بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

تحلیل فنی باج‌افزار LockBit 3.0 (Black)

گزارش فنی

شناسه سند	MaherReports_14011023
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۴۰۱/۱۰/۲۳
طبقه‌بندی سند	عادی

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک ۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

فهرست مطالب

۱ مقدمه

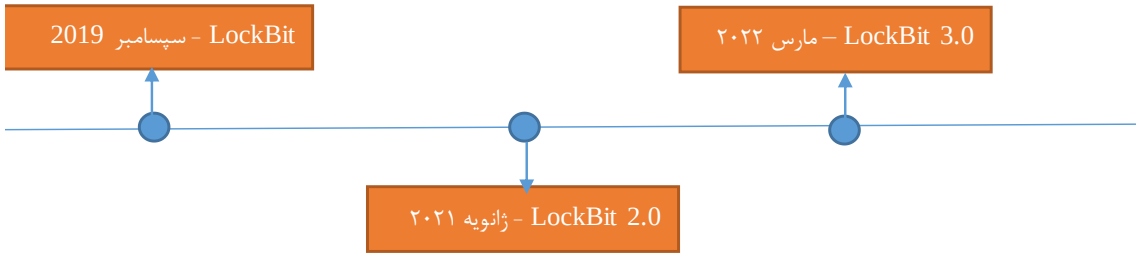
در سه ماه آخر سال ۲۰۱۹، باج‌افزار LockBit با نسخه اولیه خود که به ABCD معروف بود شروع به کار کرد، اما نتوانست توجهات خاصی را به خود جلب کند و قربانیان زیادی نداشت. در ژانویه سال ۲۰۲۱ برنامه‌نویسان LockBit نسخه دیگری از آن را با نام LockBit 2.0 عرضه کردند تا بنوانند حملات مؤثرتری را به انجام برسانند. سپس در مارس ۲۰۲۲ نسخه بتای LockBit 3 عرضه شد که درنهایت در ماه ژوئن همان سال نسخه نهایی آن منتشر گردید. بر اساس آزمایشات صورت گرفته، نسخه سوم این باج‌افزار برای فعالیت خود احتیاجی به اتصال به اینترنت ندارد و بدون دسترسی مدیر سیستم (Administrator) نیز فعالیت خود را به انجام می‌رساند. باج‌افزار LockBit 3 پس اجرا در سیستم قربانی، ۵۱۲ کیلوبایت از ابتدای هر فایل را رمزگذاری و به انتهای فایل نیز ۲۴۳ بایت اضافه می‌کند. این خانواده باج‌افزاری برای گسترش هرچه بیشتر از ابتدای سال ۲۰۲۰ روند RaaS را در پیش گرفت و پس از انتشار نسخه ۳,۰ ویژگی‌های جدیدی از جمله باگ بانتی نیز به برنامه خود افزود.

۲ مشخصات فایل اجرایی

نام فایل	c690148b6baec765c65fe91ea9f282d6a411ae90c08d74d600515b3e075e21b2.exe
MD5	A8E0D56F8C67F1F7B6E592C12D87ACAB
SHA-1	ED555F0162EA6EC5B8B8BADA743CFC628D376274
SHA-256	C690148B6BAEC765C65FE91EA9F282D6A411AE90C08D74D600515B3E075E21B2
نوع فایل	Win32 EXE
اندازه فایل	159.00 KB (162816 bytes)

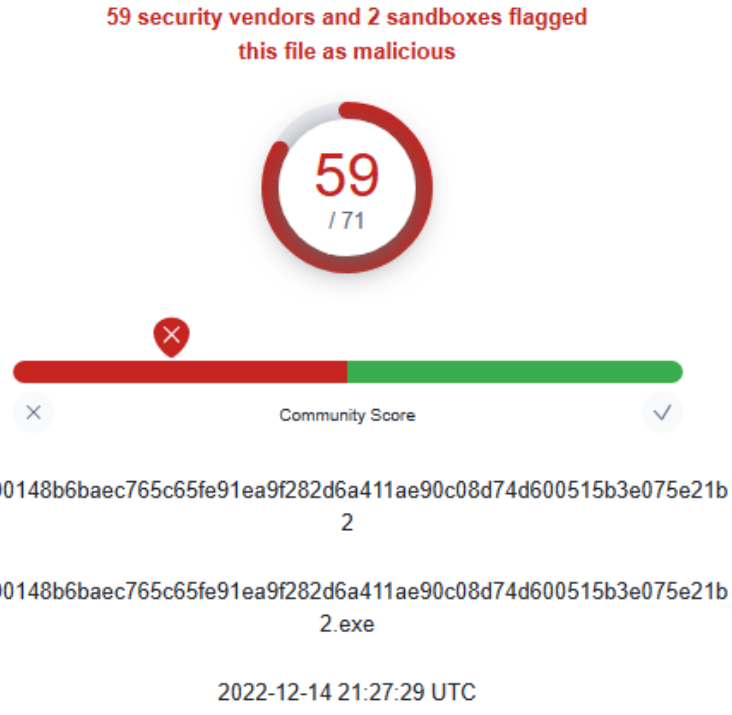
۳ شجره‌نامه

براساس شواهد موجود، تاکنون سه نسخه اصلی برای باج‌افزار LockBit منتشر شده است.



