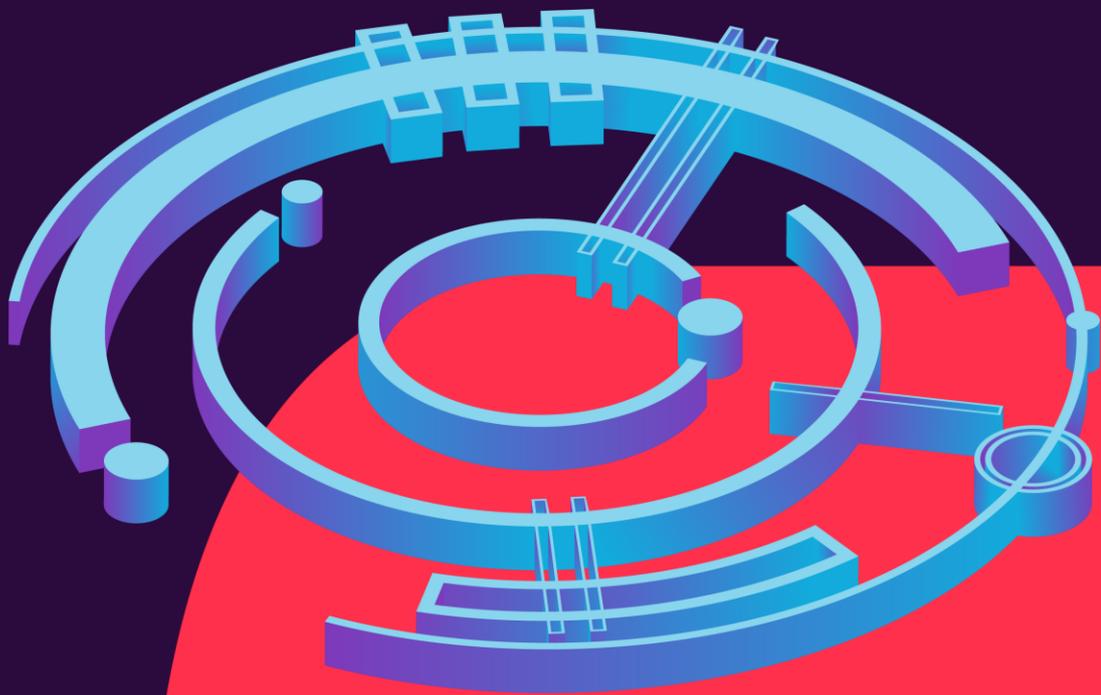


# CyberSeChronicles



# Context

**CyberseChronicles** aims at putting the spotlight on **emerging groups/malwares** that pose a serious threat to many organizations. For this reason, we share with the cybersecurity community a thorough **analysis** gathered by combining efforts of our specialized teams of the Sogeti CERT ESEC (Threat Intelligence, Incident Response/SWAT, Purple and the Security Operation Center), and this, as frequently as possible upon a year. The shared content (TLP:GREEN; Limited disclosure, restricted to the cybersecurity community)<sup>1</sup> shall be deemed as proprietary and privileged information and cannot be used as admissible proof before legal authorities.

This New Year's double extortion ransomware evolution landscape started with a peculiar specimen dubbed **Babuk**. The latter was put in the spotlight as its operators hit several corporations in a relative short range of time amongst which, the prominent global government outsourcer Serco exhibiting a revenue of over £ bn in 2019 and being behind NHS Test and Trace.

The **Sogeti CERT ESEC** Threat Intelligence (CETI) team thought that Babuk would be a textbook case for our first chronicle that illustrates how quickly inexperienced threat actors can nowadays grasp from scratch the means of conducting single, double, and even towards triple extortion schemes. Even more striking is how fast Babuk' operators adopted a Ransomware-as-a-service model by recruiting affiliates from underground Russian-speaking forums.

---

<sup>1</sup> According to ENISA "sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community."

# Executive summary

In contrast with previously observed ransomware threat actors, Babuk' operators advertise in English on more visible hacking forums. This new ransomware also **lacks « kill-switches »** that is a common feature usually tailored by the top-tier ransomware ecosystem when detecting languages of the Commonwealth of Independent States (CIS) set as default.

Another peculiar trait of Babuk' operators was a message posted on their DLS (dedicated leak site) claiming that organisations or NGOs will not be attacked except those who support LGBT or Black Lives Matter (BLM). Such **conservative political statements** are uncommon for ransomware operators but could be consistent for a hacktivist group of Muslim faith as substantiated by several elements described in our analysis from 'social media intelligence'-oriented research.

Beyond already reported operational security measures errors in the Babuk codebase pinpointed by researchers, to which Babuk' operators are very attentive to, we also found **misconfigurations** of their first version of DLS. From the former observation and thanks to the support of our internal Purple Team, we could elaborate a vaccine in a credible simulated enterprise environment that demonstrated the prevention of files encryption operated by recent variants of Babuk ransomware.

# Summary

<b>Babuk ransomware</b> .....	<b>5</b>
History .....	6
Babuk Identity Card .....	8
Activity study .....	10
Babuk's name origin .....	14
Investigation on "Biba99" avatar .....	16
Attacker's motivations .....	22
Babuk's genealogy .....	24
<b>Babuk Analysis</b> .....	<b>26</b>
Protection mechanisms .....	27
OPSEC errors from Babuk's operators .....	28
Babuk's evolution .....	30
Modus operandi .....	41
<b>SecEng</b> .....	<b>42</b>
Scope .....	43
Preparation phase .....	44
Execution phase .....	45
Hunting phase .....	46
Shadow volumes .....	53
Source code of our vaccine .....	54
GPO deployment .....	56
Limitations .....	57
Acknowledgements .....	58
<b>Appendix</b> .....	<b>59</b>

1

# Babuk ransomware

# History

1.1

## Cyber Threat Intelligence

This year started with the appearance of a new ransomware dubbed Babuk, discovered by a cybersecurity researcher at McAfee Labs (known as **@Glacius\_** on Twitter). This family of ransomware joined already the recent trend of double extortion<sup>2</sup> conducted by the top-tier1 of the ransomware ecosystem and falls into the scope of big-game hunting (the process of cybercriminals focusing on high-value data or assets within businesses). The researcher **@Glacius\_** also shared this discovery in his Twitter thread on January 2, 2021 (see **Figure 1**)<sup>3</sup>.



**Figure 1**  
*Screenshot of the first  
Tweet post about  
Babuk and*

<sup>2</sup> The strategy of threatening to expose stolen information

<sup>3</sup> [https://twitter.com/Glaciuss\\_/status/1345376488506462209](https://twitter.com/Glaciuss_/status/1345376488506462209)

**@Arkbird\_SOLG**, another cybersecurity researcher posted a preliminary reverse-engineering analysis on his Twitter thread the day after<sup>4</sup>. This discovery and first analysis was then deepened and relayed the same day on the personal blog<sup>5</sup> of a Georgia Tech student named Chuong Dong,<sup>67</sup> (currently a reverse engineering intern at FireEye).

A strong similarity in the encryption process, the enumeration of files and in stopped processes was underlined 2 days later by **@Sebdraven** on his twitter thread (see **Figure 1** on the right)<sup>8</sup> as compared with the source code of publicly available Babuk' samples. The name of this new ransomware was originally "Vasa" (and not "Babuk") and used a different technique to get ransoms via an end-to-end encrypted email service to communicate with the victim (Protonmail).



**Figure 2**  
*Screenshot of  
@Sebraven's tweet  
about Babuk and Vasa*

<sup>4</sup> [https://twitter.com/arkbird\\_solg/status/1345569395725242373?s=21](https://twitter.com/arkbird_solg/status/1345569395725242373?s=21)

<sup>5</sup> <http://chuongdong.com//reverse%20engineering/2021/01/03/BabukRansomware/>

<sup>6</sup> <https://www.linkedin.com/in/chuong-dong-1012/>

<sup>7</sup> <https://twitter.com/cPeterr>

<sup>8</sup> <https://twitter.com/Sebdraven/status/1346377590525845504>

# Babuk Identity Card

1.2

## Cyber Threat Intelligence

Babuk ransomware	
<b>1st public report</b>	January 2nd 2021 <sup>9</sup>
<b>Name</b>	<i>Babuk (Locker)</i>
<b>A.k.a</b>	<i>Vasa Locker,<sup>10</sup> Babyk</i>
<b>Threat type</b>	Doxware (ransomware & exfiltration/doxing)
<b>Motivations</b>	Opportunistic actor, financial motivation
<b>Origin</b>	Russian Speaking (probability medium-high / low probability) <sup>11</sup>
<b>Affiliation probability</b>	<b>Very low</b> It should be noted that 'state ransomware' is quite marginal in the threat landscape (e.g., Pay2Key/APT33 <sup>12</sup> , VHD/APT38 <sup>13</sup> )
<b>Impact</b>	<b>High</b>
<b>Attack vector</b>	Unknown

<sup>9</sup> [https://twitter.com/Glacijs\\_/status/1345376488506462209](https://twitter.com/Glacijs_/status/1345376488506462209)

<sup>10</sup> <https://twitter.com/Sebdraven/status/1346377590525845504>

<sup>11</sup> The cybercriminal sphere operating the ransomware/doxware ecosystem is known to be tight to CIS nations. We have found one word written with Cyrillic characters "Заврузка" when on the homepage of the Babuk dedicated leak site that indicates to the visitor that the page is loading.

<sup>12</sup> <https://www.clearskysec.com/pay2kitten/>

<sup>13</sup> <https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/>

## Points of contact

<b>Forum(s)</b>	Raidforums (user : <i>biba99</i> )
<b>Doxing site</b>	<ul style="list-style-type: none"> <li>gtmx56k4hutn3ikv[.]onion</li> <li>babukq4e2p4wu4iq[.]onion</li> <li>wavbeudogz6byhnarrrdd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd[.]onion</li> </ul>
<b>Email</b>	babukrip@protonmail.ch (see PGP public key in appendix)
<b>Contact negotiation</b>	<ul style="list-style-type: none"> <li>Chat from the onion site</li> <li>By email babukrip@protonmail.ch for the <i>Vasa Locker strain</i></li> </ul>
<b>Payment</b>	<ul style="list-style-type: none"> <li>Bitcoin via their own chat on the doxing site</li> </ul>

## Executable's data of interest

<b>Type</b>	PE32 executable 32bits, not packed
<b>Extension after encryption</b>	. __NIST_K571__ .babyk .babuk2
<b>Stopped Services</b>	memtas, mepocs, sophos, veeam, backup, GxVss, GxBlr, GxFWD, GxCVD, GxCIMgr, DefWatch, ccEvtMgr, ccSetMgr, SavRoam, RTVscan, QBFCService, QBIDPService, Intuit.QuickBooks.FCS, QBCFMonitorService, YooBackup, YooIT, zhudongfangyu, sophos, stc_raw_agent, VSNAPVSS, VeeamTransportSvc, VeeamDeploymentService, VeeamNFSSvc, veeam, PDVFSService, BackupExecVSSProvider, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, AcrSch2Svc, AcronisAgent, CASAD2DWebSvc, CAARCUupdateSvc
<b>Stopped Processes</b>	sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe, isqlplussvc.exe, xfssvcon.exe, mydesktopservice.exe, ocautoupds.exe, encsvc.exe, firefox.exe, tbirdconfig.exe, mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe

# Activity study

1.3

## Cyber Threat Intelligence

To the best of our knowledge the first appearance of a Babuk ransomware sample to the public goes back to 12/01/2021. The latter was shared onto the Malware exchange platform known as Malware Bazaar from Abuse.ch (see **Figure 3** *Erreur ! Source du renvoi introuvable.*).

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2021-02-22 18:33	391cfd153881743556f7...	exe	Babuk	Babuk	@_jZ	
2021-01-28 08:42	58ccba4fb2b3ed8b5f92a...	exe	Babuk	Babuk Ransomware	@_jZ	
2021-01-25 20:44	3dda3ee9164d6815a18a...	exe	Babuk	Babuk Ransomware v4	@cPeterr	
2021-01-22 00:07	afc265a1dcd9eab5aab2...	exe	Babuk	Babuk babuklocker Ransomware	@_jZ	
2021-01-20 08:55	06d370217abec9468bc2...	exe		Babuk babuklocker Ransomware vasa vasalocker	@_jZ	
2021-01-19 20:43	1b9412ca5e9deb29aeaa...	exe	Babuk	Babuk Ransomware	@ArkbirdDevil	
2021-01-18 22:05	550771bbf8a3e5625d6ec...	exe	Babuk	Babuk Ransomware	@ArkbirdDevil	
2021-01-17 04:36	704a0fa7de19564bc743f...	exe	Babuk	Babuk Ransomware v3	@cPeterr	
2021-01-08 06:42	30fcff7add11ea6685a233...	exe	Babuk	Babuk Locker Ransomware	@JAMESWT_MHT	
2021-01-03 01:12	8203c2f0ecd3ae960cb3...	exe	Babuk	Babuk Ransomware	@ArkbirdDevil	

**Figure 3**

Malware sample table summarizing all shared samples related to 'Babuk' made available from Abuse.ch's Malware Bazaar platform (screenshot taken the 02/25/2021). Overall 10 unique samples were already shared where only one is also tagged with 'Vasa'.

This new ransomware/doxware comes without any code source obfuscation mechanisms. It uses nonetheless a robust encryption scheme being (almost) unbreakable. More precisely, it leverages a home-made SHA256 algorithm Chacha8 for the encryption and protects the keys with ECDH, which can use between 160 and 512 bits long keys (256 here).

Babuk can take additional command line parameters upon deployment. If no parameters are given, it will only encrypt local drives. In contrast, the impact for the victims can be increased not only by additionally encrypting network drives (being connected and mounted) but also by using the Windows Restart Manager in order to close processes that are using files (thus improving the number of files encrypted).

