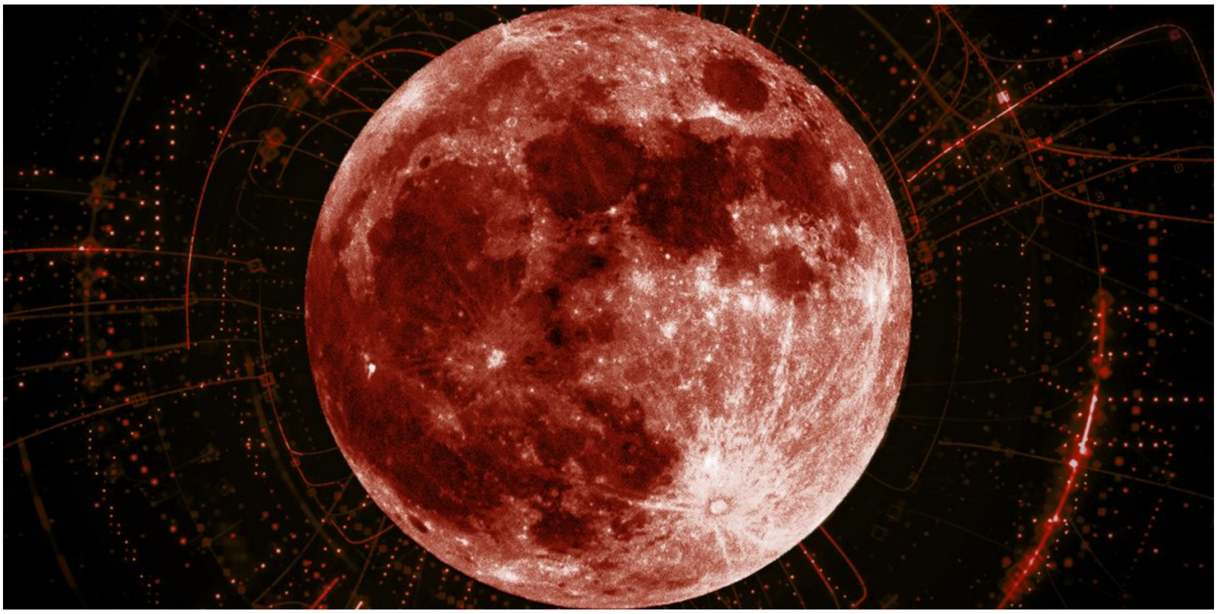
Luna and Black Basta — new ransomware for Windows, Linux and ESXi



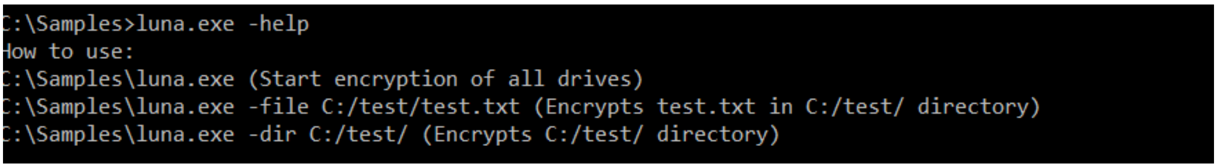
Introduction

In our crimeware reporting service, we analyze the latest crime-related trends we come across. If we look back at what we covered last month, we will see that ransomware (surprise, surprise!) definitely stands out. In this blog post, we provide several excerpts from last month's reports on new ransomware strains.

Luna: brand-new ransomware written in Rust

Last month, our Darknet Threat Intelligence active monitoring system notified us of a new advertisement on a darknet ransomware forum.

As one can see from the advertisement, the malware is written in Rust and runs on Windows, Linux and ESXi systems. Armed with this knowledge, we went hunting for samples, finding a few via the Kaspersky Security Network (KSN).



```
C:\Samples>luna.exe -help
How to use:
C:\Samples\luna.exe (Start encryption of all drives)
C:\Samples\luna.exe -file C:/test/test.txt (Encrypts test.txt in C:/test/ directory)
C:\Samples\luna.exe -dir C:/test/ (Encrypts C:/test/ directory)
```

Command line options available in Luna

Judging by the command line options available, Luna is fairly simple. The encryption scheme it uses, however, is not so typical, as it involves x25519 and AES, a combination not often encountered in ransomware schemes.