۴ میزان تهدید فایل باج‌افزار

درحال حاضر ۵۹ مورد از ۷۱ ضد بدافزار سامانه VirusTotal باج‌افزار LockBit 3.0 را به عنوان یک برنامه مخرب شناسایی می‌کنند:

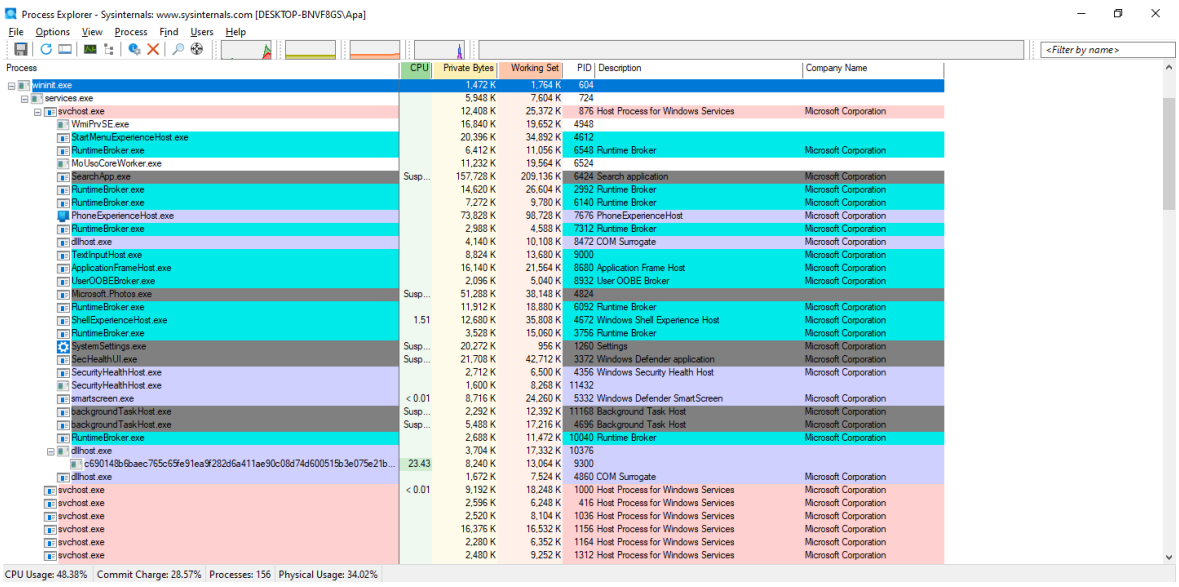


۵ تحلیل پویا

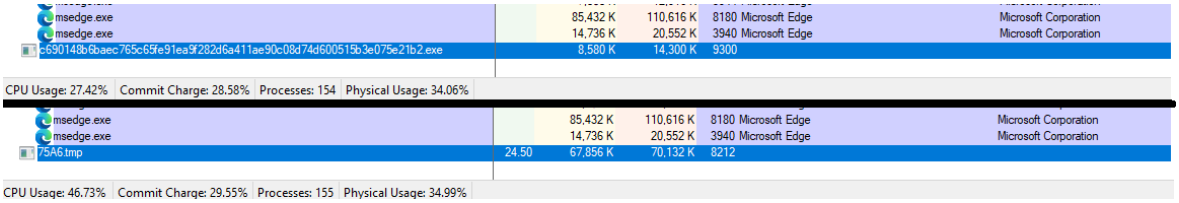
۵-۱ آناتومی حمله

پس از اجرای باج‌افزار LockBit 3.0 در محیط آزمایشگاهی، نتایج زیر مشاهده شد.

بطور کلی فعالیت این باج‌افزار از دو بخش تشکیل می‌شود که یک بخش خود فایل اصلی باج‌افزار آن را مدیریت می‌کند و بخش دوم نیز ادامه رمزگذاری فایل‌ها را انجام می‌دهد.

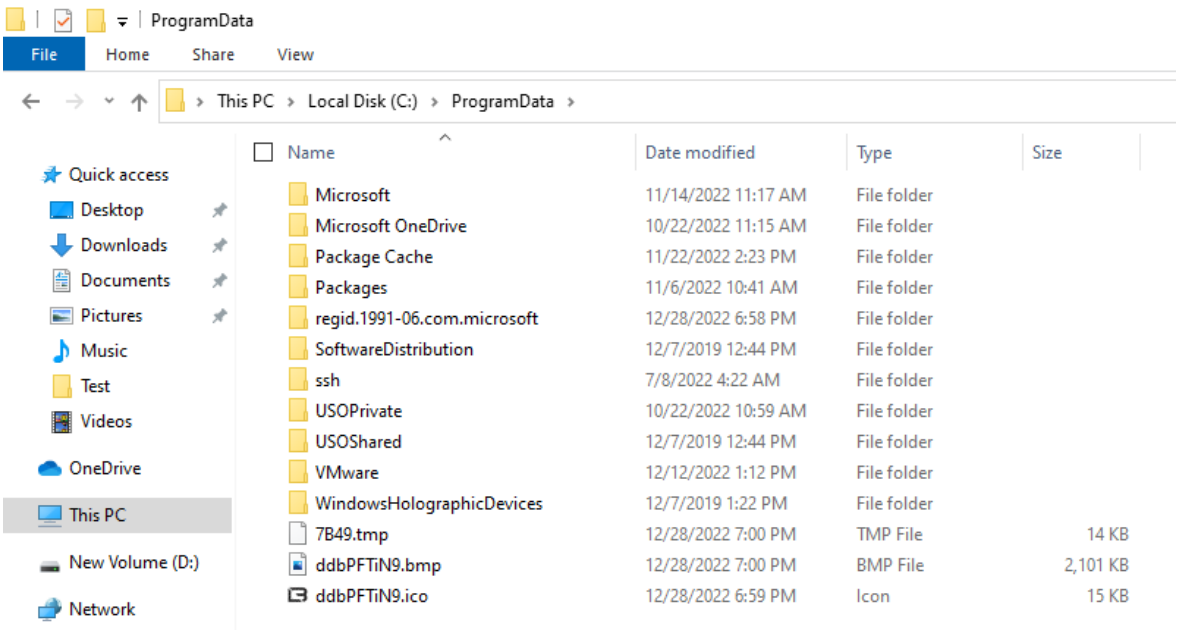


در بخش اول کلیدهای رجیستری سیستم دستکاری می‌شوند و آیکون فایل‌های رمزشده تغییر می‌کنند.

