published the leaked files and documents related to infected victim companies started on August 1, 2021. They published the leaked data of 7 infected victim companies on their leak site.

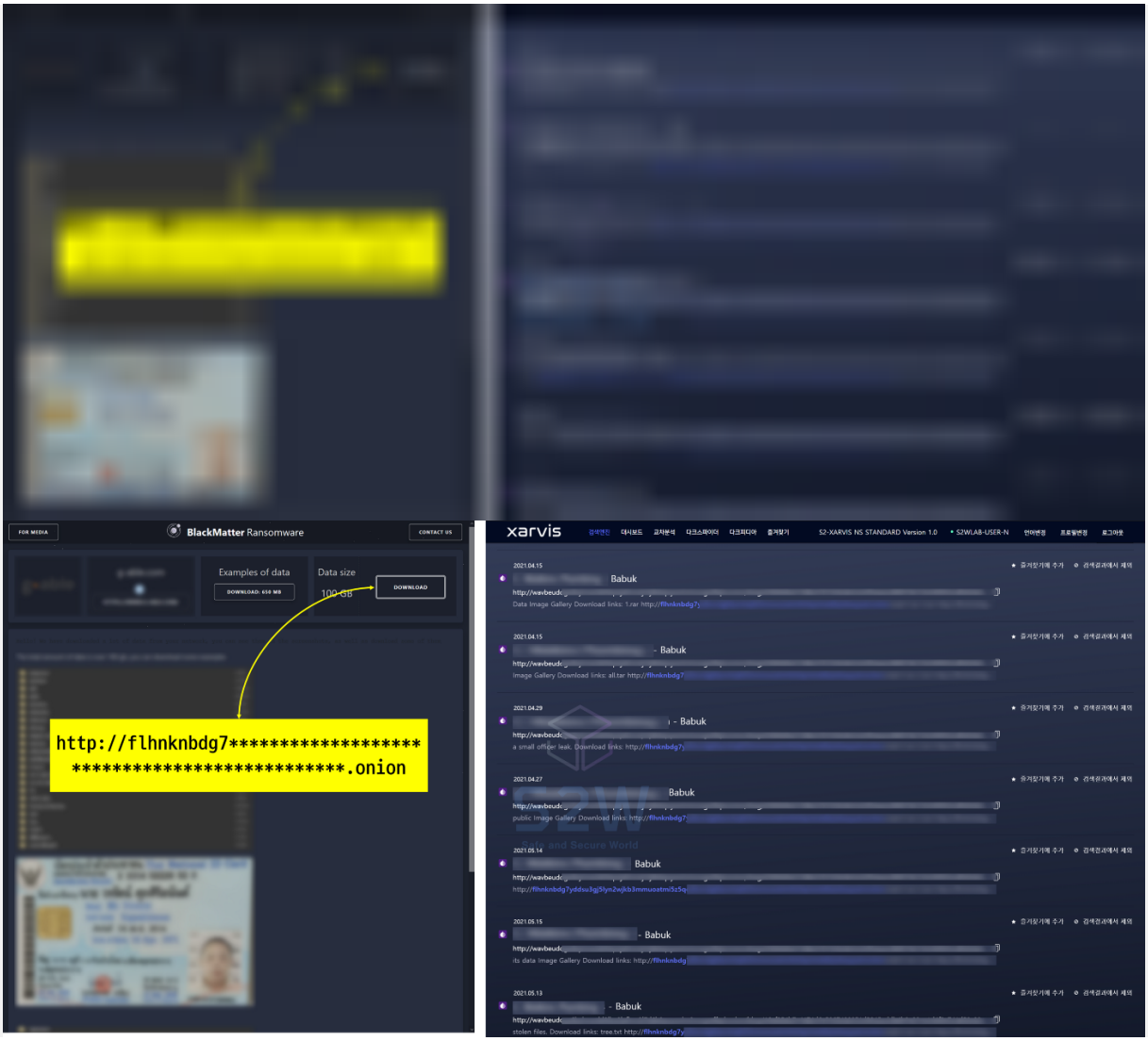


BlackMatter using file hosting services

BlackMatter is using the file hosting services on their leak site and they are not uploaded the leaked data on their own web server. We checked BlackMatter used Mega Cloud, PrivatLab, DropmeFiles, 2 Tor Web Servers on their leak site.

