Introduction

Over the past month a new ransomware group, named Black Basta, has emerged and has quickly gained popularity.

As 29 victims have already been added to Black Basta's victim list, the group is drawing the attention of security researchers and hunters in the cybersecurity community worldwide.

In the era of post-ContiLeaks ransomware groups are looking to utilize and base their product on the fairly successful Conti code. With several families recently emerging, the big question is whether we are witnessing the rise of another copycat, or is a Conti faction gaining its independence.

Victimology

As they expand their operations and victim list, it seems that Black Basta is focusing on the industrial and retail sectors (Figure 1).

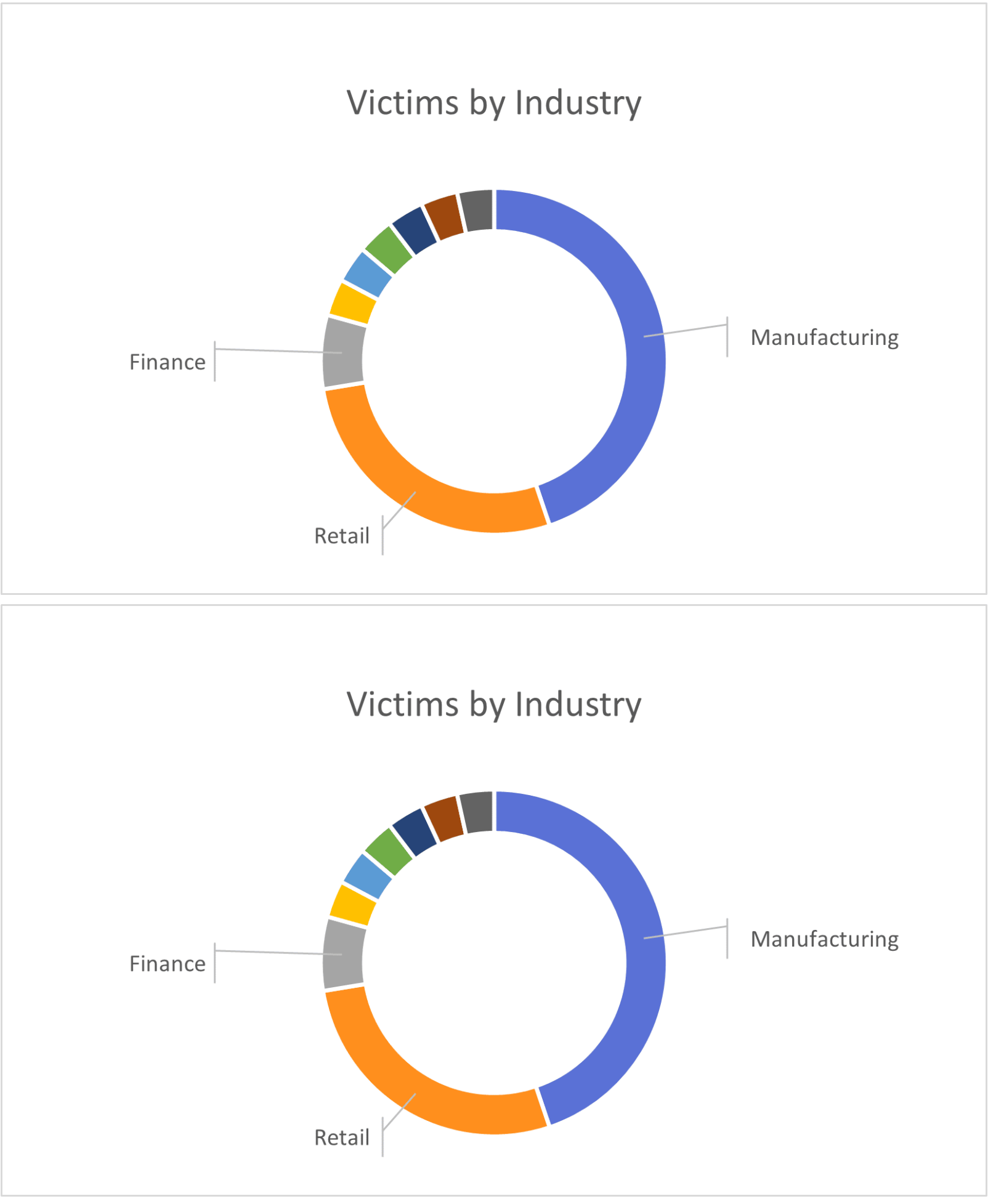


Figure 1:Black Basta victim's distribution by industry

As suspected, and commonly typical for ransomware groups, the group targets organizations in the United States and powerful Europe nations such as Germany (Figure 2) — countries favored by threat groups given the financial opportunities.