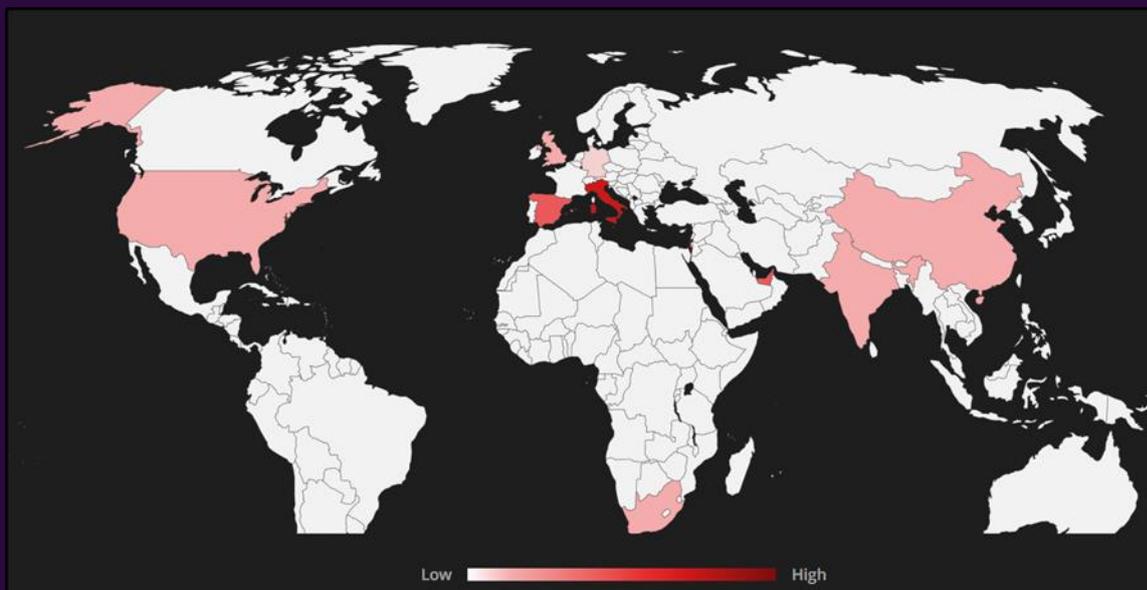
Since its first appearance in early January, Babuk already impacted several different sectors:

- Health
- Bank/Financial/Asset Management
- Retail sales
- Transport

As reported by McAfee, the impact concerns the following countries (see Figure 3 for an estimation of the global prevalence):

- Israel
- USA
- India
- Luxembourg
- Italy
- Spain
- South Africa
- United Arab Emirates
- UK
- China
- Germany





**Figure 4**  
*Global prevalence of Babuk. Italy and Spain are the two countries mostly impacted as of today. But the threat being still recent, this data sample cannot lead to conclusions.*

Establishing a sectorial victimology is still too early as it's not impossible that, like Maze, Babuk's victims could be discriminated not by their activity sector but by their financial size (except the sectors excluded as stated on their onion site, see appendix).

Concerning geographic victimology, it seems, at the moment, that they are not targeting states belonging to the

Community of Independent States (CIS), which is a common exception in the ransomware ecosystem. Indeed, several ransomware samples have been spotted with « kill-switches » when they detect Russian as default language on the system they are running on.

**Importantly, we found no such feature in none of the Babuk' studied ransoms.**

We think it is of relevance to confront that information to the initial English spoken language chosen by Babuk' authors to communicate on underground forums that is rather uncommon; though the authors show they are not English native writers as one can spot at several misspellings and non-native expressions.

The range of ransom spreads from \$60.000 to \$85.000 and at least one victim agreed to pay the highest amount according to *Bleepingcomputer*.<sup>14</sup> This amount of money remains however way below the ransom average estimated by *Coveware* from the 3<sup>rd</sup> quarter of 2018 to the 3<sup>rd</sup> quarter of 2020 (approximately 235k€ average and 120k€ median value). This could be explained due to the amateurism showed by the operators that just joined the Big-game hunting area.

Every Babuk ransomware sample is specifically customized for each targeted victim with a dedicated ransom note and a URL link pointing to the chat hosted on their onion service for the payment negotiations.

Of note is that *Babuk* operators quickly hopped into the double extortion scheme pioneered by Maze when they began to exfiltrate their victim's data in 2019.<sup>15</sup> As far as *Babuk* is concerned, the operators first leaked data samples on *RaidForums* before setting up a dedicated leak site accessible through anonymized networks at this address **gtmx56k4hutn3ikv[.]onion**.

If this new ransomware group in their targeted attacks continue at such a fast pace (5 since the beginning of the year), Babuk could become a serious threat just like Egregor who recently joined the Maze cartel. We should note, though that along the month of February no additional attacks attributed to this strain was reported to the best of our knowledge.



<sup>14</sup> <https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/>

<sup>15</sup> <https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/>

# Babuk's name origin

1.4

## Cyber Threat Intelligence

Our searches on the origin and meaning of the ransomware's name "Babuk" began with a Google Dork. A first result led us on a non-indexed Etsy page we got back from Google's cache.<sup>16</sup> On this page, a human-like figurine named "Babuk" is present, with animal features around the "paws" and the "face" (see **Figure 5**).

Such a morphology could refer to a deity or a mythological creature. Pivoting on this lead, we found the Wikipedia webpage of "Bobak" (written in February 2018), a mythological deimon from the East with features varying depending on the locality. From some stories, "Bobak" can be a humanoid figure with the possibility to change itself in a cat or a dog, which could fit the figurine in **Figure 5**.



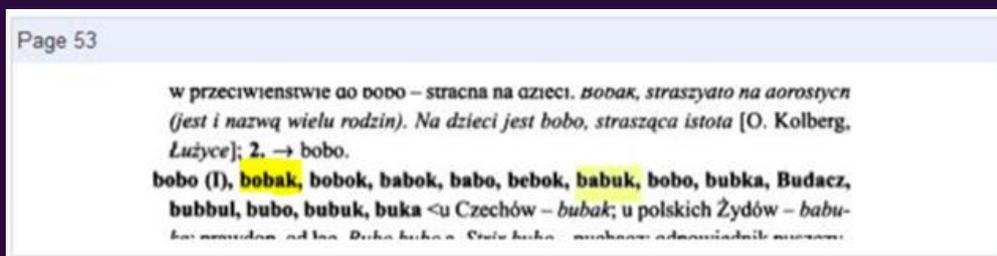
**Figure 5**

*A cached Etsy page shows a human-like figurine named "Babuk" was found. This Figurine could represent a Slavic demon, being a probable origin of the choice for the name of the ransomware.*

<sup>16</sup> <https://www.etsy.com/de/listing/811239443/hands-down-babuk>

Even if “Bobak” and “Babuk” are not identical, the two occurrences are close, which is a common thing to find for mythological creatures under different names and variations, changing with the traditions, the stories and geographical areas. The article’s author, who is bilingual in English and Polish, perhaps chose a name that was more common in his area.

We then took a look at one of the source book referenced by the author Podgórcy, Barbara i Adam (2005).<sup>17</sup> Looking for “Bobak” and “Babuk”, we quickly found an equivalence between the two names, see **Figure 6**.



**Figure 6**  
Google Books  
results for  
"Babuk" search

A link is thus clearly established between “Bobak” and “Babuk”. This name, being the name of a Slavic demon, could be the origin of the ransomware’s name. Moreover, it is not without remembering the choice of the name “ReVil”, meaning “evil ransomware”,<sup>18</sup> or the malware “Valak”, a demon name as well.

Of note is that Babuk changed its brand recently into Babyk as such that the U was replaced by the Y letter). McAfee reported that “in Russian, the Cyrillic letter Y sounds similar to the Latin letter U”. As highlighted by McAfee, the authors were then seen advertising their ‘product’ on Russian-speaking forums seeking for affiliates (posted the 8<sup>th</sup> of January).<sup>19</sup>

<sup>17</sup> *Wielka księga demonów polskich: leksykon i antologia demonologii ludowej.*, pages 53-54”

<sup>18</sup> <https://www.csoonline.com/article/3597298/revil-ransomware-explained-a-widespread-extortion-operation.html>

<sup>19</sup> <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf>

# Investigation on “Biba99” avatar

1.5

## Cyber Threat Intelligence

Seeking to establish the identity and evaluating the digital fingerprint of the attacker, we performed avatar investigations by pivoting on 'biba99' username (found on Raidforums as aforementioned).

A SOCMINT-oriented research for the presence of this avatar provided numerous results, which makes the discrimination of the results quite complex. Nevertheless, the unique occurrence across telegram channels of the avatar "Biba99"<sup>20</sup> drawn our attention.

The person behind this avatar has a channel with a profile picture

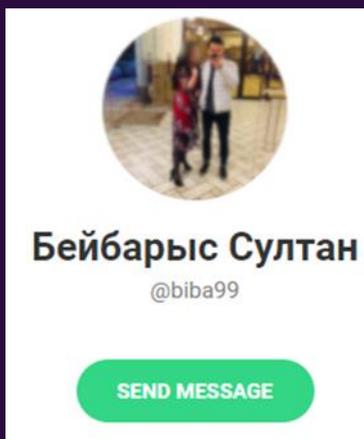
and one could conjecture that it represents him or her. Considering the following elements, we consider that "Biba99" is male. Besides, no metadata could be exploited as it is often the case for telegram channels.

We found that this person joined two groups where the main language used is Turkish. One of the two channels, called "QALB GAVXARI", is surrounded by two emoticons representing the building at the centre of Islam's most important mosque, the Masjid al-Haram in Mecca, Saudi Arabia. This information could indicate that this person could follow and practice Islam religion.

---

<sup>20</sup> <https://t.me/biba99>

**Figure 7**  
Presentation of the "Biba99"  
Telegram channel. The  
inscription in Cyrillic  
"Бейбарыс Султан" means  
"Sultan Beybarys"



**Figure 8**  
Profile picture of the "Biba99"  
Telegram channel



The inscription in Cyrillic "Бейбарыс Султан" means "Sultan Beybarys". The latter refer to the Mamluk Sultan Al-Malik az-Zâhir Rukn ad-Dîn Baybars al-Bunduqdari known as Baybars who ruled over Egypt and Syria from 1260 to 1277.

The Mamluk Sultan is a descendant of the Turkic peoples and distinguished himself by inflicting several major military defeats on King Louis IX of France during the Seventh Crusade as well as on the Mongol Empire. As such, he is regularly taken up in the Turkish-speaking diaspora in the unified narrative of the Turkish people as a vehicle for mobilizing them around the "memory" of a sparkling, conquering and victorious Turkey.

A search for avatars and individuals linked to "Бейбарыс Султан" was conducted to seek further elements beyond its picture on the identity of this individual potential tight to Babuk. We found numerous avatars on social networks using "Бейбарыс Султан" as their usernames, the vast majority of which being Kazakh. This confirms the large popularity of this reference in Kazakh popular culture. Several occurrences refer to Kazakh individuals. One particular Instagram account (@beibarys\_\_sultan<sup>21</sup>) drew our attention.

**Figure 9**  
Homepage of  
@beibarys\_sultan  
Instagram account



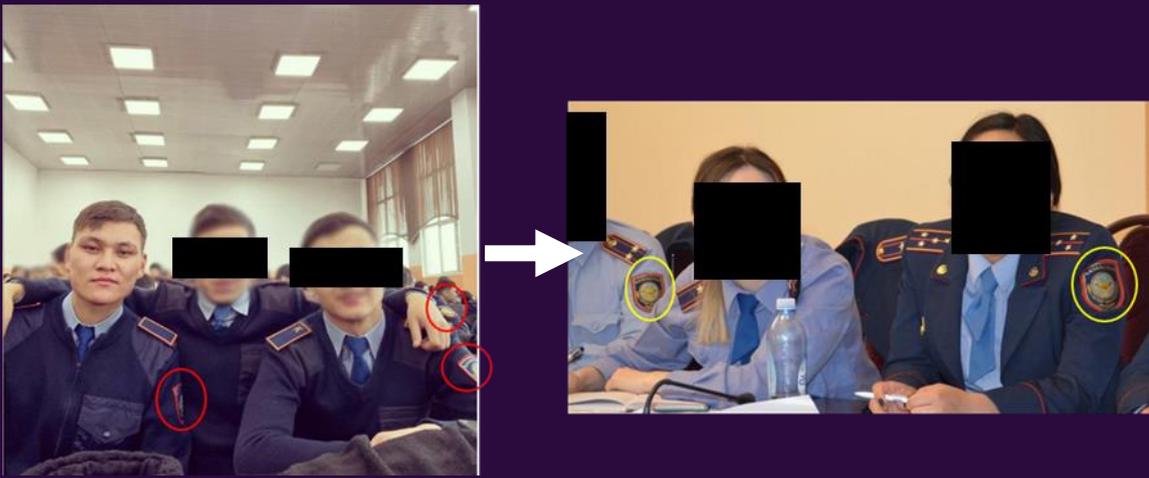
The individual appears several times in both police and military uniforms<sup>22</sup>, denoting a flagrant lack of awareness of the operational security measures (OPSEC) incumbent on the law enforcement on social networks (all the more since his account is public).



**Figure 10**  
Picture shared on  
@beibarys\_sultan's  
Instagram account  
showing the target  
in military uniform

<sup>21</sup> [https://www.instagram.com/beibarys\\_\\_sultan/](https://www.instagram.com/beibarys__sultan/)  
<sup>22</sup> <https://www.instagram.com/p/BsAm85mHN4J/>

The individual claims to be a member of the Military Police of Kazakhstan, which is highly probable given the similarity of the uniforms and insignia to open source images<sup>23 24</sup>.



**Figure 11**  
*(L) @beibarys\_sultan in uniform*  
*(R) PMK delegation in OSCE*

The Military Police of Kazakhstan (PMK) is a branch of the armed forces under the hierarchical authority of the Ministry of Defense whose role is to exercise police power within the armed forces. It oversees investigation cases involving military personnel, but also the protection of sensitive sites, including information systems, which may be of national security interest.

<sup>23</sup> <https://www.osce.org/programme-office-in-astana/353931>

<sup>24</sup> <https://www.instagram.com/p/B7KfaYxnH4s/>

Concerning the resemblance between the avatar @beibarys\_sultan and biba99 (as visible below<sup>25</sup>), we qualify it as to be average.



**Figure 12**

*(L) Profile picture of @biba99*

*(R) Picture published on the @beibarys\_sultan account*

The points of similarity determined by the analyst are as follows:

- The density of the eyebrows and their outward gradation
- The shape of the hairstyle
- The size of the eyes (despite of the crease on the first photo, their dimensions seem coherent)
- The shape of the jaw, relatively square and hollowed out below the lip line.

**NB:** *We have tried to take pictures taken or published during the same period (i.e., during the year 2018).*

---

<sup>25</sup> <https://instagram.com/p/BXesE29FJRJ>



## *To conclude*

**We would like to remind you that attribution attempts made by security companies must be taken with caution. Analysts must deal with a significant degree of uncertainty in each case. The hypotheses we formulate must be treated and understood *as is* and are not intended to incriminate one or more individuals.**

**Finally, we remind you that all the information in this section has been obtained from open sources without any offensive or intrusive actions.**

There is too little relevant open-source information about the digital identity of Babuk's developer being available to go further in the attribution (at this stage and to the best of our knowledge). Though we assessed with a low to medium probability the link between **@beibarys\_sultan** and **biba99**, too many inconsistencies and differences between the two avatars remain to affirm that they are one and the same person.

In the same vein, there is no strong evidence that 'biba99' that claimed on *Raidforums* being operating the ransomware Babuk that it is the same person that owns the Telegram account @biba99

Further analysis of the avatar ecosystem identified upon our research such as analysing status or message updates may allow us to refine the current cluster of clues.

# Attacker's motivations

1.6

## Cyber Threat Intelligence

As previously said, Babuk has a low profile in the eCrime landscape and its sectorial victimology is so far indiscriminate. In contrast, its geographical victimology shows (at the moment of writing and considering the low number of victims) that the attacker seems to spare the Federation of Russia and its foreign allies.

A message posted on Babuk's doxing website claims that its creators will not attack organisations or NGOs except those who support LGBT or Black Lives Matter (BLM). It is a common practice for ransomware operators to express their motives on their leaking site, but it is less common to see such political statements, which substantiates the link aforementioned that @biba99 on

Telegram this person could follow and practice Islam religion.