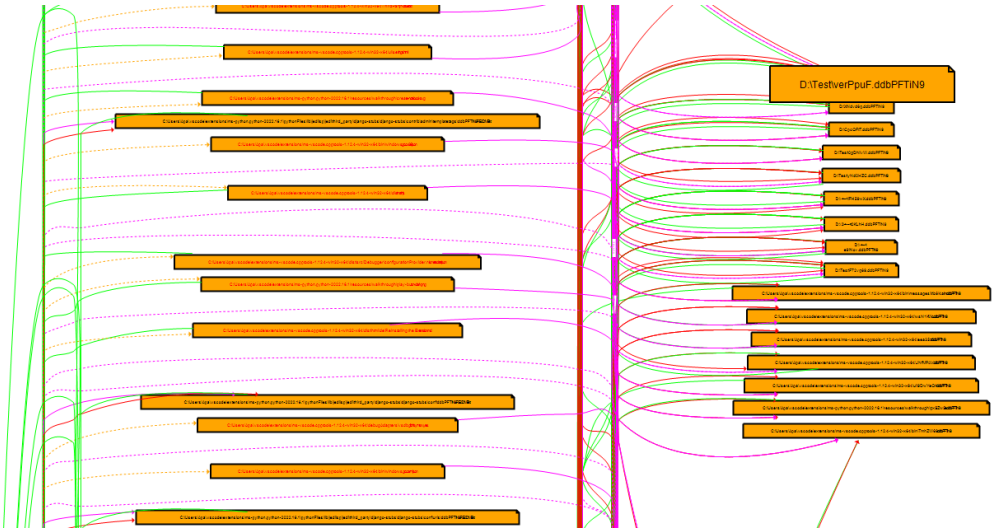


در بخش دوم نیز تغییرات اضافی دیگری در رجیستری اعمال می‌شود تا پایداری باج‌افزار در سیستم قربانی افزایش یابد.

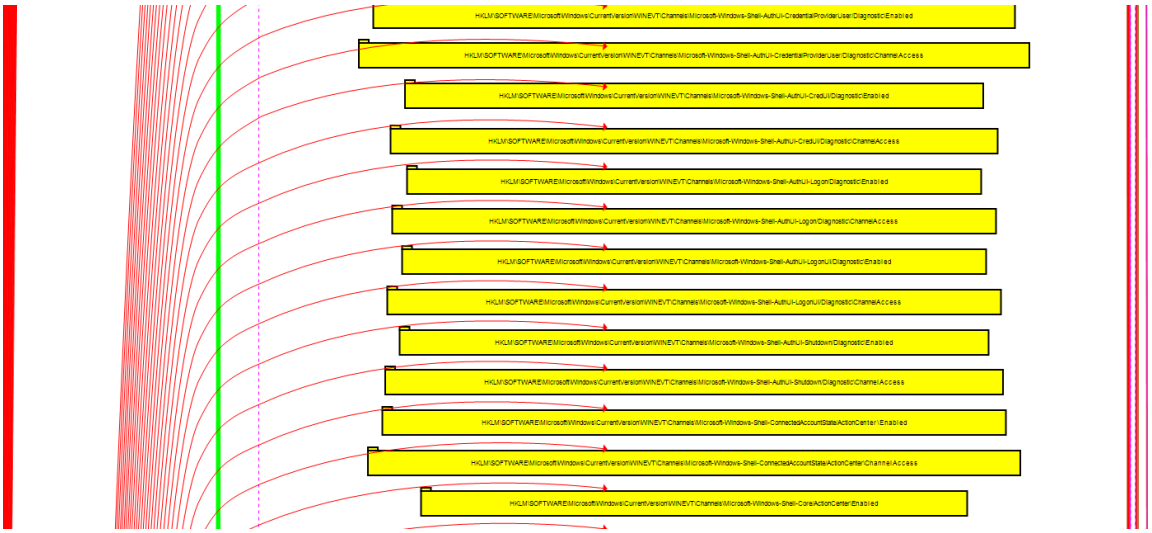
باج‌افزار LockBit 3.0 در ابتدای فعالیت خود در بخش اول در سیستم قربانی یک فایل به نام ddbPFTiN9.ico و هنگام شروع بخش دوم نیز دو فایل که یکی ddbPFTiN9.bmp و دیگری که نامی با فرمت "word-random-capital-hex-string.tmp-۴" دارد در پوشه "C:\ProgramData" ایجاد می‌کند:



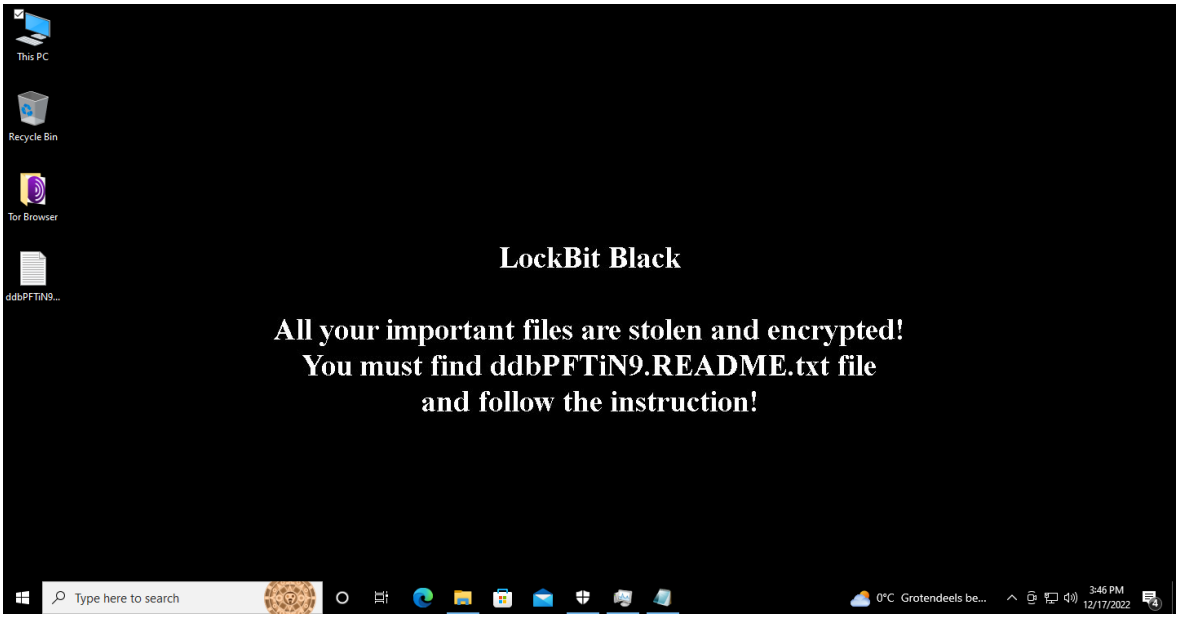
فرآیند رمزگذاری فایل‌ها به عنوان اولین فعالیت باج‌افزار بر روی سیستم قربانی، پس از دراپ کردن فایل آیکون شروع می‌شود. ابتدا تغییرات روی فایل‌ها صورت می‌گیرد و بعد از آن نام آنها تغییر می‌کند.



همچنین مقادیر بسیاری از کلیدهای رجیستری را نیز دستکاری می‌کند:

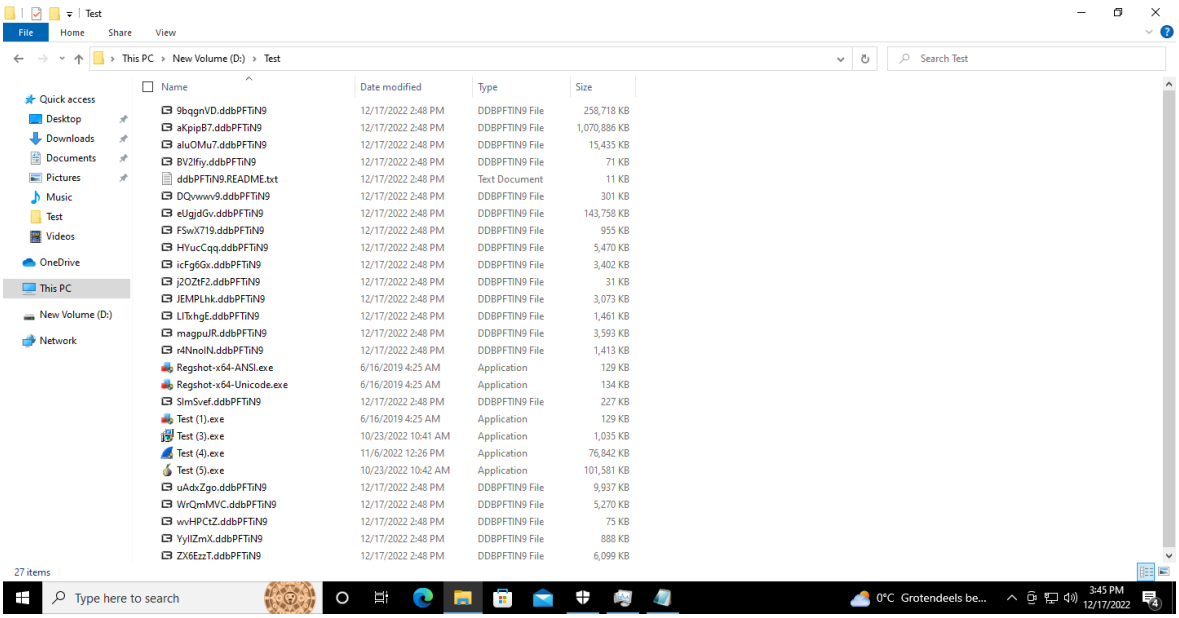


این باج‌افزار در بخش اول خود نیز تصویر دسکتاپ را تغییر می‌دهد:



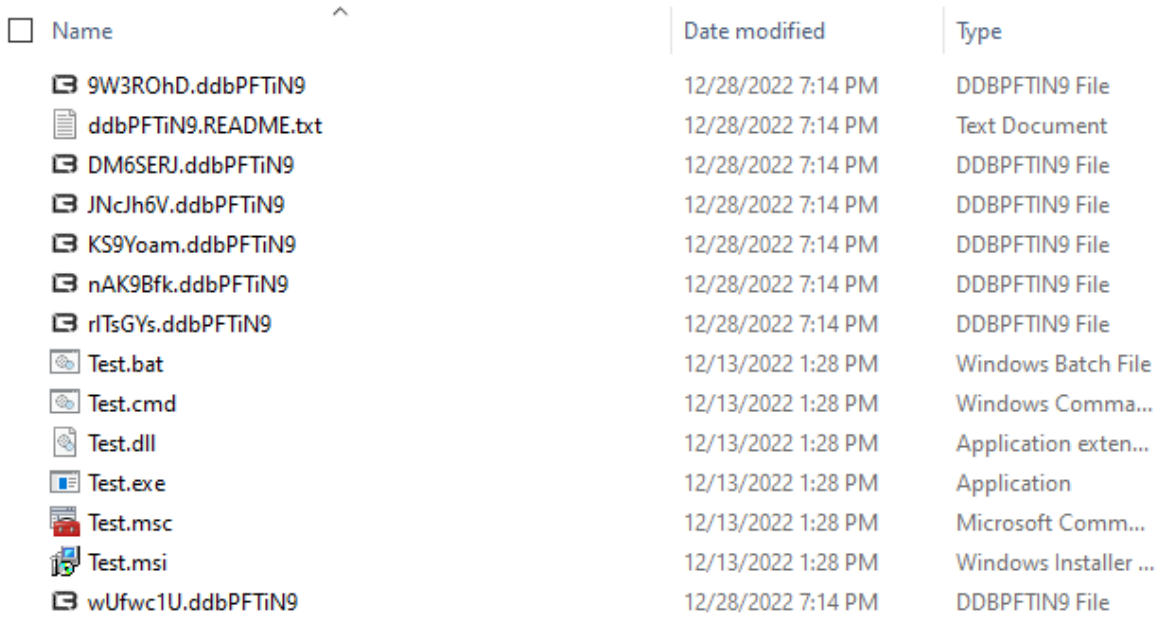
بر روی دسکتاپ پیغامی با کنتراست بالا با محتوای نام باج‌افزار "LockBit Black" و متن "تمام فایل‌های مهم شما دزدیده و رمزگذاری شده است! شما باید فایل ddbPFTiN9.README.txt را پیدا و مراحل آن‌را دنبال کنید!" مشاهده می‌شود.

تصویر زیر، فایل‌های رمزگذاری شده توسط این باج‌افزار را نشان می‌دهد.

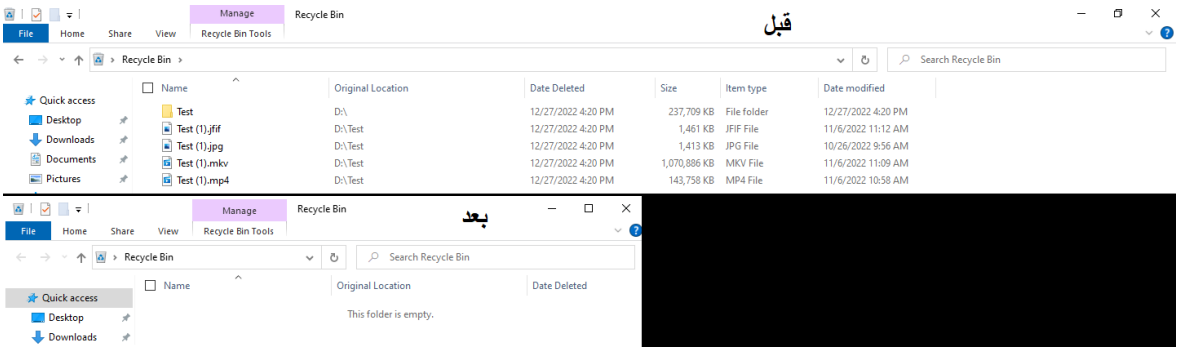


همانطور که در تصویر بالا قابل مشاهده است به انتهای هر فایل رمزشده پسوند ddbPFTiN9. اضافه شده است. الگوی نامگذاری پسوندها بصورت "7Char Random String.ddbPFTiN9" می‌باشد.

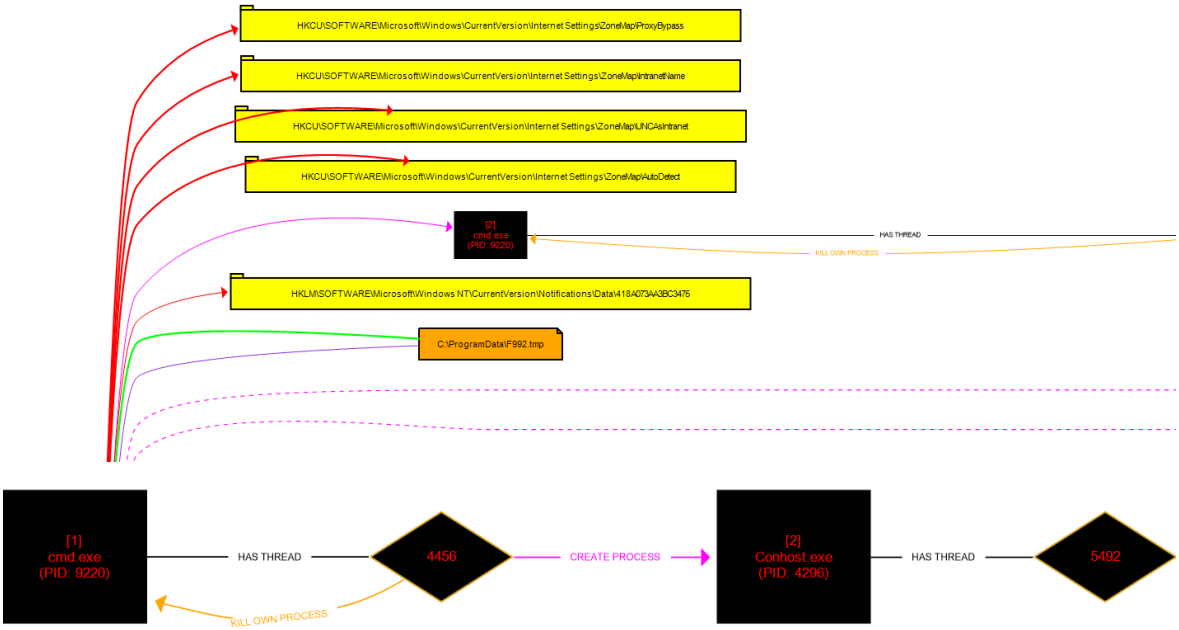
با بررسی دقیق‌تر فایل‌های هدف متوجه می‌شویم که باج‌افزار به فایل‌هایی با پسوندهایی مانند exe.، dll.، bat. ، cmd.، msi.، msc. کاری ندارد.