Black Basta victims distribution by country

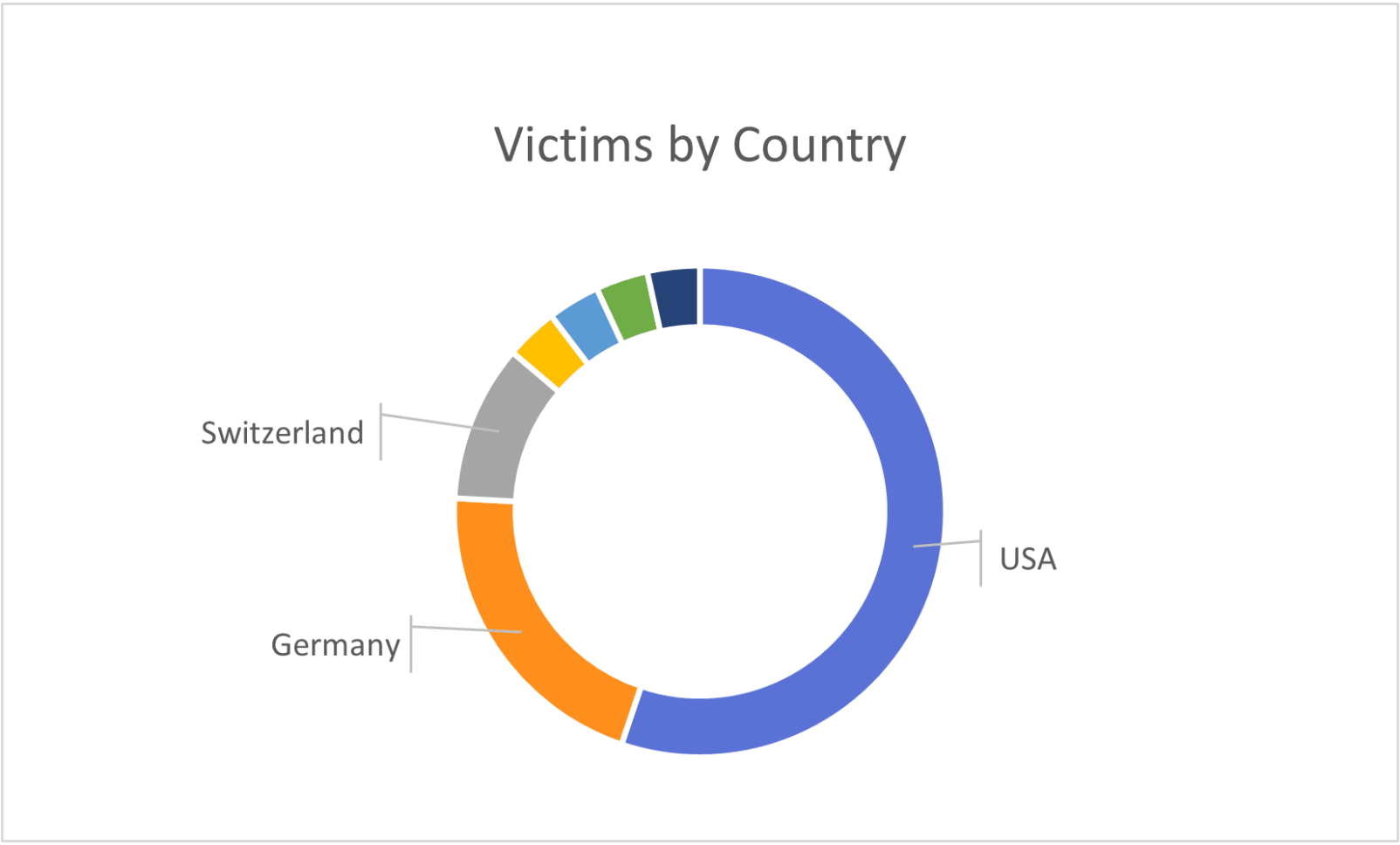


Figure 2: Black Basta victims distribution by country

Delivery

The delivery methods of ransomware groups vary depending on the potential victim's exploitability. Focusing on Black Basta, we see two main delivery methods.