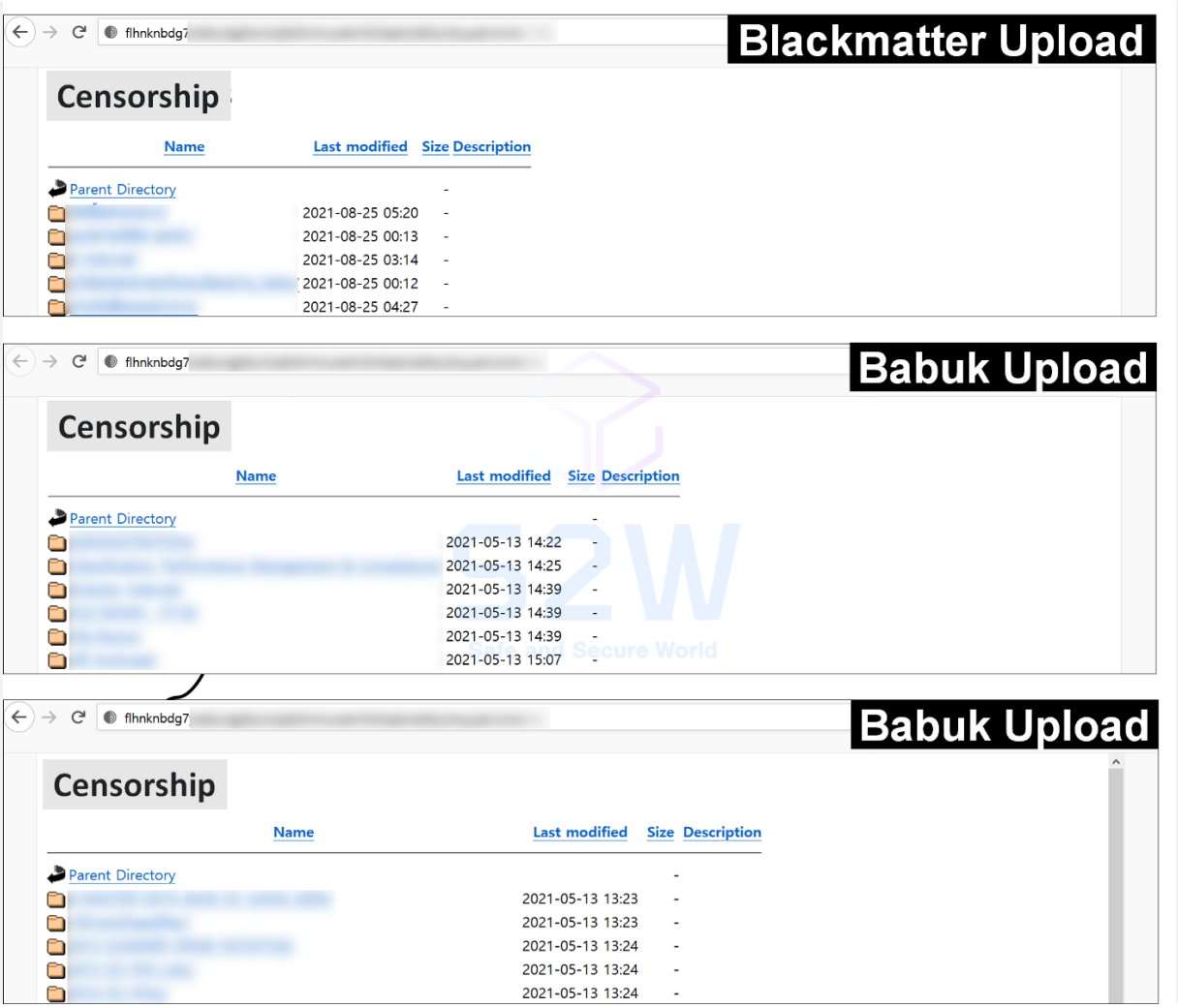
BlackMatter x Babuk : Using the same web server for sharing leaked files

The interesting point is a Tor Web Server(http://flhnknbdg7****.onion) is the same as Babuk's file server when they share the leaked files with users.



The leaked data uploaded to the same web server by BlackMatter and Babuk

In the file server of BlackMatter, we checked the leaked data uploaded by Babuk and BlackMatter as below:



The string was changed on August 28, 2021

(Previous title) 2021–05–31 BABUK STRONAGE SERVER, Joe Biden Caprophile

(Current title) 2021–08–28 GROVE STRONAGE SERVER

When Babuk uses this web server for sharing the leaked files, if we enter the root directory of the web server, we can see the string of BABUK STRONAGE SERVER, Joe Biden Caprophile. But now, the title of the web server changed the string to GROVE STRONAGE SERVER.

Conclusion

- In this post, we mentioned the fact of BlackMatter and Babuk using the same web server for sharing the leaked files.

- We could not find any pieces of the evidence whether they are in the same group.
- They may have accidentally rented the same web server, or we need to keep monitoring their activities to track the relation between BlackMatter and Babuk.