طبق نتایج بدست آمده، باج‌افزار فایل‌ها و پوشه‌های درون Recycle Bin را نیز حذف می‌کند.



باج‌افزار در انتهای اجرای خود در بخش دوم برروی تعدادی کلید رجیستری، تغییراتی را ایجاد می‌کند و همچنین cmd.exe را نیز فراخوانی می‌کند:



فایل پیغام باج‌خواهی این باج‌افزار با عنوان ddbPFTiN9.README.txt بر روی Desktop و همینطور در پوشه‌هایی که عملیات رمزگذاری انجام شده، قرار می‌گیرد. بخش اول نام این فایل متنی همان پسوند فایل‌های رمزشده می‌باشد.

درون این فایل، پیغام بسیار طولانی زیر وجود دارد:

~~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukkssplnidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukkssplnidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

Tor Browser Links for chat:
http://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion
http://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
http://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
http://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
http://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
http://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
http://lockbitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd.onion

>>>
>>>>> Your personal ID: 935BBFCDD2C9CF960F715F30C852CC0F <<<<<
>>>

>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.
They won't help and will only make things worse for you. In 3 years not a single member of our group has been caught by the police, we are top notch hackers and we never leave a trail of crime. The police will try to prohibit you from paying the ransom in any way. The first thing they will tell you is that there is no guarantee to decrypt your files and remove stolen files, this is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it is a matter of our reputation, we make hundreds of millions of dollars and are not going to lose our revenue because of your files. It is very beneficial for the police and FBI to let everyone on the planet know about your data leak because then your state will get the fines budgeted for you due to GDPR and other similar laws. The fines will be used to fund the police and the FBI, they will eat more sweet coffee donuts and get fatter and fatter. The police and the FBI don't care what losses you suffer as a result of our attack, and we will help you get rid of all your problems for a modest sum of money. Along with this you should know that it is not necessarily your company that has to pay the ransom and not necessarily from your bank account, it can be done by an unidentified person, such as any philanthropist who loves your company, for example, Elon Musk, so the police will not do anything to you if someone pays the ransom for you. If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom. The police and FBI will not be able to stop lawsuits from your customers for leaking personal and private information. The police and FBI will not protect you from repeated attacks. Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.

>>>>> What are the dangers of leaking your company's data.
First of all, you will receive fines from the government such as the GDRP and many others, you can be sued by customers of your firm for leaking information that was confidential. Your leaked data will be used by all the hackers on the planet for various unpleasant things. For example, social engineering, your employees' personal data can be used to re-infiltrate your company. Bank details and passports can be used to create bank accounts and online wallets through which criminal money will be laundered. On another vacation trip, you will have to explain to the FBI where you got millions of dollars worth of stolen cryptocurrency transferred through your accounts on cryptocurrency exchanges. Your personal information could be used to make loans or buy appliances. You would later have to prove in court that it wasn't you who took out the loan and pay off someone else's loan. Your competitors may use the stolen information to steal technology or to improve their processes, your working methods, suppliers, investors, sponsors, employees, it will all be in the public domain. You won't be happy if your competitors lure your employees to other firms offering better wages, will you? Your competitors will use your information against you. For example, look for tax violations in the financial documents or any other violations, so you have to close your firm. According to statistics, two thirds of small and medium-sized companies close within half a year after a data breach. You will have to find and fix the vulnerabilities in your network, work with the customers affected by data leaks. All of these are very costly procedures that can exceed the cost of a ransomware buyout by a factor of hundreds. It's much easier, cheaper and faster to pay us the ransom. Well and most importantly, you will suffer a reputational loss, you have been building your company for many years, and now your reputation will be destroyed.