Malspam

As is common with threats of this nature, the initial delivery method is the delivery of email lures masquerading as legitimate business communications that encourage the recipient to open an attachment.

Based on an analysis of a recent campaign, observed lure themes include content relating to urgent or pressing matters such as 'new orders', 'payments' and 'quotations', as well as the apparent reuse of prior legitimate email threads that include contact details for, and mimic, an unwitting third-party.

Insider Threat

While malspam campaigns are still the most common method used by most ransomware groups, Black Basta included, the group looks for other "leads" on darknet forums.

The insider threat is becoming a legitimate delivery method ransomware groups use for two main reasons: The first is the convenience and how it makes things way easier for the group as they can deploy their ransomware and steal data without the hassle of infecting machines and escalating privileges while staying silent. The second is that although we don't have specific cases for which we know for sure a deal was made, the fact that many ransomware groups publicly announce they would like to bribe insiders to "let them in" means this method works, and it works well. As they try to lure insiders by leveraging their greed, Black Basta has been observed on several Darknet forums offering to buy access from organizations' employees (Figure 3).

Black Basta offers to buy access from employees in underground forum

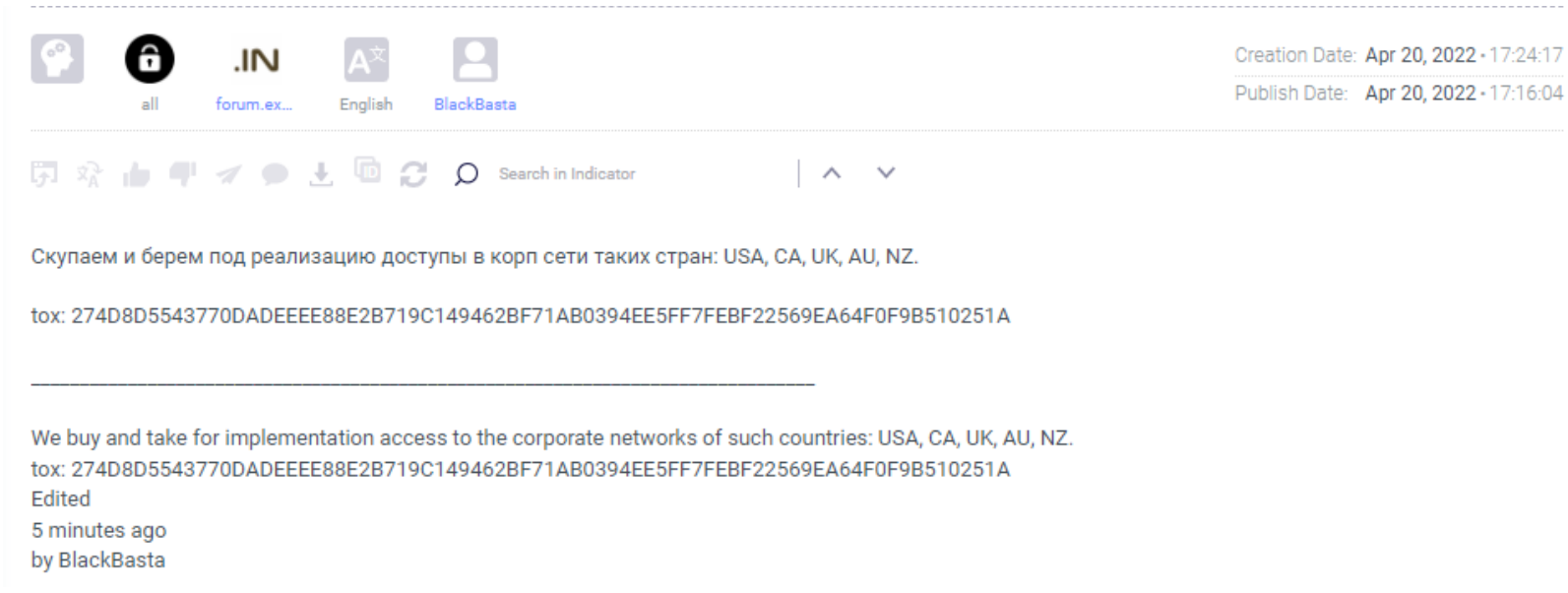


Figure 3: Black Basta offers to buy access from employees in underground forum

Technical Analysis

Recovery Services Deletion

Like many other threat groups and malware families, Black Basta's first step in the victim's machine is deleting shadow copies using the `vssadmin.exe` (Figure 4).

command line Black Basta module uses to delete shadow files

```