Both the Linux and ESXi samples are compiled using the same source code with some minor changes from the Windows version. For example, if the Linux samples are executed without command line arguments, they will not run. Instead, they will display available arguments that can be used. The rest of the code has no significant changes from the Windows version.

The advertisement states that Luna only works with Russian-speaking affiliates. Also, the ransom note hardcoded inside the binary contains spelling mistakes. For example, it says “a little team” instead of “a small team”. Because of this, we assume with medium confidence that the actors behind Luna are speakers of Russian. Since Luna is a freshly discovered group, there is still little data on its victimology, but we at Kaspersky are following Luna’s activity.

Luna confirms the trend for cross-platform ransomware: current ransomware gangs rely heavily on languages like Golang and Rust. A notable example includes BlackCat and Hive. The languages being platform agnostic, the ransomware written in these can be easily ported from one platform to others, and thus, attacks can target different operating systems at once. In addition to that, cross-platform languages help to evade static analysis.

Black Basta

Black Basta is a relatively new ransomware variant written in C++ which first came to light in February 2022. The malware, the infrastructure and the campaign were still in development mode at the time. For example, the victim blog was not online yet, but the Black Basta website was already available to victims.

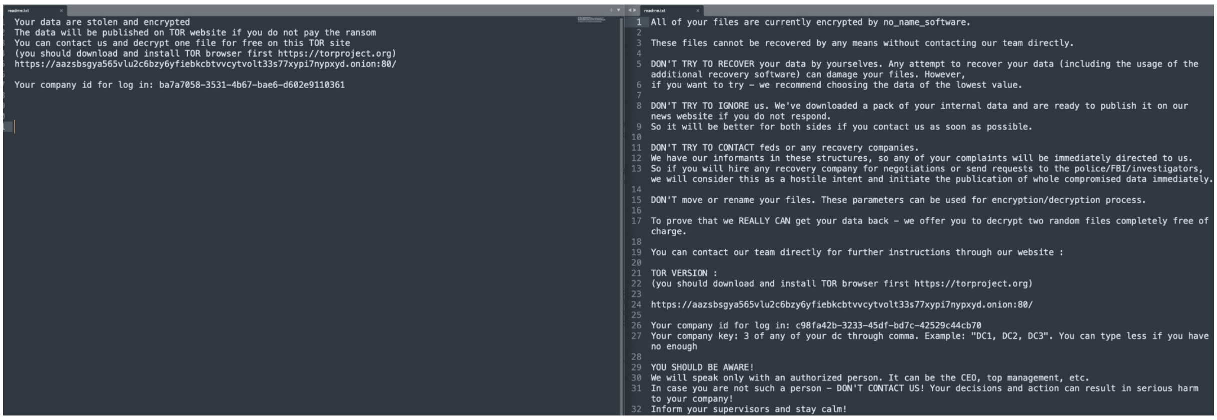
Black Basta supports the command line argument “-forcepath” that is used to encrypt only files in a specified directory. Otherwise, the entire system, with the exception of certain critical directories, is encrypted.

Two months after the first encounter, in April, the ransomware had grown more mature. New functionality included starting up the system in safe mode before encryption and mimicking Windows Services for persistence reasons.

The safe-mode reboot functionality is not something we come across every day, even though it has its advantages. For example, some endpoint solutions do not run in safe mode, meaning the ransomware will not be detected and files in the system can be “easily” encrypted. In order to start in safe mode, the ransomware executes the following commands:

- C:\Windows\SysNative\bcdedit /set safeboot networkChanges
- C:\Windows\System32\bcdedit /set safeboot networkChanges

Earlier versions of Black Basta contained a different rescue note from the one currently used, which showed similarities to the ransom note used by Conti. This is not as odd as it may seem, because Black Basta was still in development mode at the time.