Read more about the GDRP legislation::
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://gdpr.eu/what-is-gdpr/
https://gdpr-info.eu/

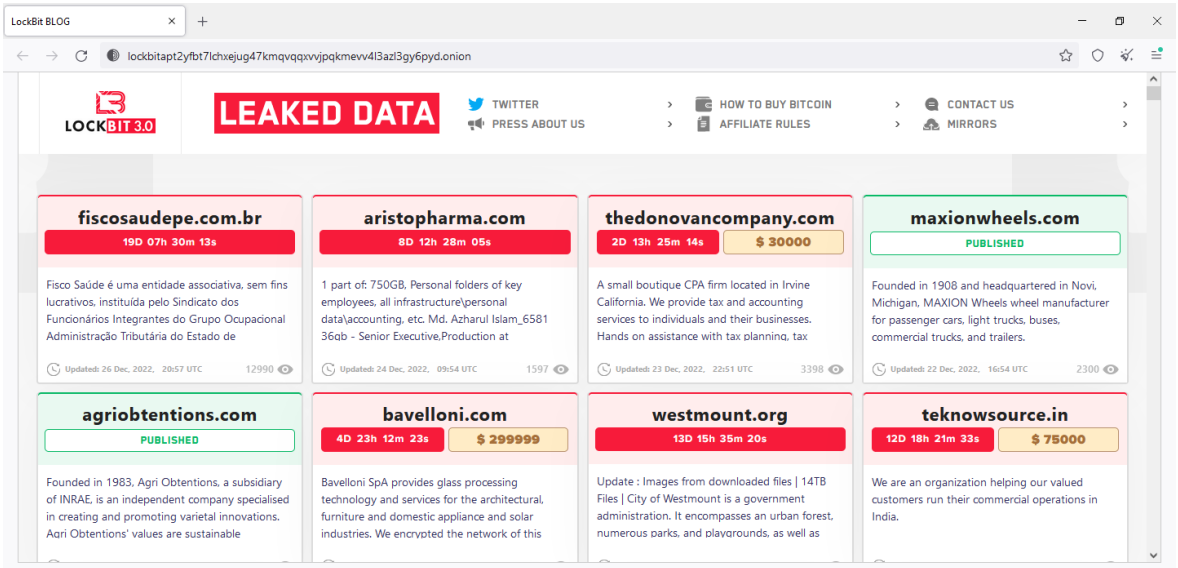
>>>>> Don't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you.
We are well aware of cases where recovery companies tell you that the ransom price is 5 million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you. If you approached us directly without intermediaries you would pay 5 times less, that is 1 million dollars.

>>>> Very important! For those who have cyber insurance against ransomware attacks.
Insurance companies require you to keep your insurance information secret, this is to never pay the maximum amount specified in the contract or to pay nothing at all, disrupting negotiations. The insurance company will try to derail negotiations in any way they can so that they can later argue that you will be denied coverage because your insurance does not cover the ransom amount. For example your company is insured for 10 million dollars, while negotiating with your insurance agent about the ransom he will offer us the lowest possible amount, for example 100 thousand dollars, we will refuse the paltry amount and ask for example the amount of 15 million dollars, the insurance agent will never offer us the top threshold of your insurance of 10 million dollars. He will do anything to derail negotiations and refuse to pay us out completely and leave you alone with your problem. If you told us anonymously that your company was insured for $10 million and other important details regarding insurance coverage, we would not demand more than $10 million in correspondence with the insurance agent. That way you would have avoided a leak and decrypted your information. But since the sneaky insurance agent purposely negotiates so as not to pay for the insurance claim, only the insurance company wins in this situation. To avoid all this and get the money on the insurance, be sure to inform us anonymously about the availability and terms of insurance coverage, it benefits both you and us, but it does not benefit the insurance company. Poor multimillionaire insurers will not starve and will not become poorer from the payment of the maximum amount specified in the contract, because everyone knows that the contract is more expensive than money, so let them fulfill the conditions prescribed in your insurance contract, thanks to our interaction.