C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet
C:\Windows\System32\vssadmin.exe delete shadows /all /quiet
```

Figure 4: Command line Black Basta module uses to delete shadow files

Deleting shadow copies in the OS usually means the victims can't recover the files that have been encrypted. This puts more pressure on them to pay the ransom as fast as possible in order to get the company back on track as soon as possible.

Desktop Background Modification

Another change in the OS that the encryption module does is to modify the Desktop's background to a one created by the group explaining to the victims that they are compromised (Figure 5). First, the sample drops the file named dlaksjdoiwq.jpg to the %TEMP% directory. Then, it modifies the background using the SystemParametersInfoW API call.

Black Basta Desktop background

Figure 5: Black Basta Desktop background

Persistence

There are many techniques to achieve persistence within the victim's machine. Black Basta gains persistence through hijacking the Fax service within Windows by deleting the service and installing a new one pointing to the Black Basta sample.

Defense Bypass

At this point, Black Basta was able to gain persistence and sabotage the backup services. In order for them to advance to the encryption phase, defense mechanisms bypass is required.

Black Basta's chosen technique to do so is to restart the victim's machine in safe mode, thus making the encryption phase easier and uninterrupted by the various defense services.

Encryption

Like other ransomware groups, the encryption phase consists of the iteration of all the files in the victim's machine, excluding some files that are essential for the OS to keep operating, for example, the readme files, Recycle Bin, and the Desktop wallpaper Black Basta drop.

All the encrypted files get the .basta file extension and their icons are changed to the customized one that Black Basta created (Figure 6, 7).