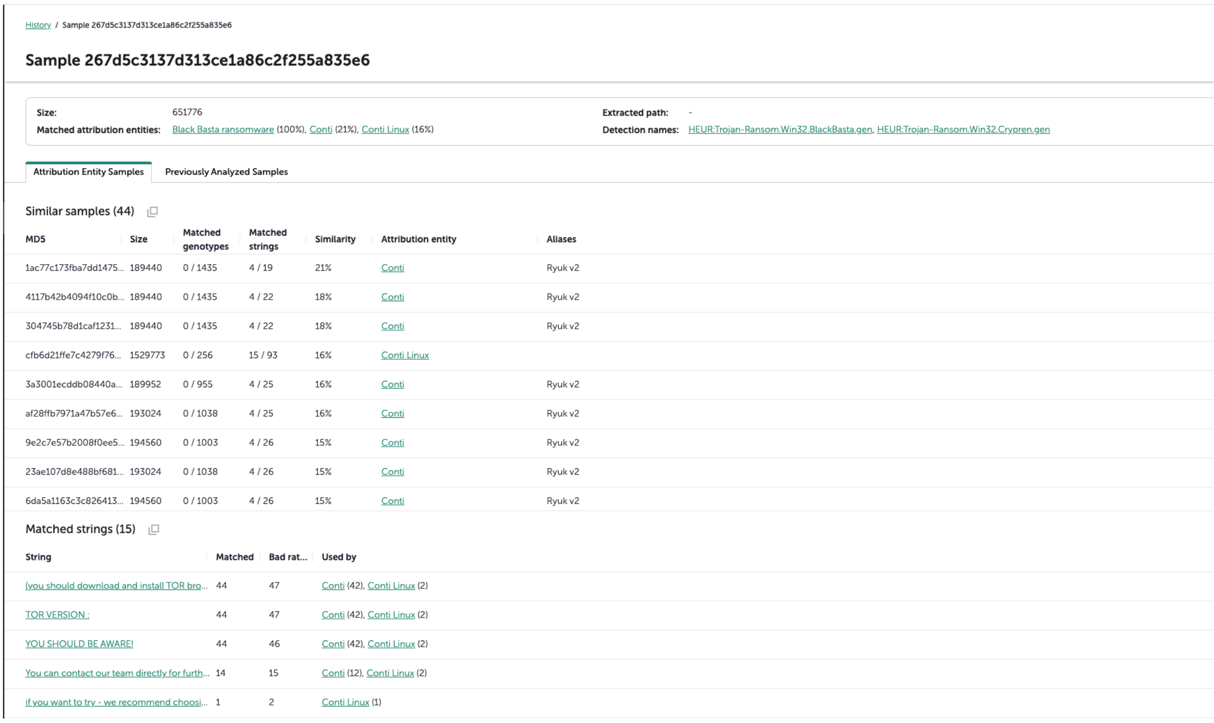


```
Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
You can contact us and decrypt one file for free on this TOR site
(you should download and install TOR browser first https://torproject.org)
https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80/

Your company id for log in: ba7a7058-3531-4b67-bae6-d602e9110361
```

```
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: c98fa42b-3233-45df-bd7c-42529c44cb70
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!
```

Rescue notes comparison

To ascertain that there was indeed no code overlap between Conti and the earlier versions of Black Basta, we fed a few samples to the Kaspersky Threat Attribution Engine (KTAE). Indeed, as shown below, only the strings overlap. There is thus no overlap in code per se.


History / Sample 267d5c3137d313ce1a86c2f255a835e6
Attribution Entity Samples
Previously Analyzed Samples

Sample 267d5c3137d313ce1a86c2f255a835e6

Size: 651776
Matched attribution entities: Black Basta ransomware (100%), Conti (21%), Conti Linux (16%)
Extracted path: -
Detection names: HEUR:Trojan-Ransom.Win32.BlackBasta.gen, HEUR:Trojan-Ransom.Win32.Crypren.gen

Similar samples (44)

MD5	Size	Matched genotypes	Matched strings	Similarity	Attribution entity	Aliases
1ac77c173fba7dd1475...	189440	0 / 1435	4 / 19	21%	Conti	Ryuk v2
4117b42b4094f10c0b...	189440	0 / 1435	4 / 22	18%	Conti	Ryuk v2
304745b78d1caf1231...	189440	0 / 1435	4 / 22	18%	Conti	Ryuk v2
cfb6d21ffe7c4279f76...	1529773	0 / 256	15 / 93	16%	Conti Linux	
3a3001ecddb08440a...	189952	0 / 955	4 / 25	16%	Conti	Ryuk v2
af28ffb7971a47b57e6...	193024	0 / 1038	4 / 25	16%	Conti	Ryuk v2
9e2c7e57b2008f0ee5...	194560	0 / 1003	4 / 26	15%	Conti	Ryuk v2
23ae107d8e488bf681...	193024	0 / 1038	4 / 26	15%	Conti	Ryuk v2
6da5a1163c3c826413...	194560	0 / 1003	4 / 26	15%	Conti	Ryuk v2

Matched strings (15)