For the CERT Sogeti ESEC, Babuk's developers are Russian speaking and located in a Central Asia country, with a medium probability for Kazakhstan. This region, even if multicultural and heterogenous, is not the most favourable in support of sexual and ethnical minorities. However, Kazakhstan is quite progressive on this aspect relatively to its Russian neighbour. Even if homosexuals don't have the same freedom as in the Western Europe, Kazakhstan does not condemn relations between persons of the same sex, recognizes the concept of gender identity and refused in a judgment of the Constitutional Court in 2015 the penalisation of homosexual « propaganda ».

Thus, if the hypothesis that **@beibarys\_sultan** is one of Babuk’s developers would appear to be true, it wouldn’t be contradictory with the message posted on their leaking site. **@beibarys\_sultan** evolving in a military institution (where homosexual recruits are forbidden), it would be in a social group<sup>26</sup> where a virilism habitus is promoted and homosexuality is taboo. These values, which are in fact internalized representations by members of social groups linked to the armed forces, tend to develop in individuals a mistrust, mockery and even hostility towards civil society organizations accused of "misrepresenting" these

ideals and values in the same way that defenders of homosexual rights can be.

Concerning the Black Lives Matter reference, this movement<sup>27</sup> is at the centre of a lot of criticism since its appearance in the public space. It gets criticized by different political groups ranging from the left universalist anti-racism current to the alt-right. Even if it’s always complex not to be ethnocentric, it seems Babuk’s developers might fall into the former latter category since anti-racism and LGBT civil rights are sensitive subjects for people with conservative mindsets.



<sup>26</sup> It should be remembered that military culture is not a homogenous whole; it moves according to socio-cultural spaces but retains a base, a common corpus based on a certain marked exaltation of masculinity.

<sup>27</sup> Again, it should be kept in mind that the BLM movement is not uniform, has diverse demands and does not carry the same level of membership depending on whether one is a supporter (or ally) or an activist.

# Babuk's genealogy

1.7

## Cyber Threat Intelligence

To the best of our knowledge and at the time of writing, there is no clear link with any other known threat actor. It is also far from being clear whether or not Babuk ransomware originates from a variant of a known ransomware family, would have been built from scratch or was patchworked by cherry-picking within the top-tier bullet-proofed ransoms. We think the latter hypothesis is the most probable.

For instance, we could first notice that Babuk ransomware possess a feature recently used by several other ransoms that is referred to as "Restart Manager". This

component of Windows being present by design as an API can be leveraged to stop either databases and/or applications (also known as the 'service stop' technique [T1489] in the Common Knowledge framework MITRE).

This technique T1489 aims at quickly close processes that allows a ransomware to encrypt a larger number of files and/or database to increase its impact on a victim. This technique was already adopted by several top-tier ransoms such as Maze/Egregor, Conti, REvil, Ruyk, Netwalker or even Ragnar Locker (this observation was also reported by Trend micro<sup>28</sup>).

---

28

[https://www.trendmicro.com/en\\_us/research/21/b/new-in-ransomware.html](https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html)

Babuk also uses the same encryption algorithm that Maze/Egregor used (chacha), which could have indicated a proximity between groups [T1486]. However, the low technicality of Babuk ransomware on some parts of the code (such as the thread management) seems to tip the hypothesis towards a new group, still in its early stages listening carefully to the feedback from security researchers in order to improve.

A similarity in the ransom note between Darkside and Babuk was pinpointed by Trendmicro.<sup>29</sup> In addition, Carbon SPIDER introduced a variant of Darkside at the end of November 2020 that turns out to be 'Linux compatible' seeking to damage virtual machines on servers having specific extensions;<sup>30</sup> Babuk also claimed recently to embed such

feature on Russian-speaking forums. Beyond Darkside, other ransomware strains have also begun to target ESXi hypervisors such as RansomEXX.

It is interesting to note that CrowdStrike stated that Darkside became independent with its own RaaS model and DLS probably "to avoid sharing profits from BGH campaigns with PINCHY SPIDER, the REvil vendor".<sup>31</sup>

In the same vein, Babuk authors could be previous affiliates of Darkside (from which a decryptor was published since the beginning of this year<sup>32</sup>) that seeks to become independent. Though, previous information and chronology on the life cycle of Darkside and Babuk, such conjecture remains rather speculative at the time of writing.



<sup>29</sup>

[https://www.trendmicro.com/en\\_us/research/21/b/new-in-ransomware.html](https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html)

<sup>30</sup> <https://socprime.com/blog/affiliates-vs-hunters-fighting-the-darkside/>

<sup>31</sup> [https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm\\_campaign=blog&utm\\_medium=soc&utm\\_source=twtr&utm\\_content=sprout](https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout)

<sup>32</sup> <https://labs.bitdefender.com/2021/01/darkside-ransomware-decryption-tool/>

2

# Babuk Analysis

# Protection mechanisms

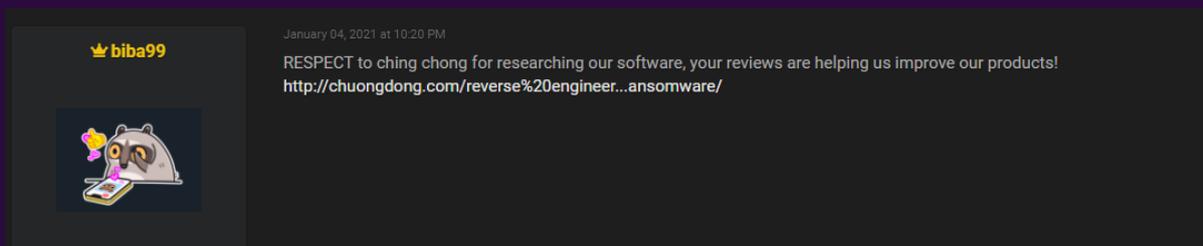
## 2.1

### Cyber Threat Intelligence

No protection or obfuscation techniques were observed upon reverse engineering analysis in the codebase of Babuk. This could translate either into a strategic choice in order to learn from recent techniques coming from researchers pointing out errors or defects and/or a lack of technical maturity to obfuscate their code (*i.e.*, consistent for ex skilled pentesting affiliates trying to become independent while being deprived of ransomware coding skills). This hypothesis is based on the following screenshot where the

Babuk' operator expresses gratitude to the student Chuong Dong, on RaidForums and more recently on their blog. However, they might also rely on affiliates to obfuscate their code because one strain has been spotted packed with custom code looking several steps beyond their coding skills comparing to their multiple OPSEC errors.

Another possibility could be that the operator's personal imperative to promptly gain ransoms that could explain the lack of obfuscation upon the first attacks.



**Figure 13**

*Screenshot of a RaidForums' post from one of Babuk's operator(s) to the student who published an analysis showing some mistakes in their code.*

# OPSEC errors from Babuk's operators

## 2.2

### Cyber Threat Intelligence

We noticed several OPSEC (Operations Security) errors. We first confirmed those cited in Chuong Dong analysis<sup>33</sup> about thread management and encryption errors. We then discovered several misconfigurations of their onion dedicated leak website.

One of them was related to a misconfiguration of the Apache web server exposing its information on the "server-status" page (see Figure 14). The latter is usually leveraged by an admin to monitor CPU load for each request by displaying the latest requests processed by the server as well as the IP address of the clients (hereby this information is not available as the server is running on TOR).

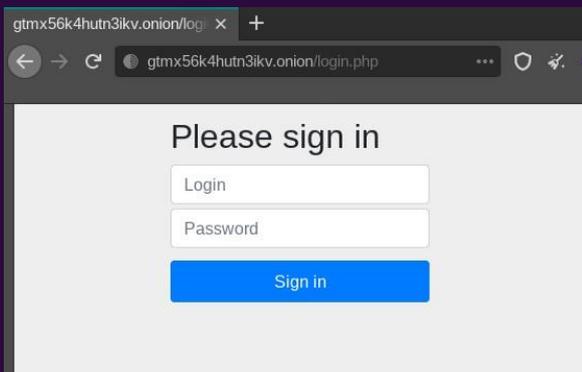
As such, we decided to monitor during a few days the activity on this page to gain information about Babuk's operators.

CPU	SS	Req	Conn	Child	Slot	Client	Protocol	VHost	Request
2.87	7	1	0.0	390.67	9656.26	127.0.0.1	http/1.1	localhost.localdomain:80	GET /server-status HTTP/1.1
1.98	0	0	8.4	28.89	50135.30	127.0.0.1	http/1.1	localhost.localdomain:80	GET /server-status HTTP/1.1
2.03	9	1	0.0	175.73	4779.53	127.0.0.1	http/1.1	localhost.localdomain:80	GET /server-status HTTP/1.1
0.00	46	1	0.0	0.08	76277.69	127.0.0.1	http/1.1	localhost.localdomain:80	GET /server-status HTTP/1.1
4.32	38	6	0.0	19.23	12568.34	127.0.0.1	http/1.1	localhost.localdomain:80	GET / HTTP/1.1
1.40	582	0	0.0	24.63	9928.23	127.0.0.1	http/1.1	localhost.localdomain:80	GET /pub/human/dump.rar HTTP/1.1
0.20	366	0	0.0	0.00	48710.39	127.0.0.1	http/1.1	localhost.localdomain:80	OPTIONS * HTTP/1.0
0.00	21	1	0.0	0.01	20313.91	127.0.0.1	http/1.1	localhost.localdomain:80	GET /server-status HTTP/1.1
0.00	20	1	0.0	0.00	1795.10	127.0.0.1	http/1.1	localhost.localdomain:80	GET /server-status HTTP/1.1

Figure 14

"server-status" page where requests received by the server are displayed

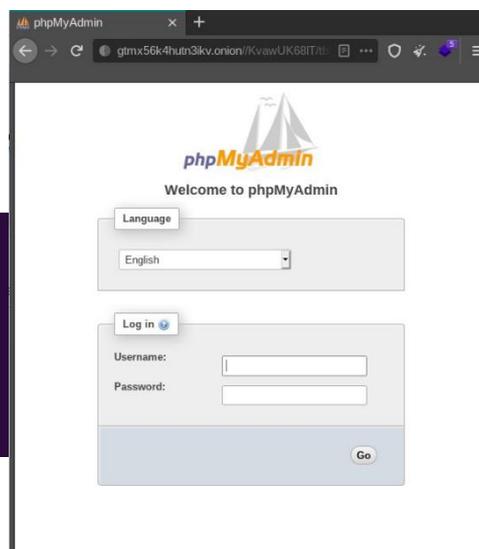
<sup>33</sup> <http://chuongdong.com/reverse%20engineering/2021/01/16/BabukRansomware-v3/>



**Figure 15**  
*login.php page*

Thanks to the monitored requests, we were able to spot at two pages hosted on the same web server that drawn our attention. The first one is a login form, that probably provides an access to an admin dashboard. This portal is thus exposed to bruteforce attacks and to a deep surveillance by CTI teams.

The other item discovered on the server is the presence of a PHPMYAdmin login form. The installed version is 4.6.6, which is not vulnerable at the time of writing. As seen in the requests from the "server-status" page, the database behind PHPMYAdmin seems to handle the blog posts as GET requests were containing parameters like « **db=blog** » and « **table=articles** ». It should be noted that the access to the PHPMYAdmin is made via randomly generated URLs, which means Babuk's operator are conscious that exposing this service is critical for their business. However, the misconfiguration we spotted of their Apache server unveiled such URL when they accessed it allowing us to reach the Phpmysadmin landpage (see Figure 16).



**Figure 16**  
*PHPMYAdmin service exposed on Babuk's doxing site*

# Babuk's evolution

2.3

## Cyber Threat Intelligence

An analysis of Babuk ransomware was made public by IT student Chuong Dong early January. The code analysis was made easier because of the lack of any obfuscation and packing.

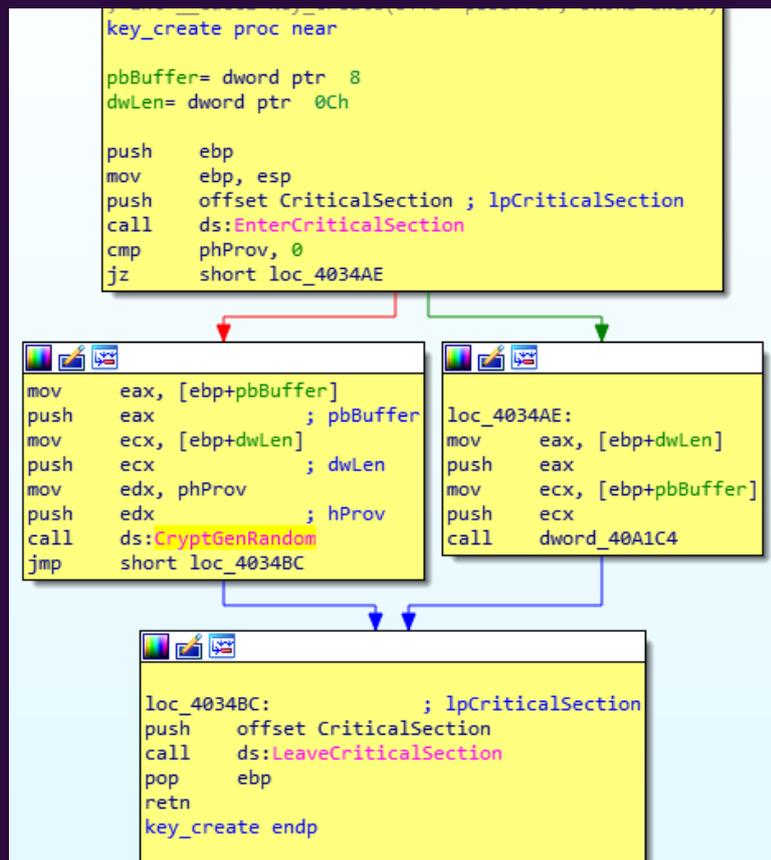
One specific point mentioned by the researcher draw our attention regarding the creation of a file called « **ecdh\_pub\_k.bin** » in the « **AppData** » folder of an infected system. This file is a local private key used to generate a shared secret that will in turn be used to encrypt the files. But we noticed via reverse engineering analysis that the creation of this file is needed for the encrypting procedure to start.

This first element as well as the potential rise in power of this ransomware which could be very impactful pushed us to develop and test a vaccine based on the creation of this private key but also of mutexes to protect against the encryption of documents by the already observed variants of the Babuk ransomware.

We now detail the two types of strains we have analysed and the respective vaccines we could produce with two types of combination, for which we are providing proof of concept.

# Babuk v1

We were able to confirm some of Chuong Dong's findings in its analysis<sup>34</sup>. The encryption process begins by generating a random seed for each host, thus generating a unique key for each infection. The randomized key is achieved via the `CryptGenRandom` function.



**Figure 17**  
Call to  
`CryptGenRandom`  
to get a random  
seed per host

Right before the call to `CryptGenRandom()`, a condition is checked that may redirect to another code branch calling `SystemFunction036()` instead. It is an old reference to `RtlGenRandom()` available for XP systems that may disappear in the future. It is only available through indirect call using `LoadLibrary()` and `GetProcAddress()`. The use of this function might just be for compatibility issues on old systems.