Encrypted files icon added to the Windows registries

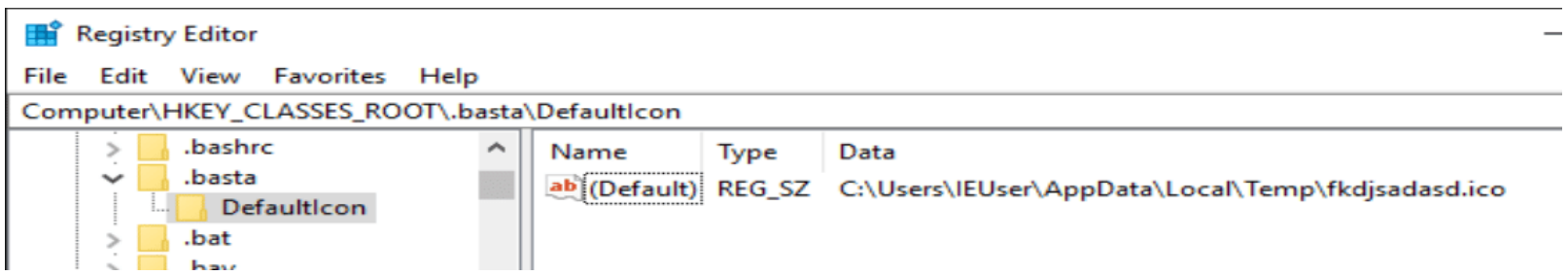


Figure 6: Encrypted files icon added to the Windows registries

Black Basta encrypted files

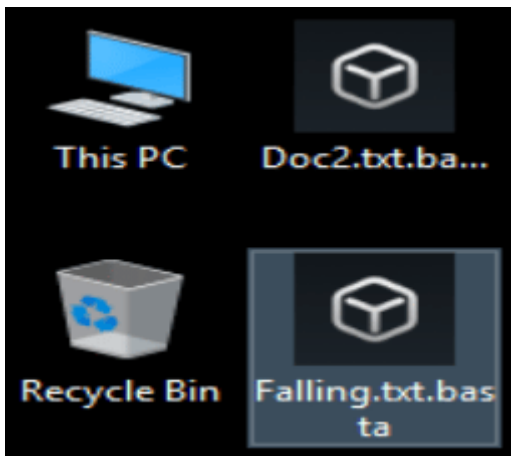
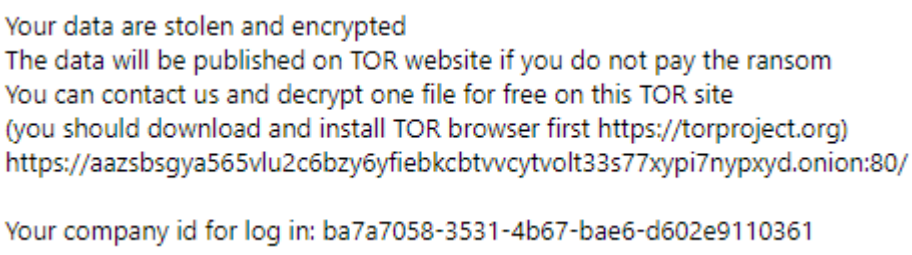


Figure 7: Black Basta encrypted files

Ransom Note

The Black Basta encryption module also generates Readme.txt files on multiple locations in the OS. Each contains a short explanation of what happened (Figure 8) along with the address of the group's Onion page and the victim's ID, which is needed in order to negotiate.



Black Basta ransom note

Figure 8: Black Basta ransom note

Negotiation

Once compromised, each victim receives a victim ID in their ransom note.

On Black Basta's Onion page, they have a negotiation section, which victims access using the victim ID they received (Figure 9)