String	Matched	Bad rat...	Used by
(you should download and install TOR bro...	44	47	Conti (42), Conti Linux (2)
TOR VERSION :	44	47	Conti (42), Conti Linux (2)
YOU SHOULD BE AWARE!	44	46	Conti (42), Conti Linux (2)
You can contact our team directly for furth...	14	15	Conti (12), Conti Linux (2)
if you want to try - we recommend choosi...	1	2	Conti Linux (1)

Overlap with Conti ransomware

Black Basta for Linux

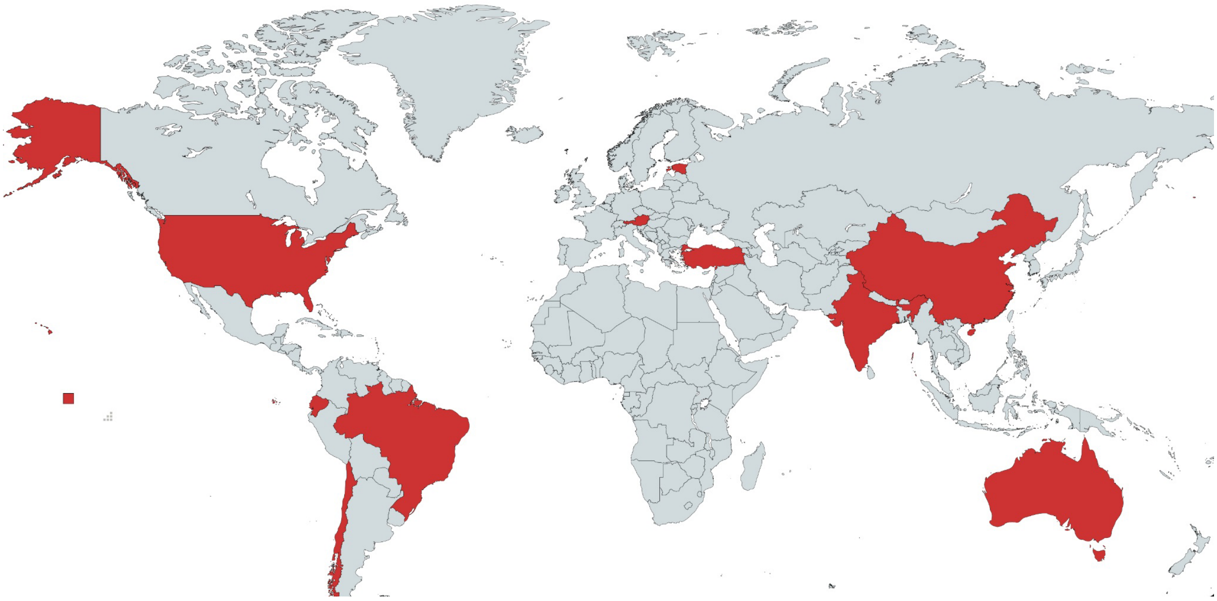
In another report we wrote last month, we discussed the Black Basta version for Linux. It was specifically designed to target ESXi systems, but it could be used for general encryption of Linux systems as well, although that would be a bit cumbersome.

Just like the version for Windows, the Linux version supports only one command line argument: “-forcepath”. When it is used, only the specified directory is encrypted. If no arguments are given, the “/vmfs/volumes” folder is encrypted.

The encryption scheme for this version uses ChaCha20 and multithreading to speed up the encryption process with the help of different processors in the system. Given that ESXi environments typically use multiple CPUs to execute a VM farm, the malware’s design, including the chosen encryption algorithm, allows the operator to have the environment encrypted as soon as possible. Prior to encrypting a file, Black Basta uses the *chmod* command to get access to it in the same context as the user level.

Black Basta targets

Analysis of the victims posted by the Black Basta group revealed that to date, the group has managed to attack more than forty different victims within a very short time it had available. The victim blog showed that various business sectors were affected including manufacturing, electronics, contractors, etc. Based on our telemetry, we could see other hits across Europe, Asia and the United States.



Conclusion

Ransomware remains a big problem for today’s society. As soon as some families come off the stage, others take their place. For this reason, it is important to stay on top of all developments in the ransomware ecosystem, so one can take appropriate measures to protect the infrastructure.

A trend, which we also discussed in our previous blog post, is that ESXi systems are increasingly targeted. The aim is to cause as much damage as possible. Luna and Black Basta are no exceptions. We expect that new variants will support encryption of VMs by default as well.