<http://chuongdong.com/reverse%20engineering/2021/01/16/BabukRansomware-v3/>

**Figure 18**  
*Call to SystemFunction036() to generate the seed even on old systems*

```
sub_402410 proc near
push    ebp
mov     ebp, esp
push    offset aSystemfunction ; "SystemFunction036"
mov     eax, hModule
push    eax ; hModule
call   ds:GetProcAddress
mov     dword_40A1C4, eax
pop     ebp
retn
sub_402410 endp
```

The encryption procedure then uses several seeds that are modified at each iteration of the encryption but remains the same for every file on the machine.

```
1 int __cdecl sub_4033B0(_DWORD *a1, int a2, int a3, int a4)
2 {
3     int result; // eax
4     signed int i; // [esp+0h] [ebp-4h]
5     signed int j; // [esp+0h] [ebp-4h]
6
7     *a1 = 1634760805;
8     a1[1] = 857760878;
9     a1[2] = 2036477234;
10    a1[3] = 1797285236;
11    for ( i = 0; i < 8; ++i )
12        a1[i + 4] = sub_403090((unsigned __int8 *) (a2 + 4 * i));
13    result = 48;
14    a1[12] = a3;
15    for ( j = 0; j < 3; ++j )
16    {
17        a1[j + 13] = sub_403090((unsigned __int8 *) (a4 + 4 * j));
18        result = j + 1;
19    }
20    return result;
21 }
```

**Figure 19**  
*Example of used seeds in the first versions of Babuk*

Another call to `sub_403090()` adds some non-linearity to the algorithm.

```
1 int __cdecl sub_403090(unsigned __int8 *a1)
2 {
3     return *a1 | ((a1[1] | (*((unsigned __int16 *) a1 + 1) << 8)) << 8);
4 }
```

**Figure 20**  
*Non-linearity added by shifting and modifying the seeds during the encryption*

From what we observe from the encryption algorithm codebase, we conjecture that the latter was built from scratch, which can induce severe errors as cryptography is a delicate subject. Even if it is an interesting approach to evade AVs and other detection mechanisms, there is the eventuality that an error in the encryption algorithm might induce a weakness allowing the development of a decryption tool by defenders. But this hypothesis deserves a proper cryptographic examination by an expert.

We also observed that the creation of the "**ecdh\_pub\_k.bin**" file impacts the launching of the encryption processes (see screenshot of the source code below).

**Figure 21**  
If the file can't be accessed, execution is stopped.

```
if (ecdhKeyFile != (HANDLE)0xffffffff) {  
    WriteFile(ecdhKeyFile,&DAT_00408278,0x90,&local_218,(LPOVERLAPPED)0x0);  
    CloseHandle(ecdhKeyFile);  
  
    FUN_00402770();  
    nbrDisques = GetLogicalDrives();  
    if (nbrDisques != 0) { // Lance un thread par disque détecté...  
    }  
  
    WaitForMultipleObjects(local_244,lpHandles,1,0xffffffff);  
    local_260 = 0;  
    while (local_260 < local_244) {  
        CloseHandle(lpHandles[local_260]);  
        local_260 = local_260 + 1;  
    }  
}  
delete_shadow_volumes();  
/* WARNING: Subroutine does not return */  
ExitProcess(0);
```

If opening the file fails, then the condition leads directly to **deletion of restore points and Shadow Copy** [T1490]. The next function called at the very end of the code triggers the 'ExitProcess(0) ;' function, causing the process to stop without starting the threads involved in the encryption process.

Luckily, the creation of the file takes place via the CreateFile function of the Windows API, with a parameter specifying that if the file exists the function should return an error. The prior creation of a file with the name "ecdh\_pub\_k.bin" in the AppData folder when launching the executable would therefore prevent data encryption.



## *Key point*

*This is the first part of the vaccine against Babuk*

```
mutex = OpenMutexA(0x1f0001,0,"babuk_v3");  
if (mutex == (HANDLE)0x0) {  
    CreateMutexA((LPSECURITY_ATTRIBUTES)0x0,0,"babuk_v3");  
    // Le lancement des threads arrive ensuite
```

**Figure 22**

*Conditional statement checking the existence of a mutex called "babuk\_v3"*

# Babuk v2/3

Variants of Babuk samples appeared with the peculiarity of conditioning the launching of encryption threads to the presence of a mutex whose name was predictable: "babuk\_vX" X being the version number of Babuk.

Versions 2 and 3 have been uploaded to abuse.ch. One of the differences between the versions is that those using the mutex does not remove shadow volumes when they are stopped by the vaccine (see shadow volumes section).

Other improvements are to be noticed between these versions. It seems that the creators of Babuk are attentive to the analysis and OPSEC errors that are being published by researchers about their ransomware.

The first version of Babuk ransomware had some weaknesses, notably in the implementation of file encryption concurrency<sup>35</sup>. A single thread had to encrypt an entire disk, with Babuk creating as many as there were disks to be encrypted. An effective competitive system should create one thread per processor and implement a task management system.

This improvement was partly implemented in subsequent versions of Babuk. However, some of the concurrent threads were set equal to twice the number of processors, which is still not optimized as threads will conflict in each processor to execute their instructions.

# Babuk v4

Another version uploaded on the January 25<sup>th</sup>, 2021 into the malware bazaar platform now uses another mutex labelled "**DoYouWantToHaveSexWithCoun  
gDong**".

It is therefore to be expected that the vaccine will no longer work for the next strains of Babuk if the developers of Babuk change the mutex in an unpredictable way. It is also interesting to see to what extent they 'play' the student who published the first analyses on Babuk.

---

<sup>35</sup> <http://chuongdong.com/reverse%20engineering/2021/01/16/BabukRansomware-v3/#Multithreading>

# Babuk v5

## Simple log management

The strain used in the attack against Serco<sup>36</sup> was uploaded on January 28<sup>th</sup>.<sup>37</sup>  
The ransom note was once again tailored to target this enterprise.



```
00h
00h
rco.com,_we_are_the_BAB_00401b10 XREF[1]: FUN_004055a0:0040580f(*)
"Hello! serco.com, we are the BABUK team and y...
402290
u".babyk"
defaultChar = HeapH
outputBufferLen = 1
WideCharToMultiByte
Err = GetLastError(
log_Errors("Can't
```

**Figure 23**

*Ransom note addressed to Serco. One finds there the extraits evoked in the article of sky.com*

A new feature has also been added by the Babuk's developers. The ransomware can now be launched with a parameter in its command line telling it a file to write its error messages to. There are 8 types of errors that are logged in this version:

- Process opening error
- Windows Restart Manager (WRM) initialization error
- Resource registration error in WRM
- Error in obtaining process list using a registered resource
- Error opening file
- Error in moving file
- Errors getting the next file in the folder

<sup>36</sup> <https://news.sky.com/story/covid-19-nhs-test-and-trace-unaffected-by-cyber-attack-at-serco-firm-says-12204747>

<sup>37</sup>

<https://bazaar.abuse.ch/sample/58ccba4fb2b3ed8b5f92adddd6ee331a6afdedfc755145e0432a7cb324c28053/>

<pre>Err = GetLastError(); log_Errors("Can't OpenProcess",HeapHandle,Err); HeapFree(HeapHandle);</pre>	<pre>log_Errors("Can't RmGetList",HeapHandle,0); HeapFree(HeapHandle);</pre>
<pre>log_Errors("Can't RmRegisterResources",HeapHandle,0); HeapFree(HeapHandle);</pre>	<pre>Err = GetLastError(); log_Errors("Can't MoveFileExW",HeapHandle,Err); HeapFree(HeapHandle);</pre>

**Figure 24**  
Examples of errors being logged

The parameter allowing to trigger this behaviour is " -debug=[file] " indicating a filename in which to collect errors.

```
indexOfDebugFlag = readArgFlag(nbrArgsPTR, (int)ArgArray, L"debug");
if (indexOfDebugFlag != (LPCWSTR)0x0) {
    DebugFlag = indexOfDebugFlag;
    CreateDebugLogFile(indexOfDebugFlag);
    _isDebugOn = 1;
}
```

**Figure 25:**  
Creation of the file if the "debug" parameter is present

With this improvement came a slight change in the way Babuk handles command line arguments. Here is the list of parameters managed by the last strains:

- lan=[before,after]
- debug=[filename]
- shares=[share1,share2,...]
- paths=[path1,path2,...]

The « lan » flag is here to tell Babuk to start network share encryption before or after local disks. « shares » is used to give Babuk a list of network shares to try to connect to and encrypt as well. The « paths » param can tell to Babuk to encrypt specific local path on disk.

# Babuk Packed

As revealed the 8<sup>th</sup> of February 2021 by @Sebdraven, a new strain of Babuk with a noticeable feature was uploaded on VirusTotal the 11<sup>th</sup> of February.<sup>38</sup> This new version of Babuk now comes packed with a custom hand-made technique which holds some similarities with GandCrab technics.<sup>39</sup>

As the underlying binary remains the same as the previous version, the Babuk' author motivation is probably twofold:

i/ to make it difficult for security researchers to analyse their samples.

ii/ packer-based malwares are modified in the runtime memory and create new signatures for the same malware on the fly, simply by changing the encryption/packing method, which makes such feature more attractive to recruit new affiliates.

As an objective, we tried to unravel how the malware leverages hidden memory processes. We first observed that the unpacking routine uses several anti-forensics analysis techniques such as importing DLLs by assessing the Process Environment Block (PEB).

```
push    large dword ptr fs:30h
pop     eax
mov     eax, [eax+0Ch]
mov     ecx, [eax+0Ch]
```

**Figure 26**  
*Accessing Process Environment Block (PEB) at fs[0x30] and then the PEB\_LDR\_DATA which holds a double linked list of the loaded DLL*

The function `sub_42DF00()` allocates some memory using `GlobalAlloc()`, and then copies a binary blob containing the encrypted payload :

---

<sup>38</sup>

<https://www.virustotal.com/gui/file/bc4066c3b8d2bb4af593ced9905d1c9c78fff5b10ab8dbed7f45da913fb2d748/details>

<sup>39</sup> <https://sebdraven.medium.com/babuk-is-distributed-packed-78e2f5dd2e62>

**Figure 27**  
*GlobalAlloc() call to copy  
the packed code into  
memory*

```

39 counter = 0;
40 lpAddress = GlobalAlloc(0, number_byte_to_allocate);
41 dword_2FB07F4 = dword_43A408;
42 if ( dwBytes )
43 {
44     do
45         copy_packed_code(counter++);
46     while ( counter < dwBytes );
47 }

```

Babuk does this 2 times before executing the final code. The whole process consists of several chained XOR operations:

```

26 do
27 {
28     v4 = 16 * v3;
29     if ( dwBytes == 879 )
30         WaitForMultipleObjects(0, 0, 0, 0);
31     v5 = v12 + (v3 >> 5);
32     dword_2F831F8 = -370538954;
33     v6 = (v9 + v3) ^ v5 ^ (v4 + v13);
34     v8 = (v9 + v3) ^ v5 ^ (v4 + v13);
35     if ( dwBytes == 1766 )
36     {
37         CreateMutexA(0, 0, 0);
38         CC.dwSize = 0;
39         memset(&CC.wVersion, 0, 0x30u);
40         SetDefaultCommConfigW(0, &CC, 0);
41         v6 = v8;
42     }
43     v1 -= v6;
44     if ( dwBytes == 2105 )
45         SleepEx(0, 0);
46     dword_2F83200 = -875163516;
47     dword_2F83204 = -1;
48     v3 -= (v9 + v1) ^ (v11 + (v1 >> 5)) ^ (v2 + 16 * v1);
49     if ( dwBytes == 1047 )
50         lstrcatA(0, 0);
51     v9 += 1640531527;
52     --v10;
53 }
54 while ( v10 );

```

**Figure 28**  
*Unpacking procedure  
using XOR*

Once it unpacks itself into memory, we can recognize strings already observed in previous strains (see **Figure 30**).

Not only the same predictable mutex **“DoYouWantToHaveSexWithCuongDong”** is visible, but also the same ransom note.

The complexity of the code related to the unpacking of the executable in memory does not seem to be compatible with the technical level of Babuk’s developer observed a few weeks ago while keeping a predictable mutex creation mechanism.

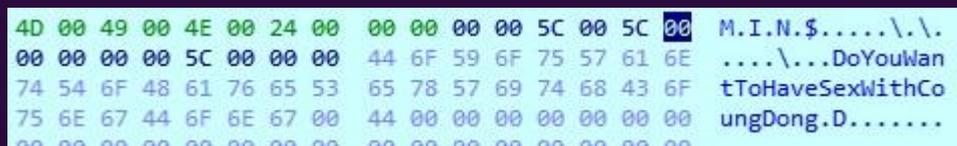
**More probable is the building of a partnership with another threat actor or they simply accessed the packer as a paid service.**



*Pushing DLL names to the stack as hexadecimal values so they don't appear as strings*



**Figure 29**  
*Part of the ransom note*



**Figure 31**  
*Mutex name taunting Chuong Dong. They did not change it for an unpredictable one, thus keeping our vaccine effective against this strain.*

# Modus operandi

2.4

## Cyber Threat Intelligence

- The modus operandi observed during the attacks involving Babuk seems compatible with an opportunistic actor motivated by a profit motive
- Its operators adopted the same double extortion method as other top-tier ransomware families with a dedicated leak site
- Several source code errors previously noted suggest that this ransomware may have been developed hastily. The same is true for the doxing site, which contains several configuration errors. We can state with a high degree of reliability that the Babuk operator is not driven by a nation state
- The techniques, tactics and procedures (TTPs) are classic and have not shown the use of particularly sophisticated attack techniques. Exception made concerning the initial infection vector that remains (to our knowledge) unknown
- The C++ coded ransom is based on public libraries and its specific code is very short in length
- The ideology displayed as anti-capitalist backed by a conservative societal ideology (anti-LGBT) is compatible with a hacktivist group of Muslim faith echoing the mention of 'sultan'

3

SecEng

# Scope

3.1

## Security Operation Center

**W**e will use our purple laboratory to run Babuk with the aim to create detection rules tailored for this threat.

Your laboratory for this topic is virtualized and composed of:

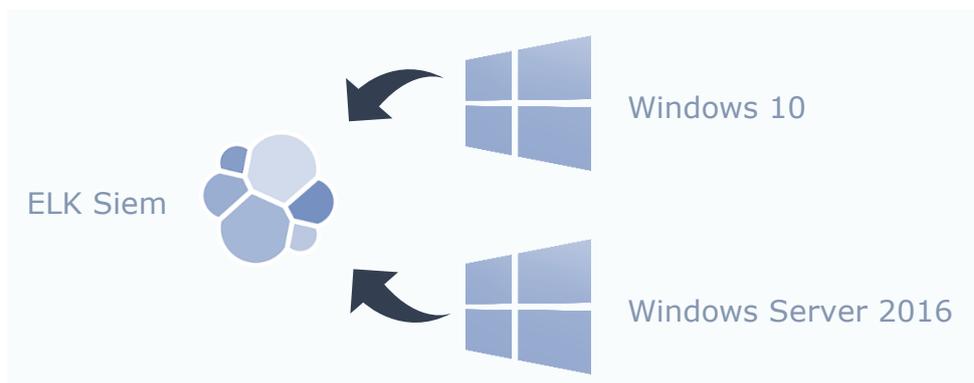
- Windows Server 2016 (Version 1607)
- Windows 10 (Version 1909)
- ELK SIEM v7.10.2
- Squid 4.14

The Windows Server is the Domain controller.