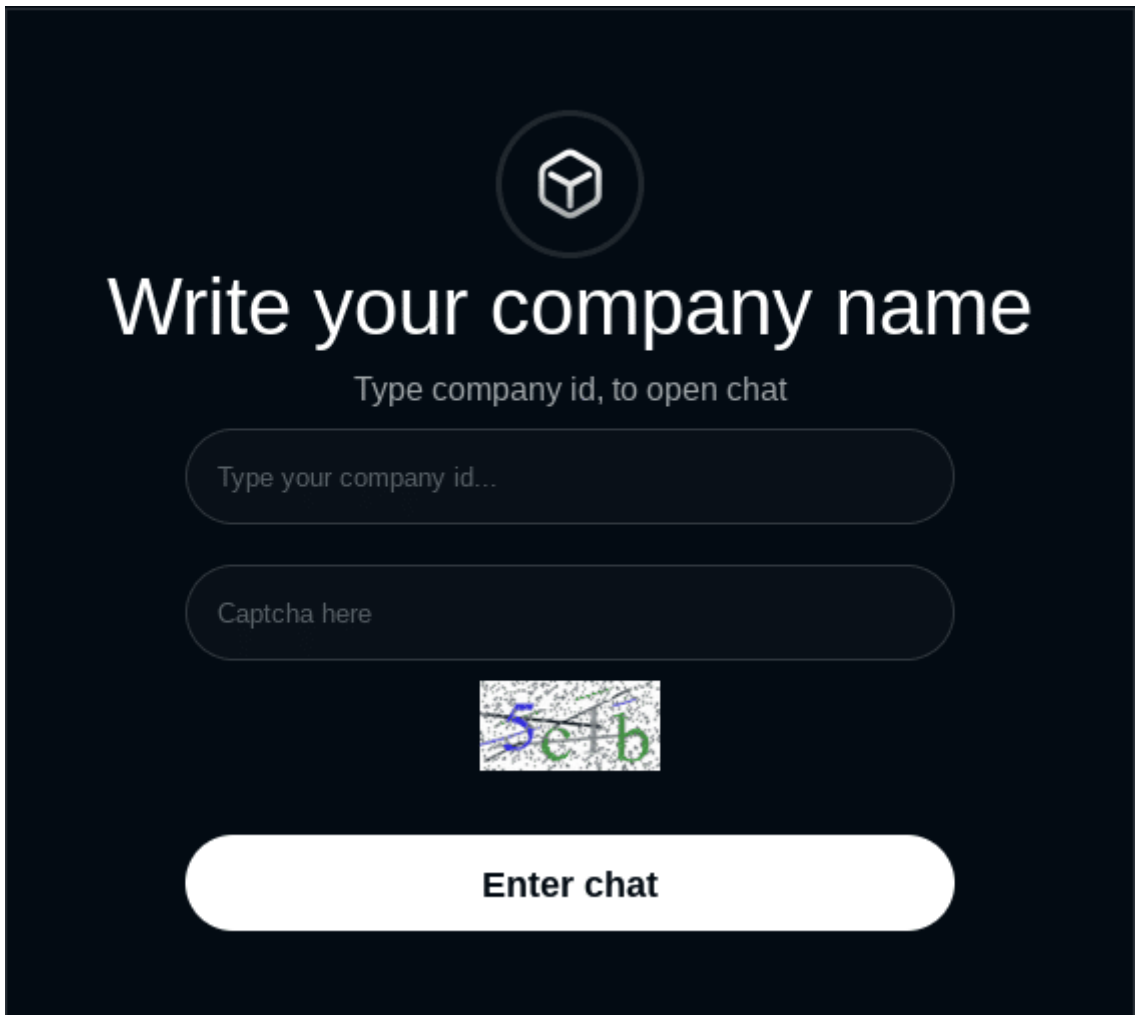


Figure 9: Black Basta negotiation landing page

Conti Relations?

Ever since Black Basta emerged, there was initially much speculation that they are a rebrand of Conti, or a faction of Conti that went rogue or opened their own group.

The assumption that Black Basta was related in any way is due to some similarities in the websites of the two groups. The Cyberint Research Team is not convinced these similarities are enough to determine that one group is connected to another. However, we cannot deny that some members might know each other from past experience, given the mutual origin of the groups.

These speculations became mainstream until a ransomware sample from February 17 (prior to the ContiLeaks incident), generating a ransom note with a group named “no_name_software” taking responsibility for the ransomware (Figure 10), was revealed.

Ransom note found on February with the same Onion site Black Basta use today

```
===============
Feb 17 01:46:11 2022 -> 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90
===============
All of your files are currently encrypted by no_name_software.

These files cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery software) can damage your files. However,
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and initiate the publication of whole compromised data immediately.

DON'T move or rename your files. These parameters can be used for encryption/decryption process.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80/

Your company id for log in: {ID}
Your company key: 3 of any of your dc through comma. Example: "DC1, DC2, DC3". You can type less if you have no enough

YOU SHOULD BE AWARE!
We will speak only with an authorized person. It can be the CEO, top management, etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!
Inform your supervisors and stay calm
```

Figure 10: Ransom note found on February with the same Onion site Black Basta use today

This sample is very important in refuting the link with Conti given the fact that the Onion page written in the ransom note is the same Onion page Black Basta currently operates.

This evidence of the group operating, or at least already developing their product in mid-February, suggest that they are not related to Conti, both personally or technically.

Conti’s Response

As these new groups emerge by the day, the cyber security community tends to immediately link them to Conti.

This situation often places Conti in a bad light as a weak group that both cannot recover from ContiLeaks and cannot retain their affiliates.

As part of the “For Peru” campaign Conti conducted, in one of their announcements they rejected the allegations that Black Basta is part of their organization or connected to them (Figure 11). Although the announcement regarding Black Basta seems very random in a post related to Peru, Conti stands behind this statement.