The Windows 10 is attached to the domain and is freshly installed with default logging policy and Sysmon with the default configuration. There is no security software.

All logs are sent by the Winlogbeat agent with the default configuration.

We used the version 5 of the sample (See chapter above)



# Preparation phase

3.2

## Security Operation Center

**B**, once running, stops a lot of services in charge of the backup. As such, we decided to create fake services.

The two services created were named "veeam" and "YooBackup" (see **Figure 32** below)

The two services are correctly started and running:

```
PS C:\WINDOWS\system32> New-Service -Name 'veeam' -BinaryPathName 'C:\service.exe' -DisplayName 'veeam' -StartupType Manual
Status  Name          DisplayName
-----  -
Stopped veeam         veeam

PS C:\WINDOWS\system32> New-Service -Name 'YooBackup' -BinaryPathName 'C:\service.exe' -DisplayName 'YooBackup' -StartupType Manual
Status  Name          DisplayName
-----  -
Stopped YooBackup     YooBackup

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> get-service | where-object {$_.Name -eq 'veeam'}
Status  Name          DisplayName
-----  -
Running veeam         veeam

PS C:\WINDOWS\system32> get-service | where-object {$_.Name -eq 'YooBackup'}
Status  Name          DisplayName
-----  -
Running YooBackup     YooBackup
```

**Figure 32**

*"Veeam" and "YooBackup" fake services up and running*

# Execution phase

3.3

## *User Execution Malicious File (T1204.002)*

### Security Operation Center

**A**T this moment, we simulate a scenario in which an analyst does not know how the sample was delivered on the endpoint and if there is any check done before the execution. For this reason, we decide to start without any parameters.

```
PS C:\Users\user1\Desktop\Samples\babuk> .\babuk_01-03.exe  
PS C:\Users\user1\Desktop\Samples\babuk> _
```

**Figure 33**  
*Execution of Babuk v5*



# Hunting phase

3.4

## Security Operation Center

### *Shadow copy – Inhibit System Recovery (T1490)*

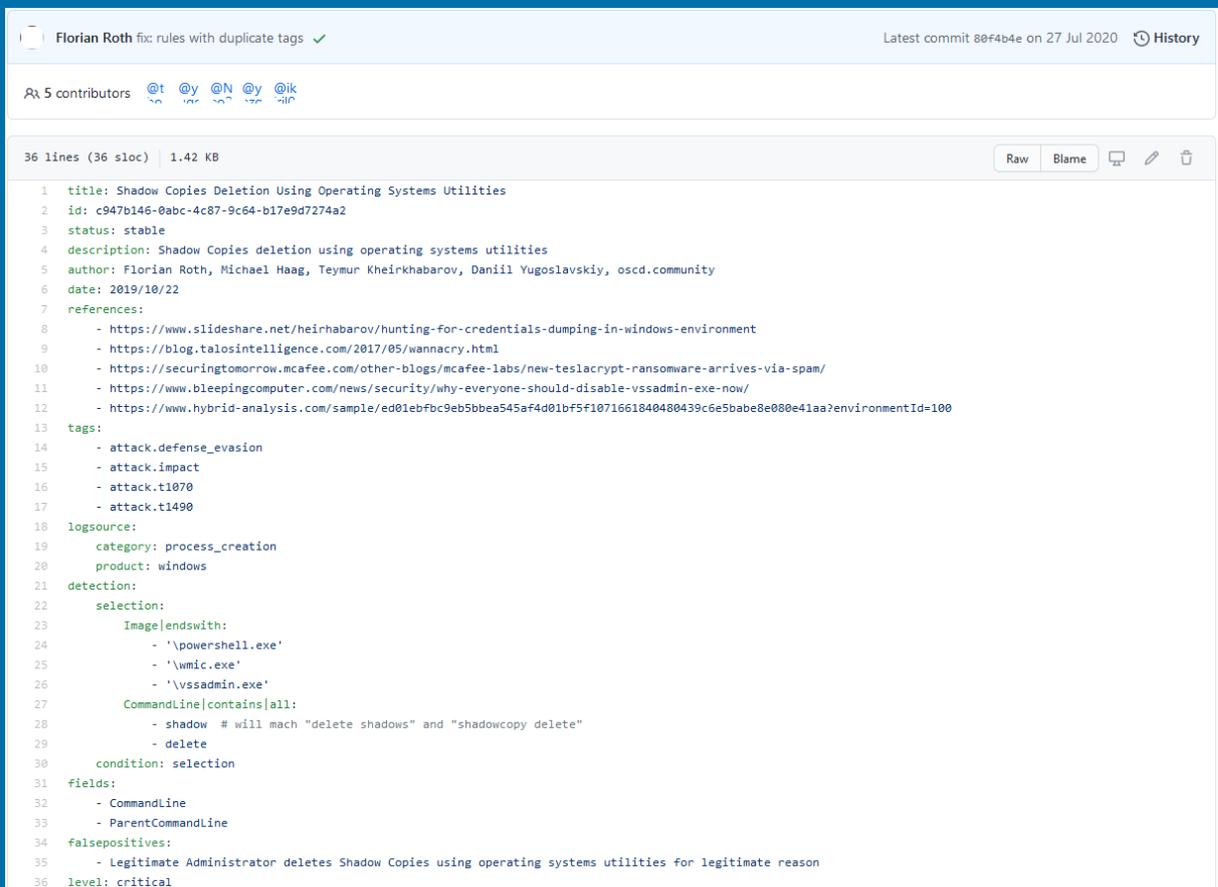
**B**abuk starts by launching two commands as displayed in the command line in order to delete the shadows volumes (so far what we witness is an expected behavior).

This operation is performed twice in less than 5 minutes.

Time ^	process.command_line	process.parent.name
> Mar 4, 2021 @ 15:56:40.791	"C:\Users\user1\Desktop\Samples\babuk\babuk_01-03.exe"	powershell.exe
> Mar 4, 2021 @ 15:56:41.193	"C:\Windows\System32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet	babuk_01-03.exe
> Mar 4, 2021 @ 15:56:41.388	vssadmin.exe delete shadows /all /quiet	cmd.exe
> Mar 4, 2021 @ 16:00:44.697	"C:\Windows\System32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet	babuk_01-03.exe
> Mar 4, 2021 @ 16:00:45.025	vssadmin.exe delete shadows /all /quiet	cmd.exe

**Figure 34**  
*Shadow copy deletion by Babuk*

The Sigma rule "Shadow Copies Deletion Using Operating Systems Utilities » should detect this behavior (T1490)<sup>40</sup>.



```
1 title: Shadow Copies Deletion Using Operating Systems Utilities
2 id: c947b146-0abc-4c87-9c64-b17e9d7274a2
3 status: stable
4 description: Shadow Copies deletion using operating systems utilities
5 author: Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community
6 date: 2019/10/22
7 references:
8   - https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
9   - https://blog.talosintelligence.com/2017/05/wannacry.html
10  - https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/new-teslacrypt-ransomware-arrives-via-spam/
11  - https://www.bleepingcomputer.com/news/security/why-everyone-should-disable-vssadmin-exe-now/
12  - https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e00e41aa?environmentId=100
13 tags:
14   - attack.defense_evasion
15   - attack.impact
16   - attack.t1070
17   - attack.t1490
18 logsource:
19   category: process_creation
20   product: windows
21 detection:
22   selection:
23     Image|endsWith:
24       - '\powershell.exe'
25       - '\wmic.exe'
26       - '\vssadmin.exe'
27     CommandLine|contains|all:
28       - shadow # will mach "delete shadows" and "shadowcopy delete"
29       - delete
30   condition: selection
31 fields:
32   - CommandLine
33   - ParentCommandLine
34 falsepositives:
35   - Legitimate Administrator deletes Shadow Copies using operating systems utilities for legitimate reason
36 level: critical
```

**Figure 35**  
Sigma rule "Shadow Copies Deletion Using Operating Systems Utilities »

Be aware that this rule can also trigger false positives due to the nature of the command (often used by IT technicians). To fine tune the Sigma detection rule one should set a threshold of 5 minutes between two executions, in order to limit the number of triggers.

40

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process\\_creation/win\\_shadow\\_copies\\_deletion.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_deletion.yml)

# Service/Process stopped – Service Stop (T1489)

As expected, Babuk is shutting down specific services and processes related to backup purposes. One can see below that the two fakes services previously created were affected by this behavior.

Time ^	event.action	process.executable
> Mar 4, 2021 @ 15:56:40.952	Process terminated (rule: ProcessTerminate)	C:\service.exe
> Mar 4, 2021 @ 15:56:40.958	Process terminated (rule: ProcessTerminate)	C:\service.exe
> Mar 4, 2021 @ 15:56:41.001	Process terminated (rule: ProcessTerminate)	C:\Program Files\Mozilla Firefox\firefox.exe
> Mar 4, 2021 @ 15:56:41.032	Process terminated (rule: ProcessTerminate)	C:\Program Files\Mozilla Firefox\firefox.exe
> Mar 4, 2021 @ 15:56:41.035	Process terminated (rule: ProcessTerminate)	C:\Program Files\Mozilla Firefox\firefox.exe
> Mar 4, 2021 @ 15:56:41.095	Process terminated (rule: ProcessTerminate)	C:\Program Files\Mozilla Firefox\firefox.exe
> Mar 4, 2021 @ 15:56:41.109	Process terminated (rule: ProcessTerminate)	C:\Program Files\Mozilla Firefox\firefox.exe

**Figure 36**  
Services stopped by Babuk

We have created a specific Sigma rule for all services closed by Babuk. Bear in mind however that this rule will raise a lot of false positive in case of any reboot of an endpoint or server.

```
title: Babuk service stopped
id: 015c11a6-7362-4497-85c8-558f4fae0185
status: experimental
description: Detects command-line argument to control how the ransomware should encrypt network shares.
references:
  - Internal research
date: 2021/03/08
tags:
  - attack.impact
  - attack.t1489
```

```

logsource:
  service: sysmon
  product: windows

detection:
  selection:
    EventID: 5
    timeframe: 60s
    EventAction|contains: 'terminated'
    Image|contains:
      - vss
      - sql
      - svc$
      - mentas
      - mepocs
      - sophos
      - veeam
      - backup
      - GxVss
      - GxBLr
      - GxFWD
      - GxCVD
      - GxCIMgr
      - DefWatch
      - ccEvtMgr
      - ccSetMgr
      - SavRoom
      - RTVscan
      - QBFCService
      - QBIDPService
      - Intuit.QuickBooks.FCS
      - QBCFMonitorService
      - YooBackup
      - YooIT
      - zhudongfangyu
      - sophos
      - stc_raw_agent
      - VSNAPVSS
      - VeeamTransportSvc
      - VeeamDeploymentService
      - VeeamNFSSvc
      - veeam
      - PDVFSService
      - BackupExecVSSProvider
      - BackupExecAgentAccelerator
      - BackupExecAgentBrowser
      - BackupExecDiveciMediaService
      - BackupExecJobEngine
      - BackupExecManagementService
      - BackupExecRPCService
      - AcrSch2Svc
      - AcronisAgent
      - CASAD2DWebSvc
      - CAARCUupdateSvc
  condition: selection

falsepositives:
  - Reboot
    level: high

```



# File creation

Babuk also creates the file "How To Restore Your Files.txt" and place it in every folder.

Below an example of the 553 files created with the same name.

Top values of file.name	Count of records
How To Restore Your Files.txt	553

The file contains the instructions to pay the ransom.

```
How To Restore Your Files.txt - Notepad
File Edit Format View Help
##### [ babyk ransomware ] #####

* What happend?
-----
Your computers and servers are encrypted, backups are deleted from your network and copied.
We use strong encryption algorithms, so you cannot decrypt your data without us.
But you can restore everything by purchasing a special program from us - a universal decoder.
This program will restore your entire network. Follow our instructions below and you will recover all your data.
If you continue to ignore this for a long time, we will start reporting the hack to mainstream media and posting
your data to the dark web.

* What guarantees?
-----
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

* How to contact us?
-----
1) Download for browser: https://www.torproject.org/download/
2) Open it
3) Follow this link in tor browser: http://babukq4e2p4wu4iq.onion/login.php?id=
```

Another file « ecdh\_pub\_k.bin” is also created in the folder AppData. This file is a local private key used to generate a shared secret that will be used to encrypt the files.

```
title: Babuk files
id: f7b573cb-5635-49d4-ae13-5b8a0beeda8f
status: experimental
description: Detects the ransom instructions file or the private key used by
babuk or the renamed files.

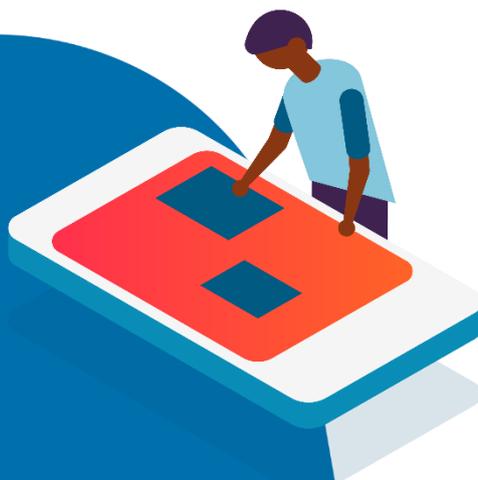
references:
  - Internal research

date: 2021/02/02

logsource:
  category: file_event
  product: windows

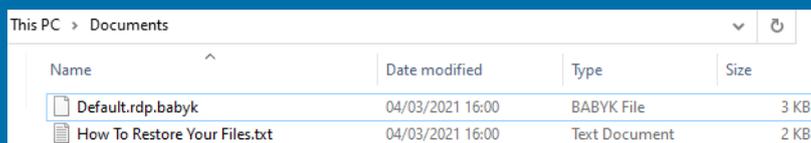
detection:
  selection:
    TargetFilename|contains:
      - '\How To Restore Your Files.txt'
      - '.babyk'
      - '.babuk2'
      - '.__NIST_K571__'
      - '\AppData\ecdh_pub_k.bin'
  condition: selection

falsepositives:
  - No
  level: high
```



# File modification

All personal files are renamed with the extension “.babyk”.



Name	Date modified	Type	Size
Default.rdp.babyk	04/03/2021 16:00	BABYK File	3 KB
How To Restore Your Files.txt	04/03/2021 16:00	Text Document	2 KB

**title:** Babuk files

**id:** f7b573cb-5635-49d4-ae13-5b8a0beeda8f

**status:** experimental

**description:** Detects the ransom instructions file or the private key used by babak or the renamed files.

**references:**

- Internal research

**date:** 2021/02/02

**logsource:**

**category:** file\_event  
**product:** windows

**detection:**

**selection:**

TargetFilename|contains:

- '\How To Restore Your Files.txt'
- '.babyk'
- '.babuk2'
- '.\_\_NIST\_K571\_\_'
- '\AppData\ecdh\_pub\_k.bin'

**condition:** selection

**falsepositives:**

- No  
level: high

# Shadow volumes

3.5

## Security Operation Center

An open-source vaccine was recently developed by Florian Roth<sup>41</sup> (CTO of Nextron) and made available on GitHub. Named “Raccine”, this tool can detect and stop any Windows process trying to delete the shadow volumes on a system.<sup>42</sup>

The use of “Raccine” tool, coupled with our custom vaccine against Babuk, provides a full protection against this ransomware family targeting windows environment.

8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9.exe -nolan	cmd.exe
"C:\Windows\System32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet	8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9.exe
\\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	cmd.exe
"C:\Program Files\Raccine\Raccine.exe" vssadmin.exe delete shadows /all /quiet	cmd.exe
vssadmin.exe delete shadows /all /quiet	Raccine.exe

<sup>41</sup> <https://github.com/Neo23x0/Raccine>

<sup>42</sup> <https://attack.mitre.org/techniques/T1490/>

# Source code of our vaccine

# 3.6

## Security Operation Center

Hereby we share the source code of the python script we developed as a proof-of-concept to protect a host from Babuk's robust encryption:

```
#TLP: AMBER (closed communities to trusted individuals only)
#Name: Babuk Ransomware Vaccine
#Author: CERT Sogeti ESEC Threat Intelligence Team
#Description: This vaccine prevents the Babuk Ransomware execution through Mutex creation
#Contact: sogetiesecctiteam.eur@capgemini.com

import win32event
import win32file
import win32con
from threading import Thread
import time
import os
from subprocess import Popen, PIPE

class MutexThread (Thread):
    def __init__(self, mutexname):
        Thread.__init__(self)
        self.mutexname = mutexname

    def run(self):
        mutex = win32event.CreateMutex(None, True, self.mutexname)
        while (True):
            time.sleep(1)

mutexNames = []
threads = []

# We added the last strain's mutex
mutexNames.append("DoYouWantToHaveSexWithCoungDong")
threads.append(MutexThread(mutexNames[0]))
threads[0].start()

for i in range(1, 11):
    mutexNames.append("babuk_v" + str(i))
    threads.append(MutexThread(mutexNames[i]))
    threads[i].start()

# Then we create the file in AppData/Roaming
# We also forbid other access with the shareMode, just in case
```

```

fileName = os.getenv("APPDATA") + "\ecdh_pub_k.bin"
# Impossible to access the file until the handle is closed
shareMode = 0
securityAttributes = 0
creationDisposition = win32con.CREATE_NEW
fileAttributes = win32con.FILE_ATTRIBUTE_NORMAL
templateFile = 0

desiredAccess = win32con.GENERIC_READ

file = win32file.CreateFile(
    fileName,
    desiredAccess,
    shareMode,
    None,
    creationDisposition,
    fileAttributes,
    None,
)

While(1):
    time.sleep(1)

file.Close()

```

The code will create the mutexes for the potential versions by incrementing up to the number 10. It also creates the file containing the public key at the following path:

**"C:\Users\[user]\AppData\Roaming\ecdh\_pub\_k.bin"**

As a result, the first versions of the ransomware are blocked (cf Babuk\_v1 version). This vaccine has been tested and validated for all versions currently available on abuse.ch. More specifically, this vaccine can be used to protect against the following versions.

The script creates mutexes for several potential Babuk versions by creating mutexes from "babuk\_v1" to "babuk\_v10". It then creates the file at the following path:

**« C:\Users\[user]\AppData\Roaming\ecdh\_pub\_k.bin »**

It renders the early strain ineffective. The vaccine was tested and validated for the following versions of Babuk:

- <https://bazaar.abuse.ch/sample/1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02/>
- <https://bazaar.abuse.ch/sample/550771bbf8a3e5625d6ec76d70ed86f6e443f07ce80ff73e47f8249ddd72a8cf/>
- <https://bazaar.abuse.ch/sample/704a0fa7de19564bc743fb68aa0652e38bf86e8ab694bc079b15f945c85f4320/>
- <https://bazaar.abuse.ch/sample/30fcff7add11ea6685a233c8ce1fc30abe67044630524a6eb363573a4a9f88b8/>
- <https://bazaar.abuse.ch/sample/8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9/>

# GPO deployment

3.7

## Security Operation Center

To anticipate such a threat, the target cannot be known in advance, it would obviously be necessary to prior deploy the vaccine against Babuk (but also against Shadow Volumes suppression) either on the whole perimeter or on a third party or several third parties deemed to be a priority. To do so, it is possible to deploy such a vaccine by Group Strategy Objects (GPO).<sup>43</sup>



<sup>43</sup> <https://github.com/Neo23x0/Raccine/tree/main/GPO>

# Limitations

3.8

## Security Operation Center

On the one hand, we do not guarantee the long-term effectiveness of the vaccines as soon as the individuals behind Babuk, which maintains the codebase of this ransomware, realizes this weakness and/or the existence of such a 'kill-switch'.

On the other hand, we must emphasize that this vaccine, with or without complementarity with 'Raccine', **does not protect against the double extortion already carried out by Babuk** (and therefore a fortiori the triple extortion by threat of denial of service<sup>44</sup>).

Finally, the 'Raccine' vaccine, which is intended to be generic for the vast majority of ransomware (those that erase shadow volumes), **has some drawbacks**. It will indeed kill any process using vssadmin.exe, which may have an impact on some backup solutions that legitimately use the functionalities of this tool.

It also does not defend against ransoms which would not have launched themselves the deletion of shadow volumes, for example by passing through a scheduled task.

---

<sup>44</sup> <https://www.bleepingcomputer.com/news/security/ransomware-gangs-add-ddos-attacks-to-their-extortion-arsenal/>

# Acknowledgements

3.9

## Security Operation Center



The authors are very grateful to **Hugo BITARD** (a former analyst of the CERT SOGETI ESEC) for contributions that enriched the reverse engineering analysis as well as active members of the National French Network (InterCERT-FR) for helpful discussions.

We also thank **Alexandre BOUILLON** (being part of the Incident Response-SWAT team of our CSIRT) for peer-reviewing this article.



# 4

# Appendix

# Mitre ATT&CK Matrix

about

Babuk Ransomware

Execution	Persistence	Defense Evasion	Discovery	Impact
Command and Scripting Interpreter	Office Application Startup	Modify Registry	File and Directory Discovery	Data Encrypted for Impact
Native API		Obfuscated Files or Information	Process Discovery	Inhibit System Recovery
Shared Modules		Subvert Trust Controls	Query Registry	Service Stop
User Execution		Install Root Certificate	System Information Discovery	
			System Network Connections Discovery	

Credits to Mitre Corporation<sup>45</sup>

**NB:** Babuk's Mitre ATT&CK matrix will be completed with the advancements of CERT Sogeti ESEC's analysts.

<sup>45</sup> <https://attack.mitre.org/>

# Ransom note

```
----- [ Hello, ██████████ ] ----->
****BY BABUK LOCKER****

what happend?
-----
Your computers and servers are encrypted, backups are deleted from your network and copied. we use strong encryption algorithms, so you cannot
But you can restore everything by purchasing a special program from us - a universal decoder. This program will restore your entire network.
Follow our instructions below and you will recover all your data.
If you continue to ignore this for a long time, we will start reporting the hack to mainstream media and posting your data to the dark web.

what guarantees?
-----
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. we will also provide support in case of problems.
we guarantee to decrypt one file for free. Go to the site and contact us.

what information compromised?
-----
we copied more than 10 gb from your internal network, here are some proofs, for additional confirmations, please chat with us
in cases of ignoring us, the information will be released to the public.

How to contact us?
-----
using TOR Browser ( https://www.torproject.org/download/ ):
http://babuk4e2p4wu4iq.onion/login.php: ██████████

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. we WILL NOT be able to RESTORE them.
!!! DANGER !!!
```

# Stopped services<sup>46</sup>

- vss
- sql
- svc\$
- memtas
- mepocs
- sophos
- veeam
- backup
- GxVss
- GxBlr
- GxFWD
- GxCVD
- GxCIMgr
- DefWatch
- ccEvtMgr
- ccSetMgr
- SavRoam
- RTVscan
- QBFCService
- QBIDPService
- Intuit.QuickBooks.FCS
- QBCFMonitorService
- YooBackup
- YooIT
- zhudongfangyu
- sophos
- stc\_raw\_agent
- VSNAPVSS
- VeeamTransportSvc
- VeeamDeploymentService
- VeeamNFSSvc
- veeam
- PDVFSService
- BackupExecVSSProvider
- BackupExecAgentAccelerator
- BackupExecAgentBrowser
- BackupExecDiveciMediaService
- BackupExecJobEngine
- BackupExecManagementService
- BackupExecRPCService
- AcrSch2Svc
- AcronisAgent
- CASAD2DWebSvc
- CAARCUUpdateSvc

<sup>46</sup> <https://github.com/StrangereAllIntel/DailyIOC/blob/master/2021-01-02/BabukLocker/Notes.txt>

# Stopped processes

- sql.exe
- oracle.exe
- ocssd.exe
- dbnmp.exe
- synctime.exe
- agntsvc.exe
- isqlplussvc.exe
- xfssvcon.exe
- mydesktopservice.exe
- ocaoutoups.exe
- encsvc.exe
- firefox.exe
- tbirdconfig.exe
- mydesktopqos.exe
- ocomm.exe
- dbeng50.exe
- sqbcoreservice.exe
- excel.exe
- infopath.exe
- msaccess.exe
- mspub.exe
- onenote.exe
- outlook.exe
- powerpnt.exe
- steam.exe
- thebat.exe
- thunderbird.exe
- visio.exe
- winword.exe
- wordpad.exe
- notepad.exe

## IOCs

Indicators of compromise below can be blocked and searched on an information system to prevent or detect a similar attack.

### Email

[babukrip@protonmail.com](mailto:babukrip@protonmail.com)

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: ProtonMail

```
xsBNBF/CueIBCADGIGfsEITt6vrrfMN2PntCPC6EvrH82ZCocTKX2xk40i
h4iqKDOoIIK79ZFaQVYAkgbKPEfMz5c8dyRg5fntLx5xjWTK/gQofmcijLv/W
5z4Tmj5W7YnnpIfooC6ON/atQZrxutmEDJByURzcXk9BejmY7LcUKPpEvU7n
h54Jijt2QZcEd5xLSRibDoyra0xN0bAG7jJ5FjXKq2ojm7rQ8adYqKc1Hrr/
muPIEYfYvrmvA8kZ6/HTqYdMpRzQqbd3BgWMOvBnmrc3NV5iDX0zp99ba1UE
nGS2qjjup24IhP7lcaNMy2ZfEKw+m0MKN0y9odH/AueOX/mcDWT7hswRABEB
AAHNL2JhYnVrcmlwQHBYb3Rvbm1haWwUy2ggPGJhYnVrcmlwQHBYb3Rvbm1h
aWwUy2g+wsCNBBABCAAQBQJfwrniBgsJBwgDAGQVCAoCBBYCAQACGQECGwMC
HgEAIQkQzVvKkyWpvmvgWISQZS283PrrLMT3Yz+mHNW8orJama+GVGCAcBrgdz
X0gTDYso0przWfdjqJlxbO9T8SxQfcZMM8L941NEICT4zou9JUTMoBZjHU5i
kmsvL/byaeQ4wOQ+6QxNZeR5/OEDdG0CEuWTCI6eD0w2sqccqUXkZ0Wupth
Gu+YeQeYEAwWUxntzEQ6NrUI5f244UmQvBqJJ7pX9qSXmRISDW/PbWMI/0D3
JIWk/esHqoEvjNRL8FuWlISDpwGvoFYfyslrz5EzcdG2zaC5x0WZw1IB3f0
vCbynidUabhTr0soOoNHdujITLzLN5h3SFA4GIXZEaw4A5hmk+IitckKnxZa
GFFb+nMboYqAsRkgavnBZ0YXmQTUII4BjBZkzsBNBF/CueIBCACw8t7zv/Cm
pV2j925TwusGh3q/4srjff60bPpf4xpikG6Wci/AA3z57bP8iu593e45LH1Gv
3b5zFvZxKMeiphoMEujEg+8vDzmcC4T7lw+PmXV5qjHuChz2wt229x2BLINb
XgV1oCpQcsb5AbzNAIGF31dnHUkseU+VxhgM3N+vyYV+KarvkCIHIDEFHxfu
L2ZQVE3N9ZyKR/N3ahOIAkdk5fLEyYu2YjMTC+qr3A4uOHU3e0YwkGyU5X
XY5N24V6I4Rl3Xe+BS/bwx/hqN5Ar41MJTOeEdNCGjAh9MNqFW1mivl7djsa
qZBTiv+6EzRF5S20HPxKn7xs0TuV+zdABEBAAHCwHYEGAEIAAkFAI/CueIC
GwwAIQkQzVvKkyWpvmvgWISQZS283PrrLMT3Yz+mHNW8orJama+FNhB/9dADjc
GGVlx8qHfxsdqSHrNjE2AUrG2FFm57Jcwn//kzU6BFJmqmO67ru4w96SQjxi
nKqwXe8J4kV3WZsuoGEpt+CIQBIV+pAilKqS1LhkU5U9LXCwJR/WqcNwRntb
4mqk4swtIDXoVE2o+DeC5duxrojc0wqQroLb0h8wtYXuq7MJfsyCnXiAyb+0
qdLxHafgrm4dGBvIEvYaznagiG+jM45Rq/Ctrs7entafUwN3t440cSozXu
pzE4XsmSa5gu7we3J8kmMOnQISoLR3R20ItkaNwJddUnvlpFVHsooouZWJDZ
6MY7F8e30sgd8dlMkBoFj4+C5wzDclUjxqyFC
=hqrc
```

-----END PGP PUBLIC KEY BLOCK-----

## URLs

- Siteweb: `hxxp://babukq4e2p4wu4iq.onion/login.php?id= <ID_VICTIME>`
- Dedicated leak Site (DLS): `hxxp://gtmx56k4hutn3ikv.onion`

## Hashs

### SHA256

- `afcf265a1dcd9eab5aab270d48aa561e4ddeb71c05e32c857d3b809bb64c0430`
- `704a0fa7de19564bc743fb68aa0652e38bf86e8ab694bc079b15f945c85f4320`
- `1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02`
- `550771bbf8a3e5625d6ec76d70ed86f6e443f07ce80ff73e47f8249ddd72a8cf`
- `30fcff7add11ea6685a233c8ce1fc30abe67044630524a6eb363573a4a9f88b8`
- `8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9`
- `58ccba4fb2b3ed8b5f92adddd6ee331a6afdedfc755145e0432a7cb324c28053`
- `3dda3ee9164d6815a18a2c23651a53c35d52e3a5ad375001ec824cf532c202e6`
- `ef326291febe84d6b39d2e5cea7e99a02407892729d688c27dcc444a2ae0b544`
- `8140004ff3cf4923c928708505754497e48d26d822a95d63bd2ed54e14f19766`