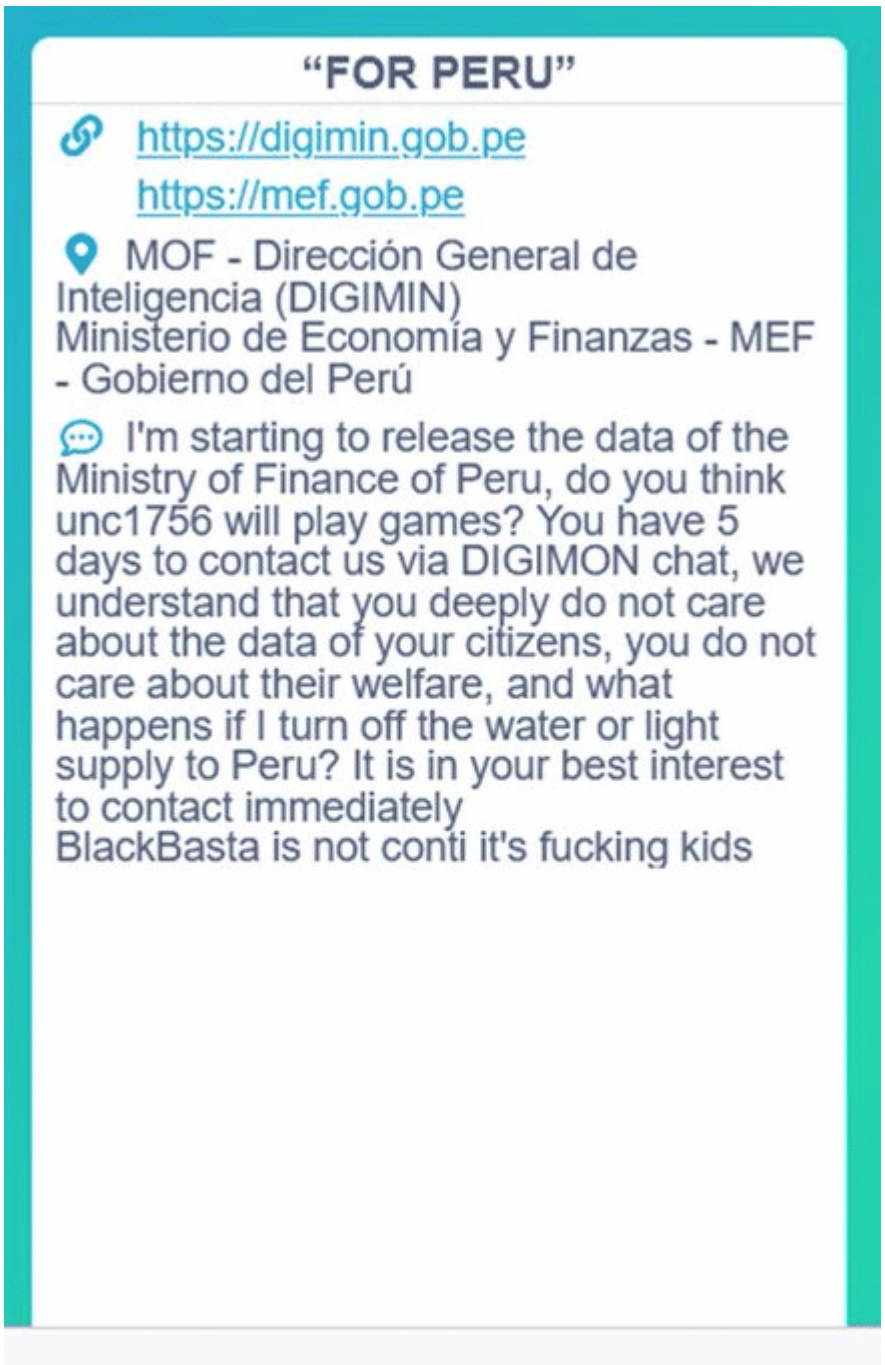


Figure 11: Conti’s response to being related to Black Basta

Figure 11: Conti’s response to being related to Black Basta

Conclusion

As we reach the end of the first half of 2022, we have counted many new groups that were introduced to the ransomware industry. However, most of them vanish due to inconsistency in their campaigns or poor OpSec, which leads them to go off-grid fairly quickly after they are launched.

Black Basta looks like one of the more “promising” groups that is here to stay. Much like AvosLocker of the past year, they display the same consistency and ambition.

In addition, the fact that a veteran such as Conti addresses them in their blog, along with the speculations around their connection, is also somewhat of an indicator of their popularity and talent.

Although the group is new, examining their samples didn’t provide any technical breakthroughs or other special TTPs.

As mentioned, the ransomware industry greatly rewards those who know how to remain consistent, bold and anonymous, and it seems that BlackBasta embodies these characteristics. This might result them becoming another notorious group in our lives for the rest of the year.

Want to speak to our experts? Contact us!