### SHA1

- `b040f2bdee3999aad415396f9f79e43b2aa9452b`
- `9d9c33493aa0e1a12efe472e7cfc74bebec9a270`
- `21febf36da69c8a611a9eae5cc826cfd5684d7`
- `499c21991aecc205fd9c64784909d94eb34a9a71`
- `ca205a28b8dbd74c60fdeaf522804d5a2a45dd0b`
- `320d799beef673a98481757b2ff7e3463ce67916`
- `72cad5a81ce546b42844b5b8fc2ab55e99f2b5d4`
- `7925725cfb04d796f497e5142cba62860fbf87a9`

### MD5

- `be76ed428523b9aefe706aeaa72bb6b2`
- `8b9a0b44b738c7884e6a14f4cb18aff`
- `e25e078255b56b47897ac96a7842de92`
- `64f7ac45f930fe0ae05f6a6102ddb511`
- `dd7f88a68a76acc0be9eb0515d54a82a`
- `e10713a4a5f635767dcd54d609bed977`
- `67e49cfcd12103b5ef2f9f331f092dbe`
- `9478050023c7f8668df4fc39b0ddd79c`

<b>Vhash</b>	0340466d15555068z3ahz2lz 0340566d1555155088z3dhz2lz 0240466d15555az33hz13z1fz
<b>Fuzzyhash</b>	768:S4DnL4DGrUVvP917yo6Xee7amb26ZghLybmGJ87tHvg7jzTzt:SiLd639NdCbXZxby tH6 768:73QN4DGrqBLP977YowZe478mR26fgjVyBm8Je7tFv/7iJFzMW:7gdoT93DaRXf5B+ tFcJe 768:oD4vI0cdqNwbWSPHEV8X3QEJPTgyvZ+KgoS2:u478EkR2uUoS 192:+U0PXSFXQKapFmtHlOvvcQsfN2aFW/qiXSOGyvCcjjporSQ1Ba3DLUIk0kxVbE0z:+ UR4mSC41i0dvCk21UcNOSdCFh7Vd+ 768:C4iPMK4DGro0BLP9L7ooDee/7xm626AgkIyamLJT7tevG7FZFz:C4e3do8T9HzC6XA 3aatek 768:Fwi7jIIQoMmp9079ob2eH7pmC26IgMwym9Jr7tGvu7t9p:FwUyK9ueSCXIXiatG 768:xDkvIOcdqNwbWSPHEV8X3QEJPTgyYcKgoSr:1k78EkR28oS 384:n0qU/Gju0TUvqglfh5X8Y7we5LtS59tDvPrHC667YXdu9LLaq5SRgFvoR4+ YuS6s:Meyvq+sY7wLpvDHxq5ioH+8Q
<b>TLSH</b>	CCE218116F555276F3E2813062BB92B7C83838218376C2D723C019E9FA756A8BD39F57 BEE219116F455276F3D2C135227BA2B7D83438208376C2D7238019E9FA696A8BE3DF57 E403B3122E5BD62CC2C1B2315221E5B5C53A5C6053F1729B63C015EB3E62EECE1BDF66 DDA229146FE5A534F2A2C97966B742B5CC393C30131780DBA7C01DC52AB54E5BA3DA17 D9E219216F455276F3E2813062BB92A7C83838208376C1D727C019E9FA656E8BD3DF57 T11AC2F9206F14D2B7F3D19171A27B95F7DA392C60537280D326C035EAF938294B639B 57 CD03A3122F5BD62CC2C1A2315221E5B5C52A5CA053F1729B63C015EB3E62EECE1BDF66 47E229676FB15430F1A6C4B426B59259E43AB430875643A7BFD006CA64E0 AE9EE3CF07 D0D2E8166B81D432F6A24C71663A12A7E63E29344733C3AB77807DF839F8 AD15535B0B
<b>Imphash</b>	a07d82bc384cbae972c1524ff6fb5cc1 0c89550c464c4d83cfa77b67633170e7 7f859628bfaa9e07b62f58214585994e 6c36a54c4339bbd0f14fcf7de525cbb6
<b>Poids</b>	31 232 octets 31 744 octets 39 424 octets 22 528 octets 31 744 octets 31 668 octets 39 424 octets
<b>PE section counter</b>	4 ou 5 (v3, v4)
<b>PE entry point</b>	35152

# First version of the Babuk' Dedicated Leak Site

[ABOUT US](#) | [RULES](#)

## Home Page of Leaks site

We do not audit next categories of organizations:

\*Hospitals (except private plastic surgery clinics, private dental clinics)

\*Any non-profitable charitable foundation (except the foundations who help LGBT and BLM)

\*Schools (except the major universities)

\*Companies with annual revenue less than 4 mln\$ (info about revenue we take from zoominfo)

**[REDACTED] stolen more 1TB data**  
views: 93 | Published: 2021-01-27 22:34:46

**[REDACTED]**  
views: 1908 | Published: 2021-01-24 03:28:55

**[REDACTED] 100gb data by BABUK locker**  
views: 3038 | Published: 2021-01-17 12:38:24

**Official request to [REDACTED]**  
views: 3150 | Published: 2021-01-15 01:44:08

**[REDACTED]**  
views: 3463 | Published: 2021-01-14 21:38:37

**Figure 37**  
Home page (Wall of shame) of the Babuk' Dedicated Leak Site.

[<<HOME](#)

### **Payment Rules:**

- We will give Bitcoin wallet to a client directly in chat. (please request BTC wallet once you ready for payment)
- Client should send at first 1 bitcoin on our wallet, just for verification purposes. After we will confirm this transaction, client can send the whole amount.
- After the 1st confirm on blockchain would be received, we will initiate process of providing you with all that was claimed

### **HOW-to-USE DECRYPTOR**

- Before install it on any server or host, you should turn off Anti-virus software and windows defender, also better switch off internet connection.
- Than you have to RUN program "As Administrator", after decryption will be finished you will get the message,so wait for it.
- You have to copy and paste Decryption tool on each Locked server or host and execute it there.

**Figure 38**  
*Payment Rules'*  
*section of the*  
*Babuk' Dedicated*  
*Leak Site*

<<HOME

## About Us

### What is BABUK?

Non malicious, specialized software, created with purpose to show the security issues inside the corporate networks.

Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to protect its keys and encrypt files

What issues are we talking about and why we are not a criminals?

In our understanding - we are some kind of a cyberpunks, we randomly test corporate networks security and in case of penetration, we ask money, and publish the information about threats and vulnerabilities we found, in our blog if company doesn't want to pay.

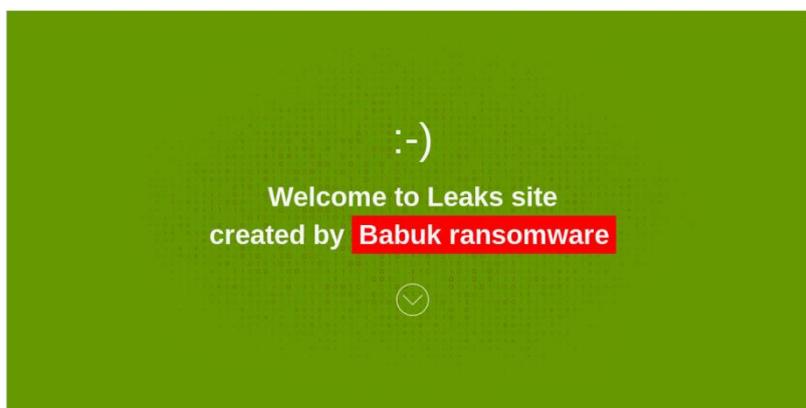
For example, imagine the situation: villians intruding the building company's network (huge developer who specializes on sport objects), those villians doesn't care about money, they are crazy fanatics from terroristic organization, they get the blueprints and schematics... just think what going to be furter..

Our audit is not the worst thing can happen to your company, but think twice, pay by money, of maybe the people lives...

**Figure 39**  
*About Us section of the Babuk' Dedicated Leak Site*

# Second version of the Babuk's Dedicated Leak Site

**Figure 40**  
*Homepage of the rebranded version of the Babuk' Dedicated Leak Site (taken the 4<sup>th</sup> of March, 2021).*



# Detection rule: Yara rule<sup>47</sup>

```
rule VasaLocker_1 : malware {
  meta:
    description = "VasaLocker aka Babuk ransomware, january 2021."
    researcher = "Alexandre MATOUSEK"
    date = "18-01-21"
    source = "OCD"
    category = "ransom"
  strings:
    $ = "BY VASA LOCKER" ascii
    $ = "babuk" ascii
    $ = "-lan" ascii
    $ = "RECOVER" ascii
    $ = "SystemFunction036" ascii
    $ = "DECR.txt" wide nocase
    $ = "vasa_dbg.txt" wide
    $ = "ecdh_pub_k.bin" wide
  condition:
    all of them
}
```

```
rule BabukRansomware {
  meta:
    description = "YARA rule for Babuk Ransomware"
    reference = "http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/"
    author = "@cPeterr"
    date = "2021-01-03"
    rule_version = "v1"
    malware_type = "ransomware"
    tlp = "white"
  strings:
    $lanstr1 = "-lanfirst"
    $lanstr2 = "-lansecond"
    $lanstr3 = "-nolan"
    $str1 = "BABUK LOCKER"
    $str2 = ".__NIST_K571__" wide
    $str3 = "How To Restore Your Files.txt" wide
    $str4 = "ecdh_pub_k.bin" wide
  condition:
    all of ($str*) and all of ($lanstr*)
}
```

A Yara rule given by the researcher in cybersecurity who observed Babuk<sup>48</sup> for the first time:

```
Rule
Ran_BabukLockers_Jan_2021_1 {
  meta:
    description = "Detect the BabukLocker ransomware"
    author = "Arkbird_SOLG"
    reference = "Internal Research"
    date = "2020-01-03"
```

<sup>47</sup> <https://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/>

<sup>48</sup> [https://github.com/StrangereallIntel/DailyIOC/blob/master/2021-01-02/BabukLocker/Ran\\_BabukLockers\\_Jan\\_2021\\_1.yar](https://github.com/StrangereallIntel/DailyIOC/blob/master/2021-01-02/BabukLocker/Ran_BabukLockers_Jan_2021_1.yar)

```

hash1
"8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9"
level = "Experimental"
strings:
// sequence of the discovery process from imported DLL (TTPs)
$seq1 = { 55 8b ec 83 ec 14 a1 b0 81 40 00 33 c5 89 45 fc c7 45 f8 ff ff ff ff c7
45 f4 00 40 00 00 8d 45 f0 50 8b 4d 08 51 6a 13 6a 00 6a 02 e8 85 2b 00 00 85 c0
0f 85 a3 00 00 00 8b 55 f4 52 e8 ae 06 00 00 83 c4 04 89 45 08 83 7d 08 00 0f 84
81 00 00 00 8d 45 f4 50 8b 4d 08 51 8d 55 f8 52 8b 45 f0 50 e8 55 2b 00 00 85 c0
75 5c c7 45 ec 00 00 00 eb 09 8b 4d ec 83 c1 01 89 4d ec 8b 55 ec 3b 55 f8 73
40 8b 45 ec c1 e0 05 8b 4d 08 8b 54 01 0c 83 e2 02 74 14 8b 45 ec c1 e0 05 03 45
}
// sequence of the parsing arguments + shutdown process
$seq2 = { 68 68 22 40 00 b8 04 00 00 00 c1 e0 00 8b 8d 9c fd ff ff 8b 14 01 52
ff 15 b8 90 40 00 85 c0 75 0c c7 85 b0 fd ff ff 01 00 00 00 eb 58 68 74 22 40 00 b8
04 00 00 00 c1 e0 00 8b 8d 9c fd ff ff 8b 14 01 52 ff 15 b8 90 40 00 85 c0 75 0c c7
85 b0 fd ff ff 00 00 00 00 eb 2b 68 80 22 40 00 b8 04 00 00 00 c1 e0 00 8b 8d 9c fd
ff ff 8b 14 01 52 ff 15 b8 90 40 00 85 c0 75 0a c7 85 b0 fd ff ff ff ff ff ff e9 55 ff ff ff
6a 00 6a 00 ff 15 a8 90 40 00 e8 aa 04 00 00 e8 05 }
// sequence of write op (key) in the disk
$seq3 = { 83 c4 0c 68 f4 00 00 00 8d 85 f4 fd ff ff 50 68 88 22 40 00 ff 15 6c 90
40 00 68 98 22 40 00 8d 8d f4 fd ff ff 51 ff 15 c4 90 40 00 c7 85 ec fd ff ff 00 00 00
00 6a 00 68 80 00 00 00 6a 01 6a 00 6a 01 68 00 00 00 40 8d 95 f4 fd ff ff 52 ff 15
70 90 40 00 89 85 98 fd ff ff 83 bd 98 fd ff ff 0f 84 2e 03 00 00 6a 00 8d 85 ec fd
ff ff 50 68 90 00 00 00 68 78 82 40 00 8b 8d 98 fd ff ff 51 ff 15 90 90 }
$s1 = "\\ecd_h_pub_k.bin" fullword wide
$s2 = "ntuser.dat.log" fullword wide
$s3 = "cmd.exe" fullword ascii
$s4 = "/c vssadmin.exe delete shadows /all /quiet" fullword wide
$s5 = { 5c 00 5c 00 3f 00 5c 00 00 00 00 00 3a 00 00 00 98 2f }
condition:
uint16(0) == 0x5a4d and filesize > 15KB and 2 of ($seq*) and 3 of ($s*)
}

```

The following one is a detection rule written by ReversingLabs<sup>49</sup>:

```

rule
Win32_Ransomware_Babuk :
tc_detection malicious
{
meta:
author = "ReversingLabs"
source = "ReversingLabs"
status = "RELEASED"
sharing = "TLP:WHITE"
category = "MALWARE"
malware = "BABUK"
description = "Yara rule that detects Babuk ransomware."

tc_detection_type = "Ransomware"
tc_detection_name = "Babuk"
tc_detection_factor = 5

strings:
$find_files = {
55 8B EC 81 EC ?? ?? ?? ?? A1 ?? ?? ?? ?? 33 C5 89 45 ?? 68 ?? ?? ?? ?? E8 ??
?? ??
?? 83 C4 ?? 89 85 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 0F 84 ?? ?? ?? ?? 8B 45 ?? 50
8B
8D ?? ?? ?? ?? 51 FF 15 ?? ?? ?? ?? 68 ?? ?? ?? ?? 8B 95 ?? ?? ?? ?? 52 FF 15 ??
??
?? ?? 8D 85 ?? ?? ?? ?? 50 8B 8D ?? ?? ?? ?? 51 FF 15 ?? ?? ?? ?? 89 85 ?? ?? ??
??
}
}

```

<sup>49</sup> <https://github.com/reversinglabs/reversinglabs-yara-rules/blob/develop/yara/ransomware/Win32.Ransomware.Babuk.yara>

```
83 BD ?? ?? ?? ?? 0F 84 ?? ?? ?? C7 85 ?? ?? ?? ?? ?? ?? EB ?? 8B 95
??
?? ?? ?? 83 C2 ?? 89 95 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 73 ?? 8B 85 ?? ?? ?? ??
8B
0C 85 ?? ?? ?? ?? 51 8D 95 ?? ?? ?? ?? 52 FF 15 ?? ?? ?? ?? 85 C0 75 ?? E9 ??
?? ??
?? E9 ?? ?? ?? ?? EB ?? 8B 45 ?? 50 8B 8D ?? ?? ?? ?? 51 FF 15 ?? ?? ?? ?? 68 ??
??
?? ?? 8B 95 ?? ?? ?? ?? 52 FF 15 ?? ?? ?? ?? 8D 85 ?? ?? ?? ?? 50 8B 8D ?? ?? ??
??
51 FF 15 ?? ?? ?? ?? 8B 95 ?? ?? ?? ?? 83 E2 ?? 74 ?? 83 7D ?? ?? ?? ?? 8B 45
?? 83
C0 ?? 50 8B 8D ?? ?? ?? ?? 51 E8 ?? ?? ?? ?? 83 C4 ?? E9 ?? ?? ?? ?? 68 ?? ?? ??
??
8D 95 ?? ?? ?? ?? 52 FF 15 ?? ?? ?? ?? 85 C0 74 ?? 8D 85 ?? ?? ?? ?? 50 FF 15
?? ??
?? ?? 89 85 ?? ?? ?? ?? EB ?? 8B 8D ?? ?? ?? ?? 83 E9 ?? 89 8D ?? ?? ?? ?? 83
BD ??
?? ?? ?? ?? 7C ?? 8B 95 ?? ?? ?? ?? 0F B7 84 55 ?? ?? ?? ?? 83 F8 ?? 75 ?? 68 ??
??
?? ?? 8B 8D ?? ?? ?? ?? 8D 94 4D ?? ?? ?? ?? 52 FF 15 ?? ?? ?? ?? 85 C0 75 ??
EB ??
EB ?? EB ?? EB ?? EB ?? 8B 85 ?? ?? ?? ?? 50 E8 ?? ?? ?? ?? 83 C4 ?? 8D 8D ??
?? ??
?? 51 8B 95 ?? ?? ?? ?? 52 FF 15 ?? ?? ?? ?? 85 C0 0F 85 ?? ?? ?? ?? 8B 85 ?? ??
??
?? 50 FF 15
}

$encrypt_files_p1 = {
55 8B EC B8 ?? ?? ?? ?? E8 ?? ?? ?? ?? A1 ?? ?? ?? ?? 33 C5 89 45 ?? C7 85 ??
?? ??
?? ?? ?? ?? ?? 68 ?? ?? ?? ?? 8B 45 ?? 50 FF 15 ?? ?? ?? ?? 6A ?? 68 ?? ?? ?? ??
6A
?? 6A ?? 6A ?? 68 ?? ?? ?? ?? 8B 4D ?? 51 FF 15 ?? ?? ?? ?? 89 85 ?? ?? ?? ?? 83
BD
?? ?? ?? ?? ?? 0F 84 ?? ?? ?? ?? 8D 95 ?? ?? ?? ?? 52 8B 85 ?? ?? ?? ?? 50 FF 15
??
?? ?? ?? 6A ?? 6A ?? 6A ?? 6A ?? 6A ?? 8B 8D ?? ?? ?? ?? 51 FF 15 ?? ?? ?? ?? 89
85
?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 0F 84 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 0F 8C ??
??
?? ?? 7F ?? 81 BD ?? ?? ?? ?? ?? ?? ?? ?? 0F 86 ?? ?? ?? ?? 6A ?? 68 ?? ?? ?? ??
8B
95 ?? ?? ?? ?? 52 8B 85 ?? ?? ?? ?? 50 E8 ?? ?? ?? ?? 6A ?? 6A ?? 52 50 E8 ?? ??
??
?? 89 85 ?? ?? ?? ?? 89 95 ?? ?? ?? ?? 0F 57 C0 66 0F 13 85 ?? ?? ?? ? ? EB
?? 8B 8D
?? ?? ?? ?? 83 C1 ?? 8B 95 ?? ?? ?? ?? 83 D2 ?? 89 8D ?? ?? ?? ?? 89 95 ?? ?? ??
??
83 BD ?? ?? ?? ?? ?? 0F 8F ?? ?? ?? ?? 7C ?? 83 BD ?? ?? ?? ?? ?? 0F 83 ?? ?? ??
??
8B 85 ?? ?? ?? ?? 50 8B 8D ?? ?? ?? ?? 51 8B 95 ?? ?? ?? ?? 52 8B 85 ?? ?? ??
?? 50
}

$encrypt_files_p2 = {
E8 ?? ?? ?? ?? 6A ?? 68 ?? ?? ?? ?? 52 50 E8 ?? ?? ?? ?? 89 85 ?? ?? ?? ?? 89 95
??
?? ?? ?? 68 ?? ?? ?? ?? 8B 8D ?? ?? ?? ?? 51 8B 95 ?? ?? ?? ?? 52 68 ?? ?? ?? ??
8B
85 ?? ?? ?? ?? 50 FF 15 ?? ?? ?? ?? 89 85 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 74 ??
68
?? ?? ?? ?? 8B 8D ?? ?? ?? ?? 51 8B 95 ?? ?? ?? ?? 52 68 ?? ?? ?? ?? 6A ?? 68 ??
??
?? ?? E8 ?? ?? ?? ?? 83 C4 ?? 68 ?? ?? ?? ?? 8B 85 ?? ?? ?? ?? 50 8B 8D ?? ?? ??
??
51 68 ?? ?? ?? ?? 6A ?? 68 ?? ?? ?? ?? E8 ?? ?? ?? ?? 83 C4 ?? 8B 95 ?? ?? ?? ??
52
FF 15 ?? ?? ?? ?? E9 ?? ?? ?? ?? E9 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 0F 8C ?? ??
??
??
```

```
68    ?? 7F ?? 83 BD ?? ?? ?? ?? ?? 0F 86 ?? ?? ?? ?? 8B 85 ?? ?? ?? ?? 50 6A ?? 6A ??
??    ?? ?? ?? ?? 8B 8D ?? ?? ?? ?? 51 FF 15 ?? ?? ?? ?? 89 85 ?? ?? ?? ?? 83 BD ?? ??
??    ?? ?? 74 ?? 8B 95 ?? ?? ?? ?? 52 8B 85 ?? ?? ?? ?? 50 8B 8D ?? ?? ?? ?? 51 68
?? ??    ?? ?? 6A ?? 68 ?? ?? ?? ?? E8 ?? ?? ?? ?? 83 C4 ?? 8B 95 ?? ?? ?? ?? 52 8B 85 ??
??    ?? ?? 50 8B 8D ?? ?? ?? ?? 51 68 ?? ?? ?? ?? 6A ?? 68 ?? ?? ?? ?? E8 ?? ?? ?? ??
83    }
$encrypt_files_p3 = {
C4 ?? 8B 95 ?? ?? ?? ?? 52 FF 15 ?? ?? ?? ?? 8B 85 ?? ?? ?? ?? 50 FF 15 ?? ?? ??
??    8B 8D ?? ?? ?? ?? 51 FF 15 ?? ?? ?? ?? 8B 95 ?? ?? ?? ?? 52 FF 15 ?? ?? ?? ?? 68
??    ?? ?? ?? E8 ?? ?? ?? ?? 83 C4 ?? 89 85 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 74 ?? 8B
45    ?? 50 8B 8D ?? ?? ?? ?? 51 FF 15 ?? ?? ?? ?? 68 ?? ?? ?? ?? 8B 95 ?? ?? ?? ?? 52
FF    15 ?? ?? ?? ?? 6A ?? 8B 85 ?? ?? ?? ?? 50 8B 4D ?? 51 FF 15 ?? ?? ?? ?? 8B 95
?? ??    ?? ?? 52 E8 ?? ?? ?? ?? 83 C4 ?? E9 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 0F 84 ?? ??
??    ?? 6A ?? 6A ?? 8D 45 ?? 50 E8 ?? ?? ?? ?? 83 C4 ?? 8D 4D ?? 51 6A ?? 8D 95 ??
?? ??    ?? 52 E8 ?? ?? ?? ?? 85 C0 0F 85 ?? ?? ?? ?? 6A ?? 6A ?? 6A ?? 6A ?? 8D 45 ??
50 6A    ?? 8B 8D ?? ?? ?? ?? 51 E8 ?? ?? ?? ?? 85 C0 0F 85 ?? ?? ?? ?? C7 85 ?? ?? ?? ??
??    ?? ?? ?? 8D 95 ?? ?? ?? ?? 52 8D 85 ?? ?? ?? ?? 50 8D 8D ?? ?? ?? ?? ?? 51 8D 95
?? ??    ?? ?? 52 8B 85 ?? ?? ?? ?? 50 E8 ?? ?? ?? ?? 85 C0 0F 85 ?? ?? ?? ?? C7 85 ?? ??
??    ?? ?? ?? ?? ?? EB ?? 8B 8D ?? ?? ?? ?? 83 C1 ?? 89 8D ?? ?? ?? ?? 8B 95 ?? ?? ??
??    3B 95 ?? ?? ?? ?? 0F 83 ?? ?? ?? ?? 69 85 ?? ?? ?? ?? ?? ?? ?? ?? 83 BC 05 ?? ??
??    ?? ?? 0F 84 ?? ?? ?? ?? 69 8D ?? ?? ?? ?? ?? ?? ?? ?? 81 BC 0D ?? ?? ?? ?? ?? ??
??    ?? 74 ?? FF 15 ?? ?? ?? ?? 69 95 ?? ?? ?? ?? ?? ?? ?? ?? 3B 84 15 ?? ?? ?? ?? 74
??    69 85 ?? ?? ?? ?? ?? ?? ?? ?? 8B 8C 05 ?? ?? ?? ?? 51 6A ?? 68 ?? ?? ?? ?? FF 15
??    ?? ?? ?? 89 85 ?? ?? ?? ?? 83 BD ?? ?? ?? ?? ?? 74 ?? 6A ?? 8B 95 ?? ?? ?? ?? 52
FF    15 ?? ?? ?? ?? 68 ?? ?? ?? ?? 8B 85 ?? ?? ?? ?? 50 FF 15 ?? ?? ?? ?? 8B 8D ?? ??
??    ?? 51 FF 15 ?? ?? ?? ?? E9 ?? ?? ?? ?? 8B 95 ?? ?? ?? ?? 52 E8 ?? ?? ?? ?? C7 85
??    ?? ?? ?? ?? ?? ?? E9 ?? ?? ?? ?? 8B 4D ?? 33 CD E8 ?? ?? ?? ?? 8B E5 5D C3
}
$enum_resources = {
55 8B EC 83 EC ?? A1 ?? ?? ?? ?? 33 C5 89 45 ?? C7 45 ?? ?? ?? ?? C7 45 ??
?? ??    ?? ?? 8D 45 ?? 50 8B 4D ?? 51 6A ?? 6A ?? 6A ?? E8 ?? ?? ?? ?? 85 C0 0F 85 ??
?? ??    ?? 8B 55 ?? 52 E8 ?? ?? ?? ?? 83 C4 ?? 89 45 ?? 83 7D ?? ?? 0F 84 ?? ?? ?? ??
8D 45    ?? 50 8B 4D ?? 51 8D 55 ?? 52 8B 45 ?? 50 E8 ?? ?? ?? ?? 85 C0 75 ?? C7 45 ??
?? ??    ?? ?? EB ?? 8B 4D ?? 83 C1 ?? 89 4D ?? 8B 55 ?? 3B 55 ?? 73 ?? 8B 45 ?? C1 E0
?? 8B    4D ?? 8B 54 01 ?? 83 E2 ?? 74 ?? 8B 45 ?? C1 E0 ?? 03 45 ?? 50 E8 ?? ?? ?? ??
83 C4    ?? EB ?? 6A ?? 8B 4D ?? C1 E1 ?? 8B 55 ?? 8B 44 0A ?? 50 E8 ?? ?? ?? ?? 83 C4
?? EB    ?? EB ?? 8B 4D ?? 51 E8 ?? ?? ?? ?? 83 C4 ?? 8B 55 ?? 52 E8 ?? ?? ?? ?? 8B 4D
?? 33
```

```

        CD E8 ?? ?? ?? ?? 8B E5 5D C3
    }

    condition:
        uint16(0) == 0x5A4D and
        (
            $find_files
        ) and
        (
            all of ($encrypt_files_p*)
        ) and
        (
            $enum_resources
        )
    }
}

```

```

/*
YARA Rule Set50
Author: Oxthreatintel
Date: 2021-04-17
Identifier: Babuk Ransom
Reference: Blog from Oxthreatintel: https://medium.com/@Oxthreatintel/internals-of-babuk-ransomware-bb6aa9618857
*/
/* Rule Set */
rule babak_ransom {
    meta:
        description = "Babuk_Ransom - file babak_ransom. exe"
        author = "Oxthreatintel"
        reference = "Blog from Oxthreatintel: https://medium.com/@Oxthreatintel/internals-of-babuk-ransomware-bb6aa9618857"
        date = "2021-04-17"
        hash1 = "18e299d4331cfff805275b21f33be0a3bd3d1d9ce72a79ba78d2f32dd657bfbb"

    strings:
        $s1 = "mydesktopservice.exe" fullword wide
        $s2 = "tbirdconfig.exe" fullword wide
        $s3 = "ocomm.exe" fullword wide
        $s4 = "sqbcoreservice.exe" fullword wide
        $s5 = "oracle.exe" fullword wide
        $s6 = "ocssd.exe" fullword wide
        $s7 = "dbsnmp.exe" fullword wide
        $s8 = "synctime.exe" fullword wide
        $s9 = "agntsvc.exe" fullword wide
        $s10 = "isqlplussvc.exe" fullword wide
        $s11 = "xfssvccon.exe" fullword wide
        $s12 = "encsvc.exe" fullword wide
        $s13 = "mydesktopqos.exe" fullword wide
        $s14 = "dbeng50.exe" fullword wide
        $s15 = "mispub.exe" fullword wide
        $s16 = "steam.exe" fullword wide
        $s17 = "visio.exe" fullword wide
        $s18 = "BackupExecManagementService" fullword ascii
        $s19 = "BackupExecDiveciMediaService" fullword ascii
        $s20 = "BackupExecRPCService" fullword ascii

    condition:
        uint16(0) == 0x5a4d and filesize < 200KB and
        8 of them
}

```

<sup>50</sup> <https://Oxthreatintel.medium.com/internals-of-babuk-ransomware-bb6aa9618857>

## About Sogeti

---

Part of the Capgemini Group, Sogeti operates in more than 100 locations globally. Working closely with clients and partners to take full advantage of the opportunities of technology, Sogeti combines agility and speed of implementation to tailor innovative future-focused solutions in Digital Assurance and Testing, Cloud and Cybersecurity, all fueled by AI and automation. With its hands-on 'value in the making' approach and passion for technology, Sogeti helps organizations implement their digital journeys at speed.

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 270,000 team members in nearly 50 countries. With its strong 50 year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2020 global revenues of €16 billion. Get the Future You Want.

Visit us at [www.sogeti.com](http://www.sogeti.com)