>>>>> If you do not pay the ransom, we will attack your company again in the future.
~~~~

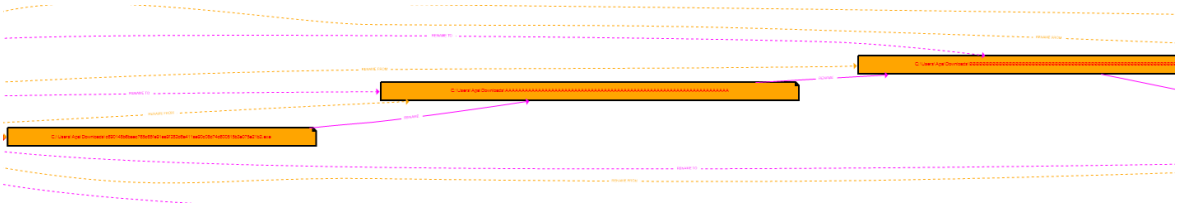
در ابتدای پیغام باج‌خواهی، اشاره به اسم این باج‌افزار شده است، در ادامه نیز گفته شده که دیتای شما دزدیده و رمزگذاری شده است و اگر باج را پرداخت نکنید برروی دارک‌وب ما قرار می‌گیرد و امکان به فروش رسیدن و سواستفاده از آن بیشتر خواهد شد. مهاجمین برای اثبات حرف خود چندین لینک درون پیغام باج قرار داده‌اند که به صفحه اصلی LockBit هدایت می‌شوند. سپس برای اطمینان دادن از بازیابی اطلاعات پس از پرداخت باج می‌گویند که آنها نمی‌خواهند اعتبار خود را در دنیای باج‌افزارها خدشه‌دار کنند و پیشنهاد بازیابی یک فایل با Personal ID موجود در فایل متنی را می‌دهند. برای انجام این فرآیند و شروع مذاکره خواسته می‌شود که Tor را نصب و از طریق Personal ID موجود با آن‌ها به صحبت پرداخته شود. در قسمت دوم (آخر) پیام نیز تهدید به افشای فایل‌ها در صورت درگیر کردن نیروهای امنیتی را می‌کند و همچنین مشاوره‌ای با این مضمون که با شرکت‌های بازیابی اطلاعات و همینطور بیمه همکاری نشود ارائه شده است. در این بین نیز از دست‌وپاگیری قوانین GDRP مثال زده و لینک‌هایی برای معرفی آن در فایل متنی قرار می‌دهند. در پیام خود به ما پیشنهاد داده می‌شود که درصورت پرداخت باج و همکاری دیگر به آن‌ها حمله نمی‌کنند و علاوه بر آن مشاوره‌هایی برای افزایش امنیت سازمان نیز آن‌ها نیز می‌دهند و تهدید نهایی نیز در انتها آمده است که اگر باج را پرداخت نکنید ما به سازمان شما درآینده نیز حمله می‌کنیم.

با مراجعه به لینک موجود در فایل به صفحه اصلی باج‌افزار منتقل می‌شویم:

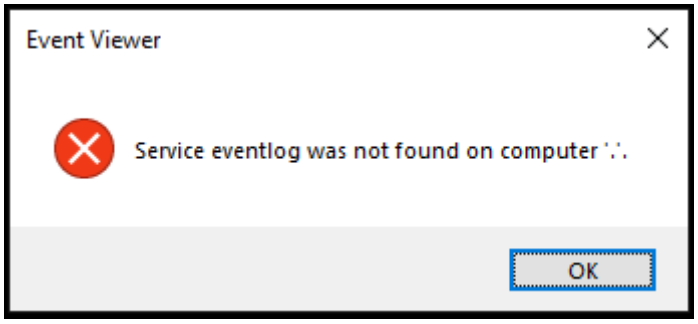


فرآیند مربوط به باج‌افزار LockBit 3.0 پس از انجام وظیفه اصلی خود وارد بخش دوم اجرای خود می‌شود.

باج‌افزار پس از دراپ کردن تمام فایل‌های موردنیاز برای ادامه اجرا در "C:\ProgramData" فایل اجرایی اصلی خود را برای جلوگیری از عدم شناسایی، بصورت زیر با تغییر نام تمام کاراکترها به حروف انگلیسی حذف می کند:



سپس سرویس‌های دیفندر ویندوز، فضای VSS و همینطور ابزار Event Viewer را از کار می‌اندازد.



درنهایت پس از اعمال تمام تغییرات گفته شده، برای جلوگیری از اقدامات فارنزیکی، فعالیت‌های خود در سیستم قربانی متوقف می‌کند و فایل اجرایی tmp. را نیز پاک می‌کند.

۵-۲ روش انتشار

هدف اصلی خانواده باج‌افزار LockBit شرکت‌ها و سازمان‌های خصوصی و دولتی می‌باشند و در خطمشی هایشان اشاره شده که به مراکز درمانی، مراکز آموزشی، خیریه‌ها و ارگان‌های خدمت‌رسانی به جامعه حمله نکنند. البته مواردی نیز از نقض این خطمشی وجود داشته است. این باج‌افزار معمولاً از طریق ایمیل‌های فیشینگ منتشر می‌شود و یا بصورت ماکرو در سندهای ورد قرار داده می‌شود. درصورت غیرفعال بودن آنتی ویروس و اجرای مستقیم یا فعال‌سازی ماکروها در اسناد اجرا می‌شود.

۵-۳ روش مقابله

باج‌افزار LockBit 3.0 در صورت فعال بودن لایه‌های محافظتی ویندوز توانایی اجرا شدن ندارد پس با آپدیت بودن بخش‌های امنیتی سیستم یا استفاده از برنامه‌های ضدبدافزار و نصب وصله‌های امنیتی، نگرانی بابت فعالیت و صدمه این باج‌افزار به سیستم بسیار پایین خواهد آمد.

۶ تحلیل ایستا

بررسی‌های اولیه بر روی نمونه فایل تست شده نشان می‌دهد که باج‌افزار LockBit 3.0 بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از XP به بعد، اجرا خواهد شد.

os-version	5.1	Windows XP

۶-۱ تحلیل کد

کد باج‌افزارهای خانواده LockBit 3.0 برای جلوگیری از تحلیل توسط متخصصین بدافزار، شدیداً Obfuscate شده است. در این بخش به چند مورد در رابطه با رفتار باج‌افزار اشاره می‌شود.

```
.idata:0041A04C ; Imports from gdi32.dll
.idata:0041A04C ;
.idata:0041A04C ; BOOL (__stdcall *TextOutW)(HDC hdc, int x, int y, LPCWSTR lpString, int c)
.idata:0041A04C                 extrn __imp_TextOutW:dword
.idata:0041A04C                                         ; DATA XREF: TextOutW↑r
.idata:0041A04C                                         ; .rdata:0041A240↓o
.idata:0041A050 ; COLORREF (__stdcall *SetTextColor)(HDC hdc, COLORREF color)
.idata:0041A050                 extrn __imp_SetTextColor:dword
.idata:0041A050                                         ; DATA XREF: SetTextColor↑r
.idata:0041A054 ; HGDIOBJ (__stdcall *SelectObject)(HDC hdc, HGDIOBJ h)
.idata:0041A054                 extrn __imp_SelectObject:dword
.idata:0041A054                                         ; DATA XREF: SelectObject↑r
.idata:0041A058 ; COLORREF (__stdcall *GetPixel)(HDC hdc, int x, int y)
.idata:0041A058                 extrn __imp_GetPixel:dword
.idata:0041A058                                         ; DATA XREF: GetPixel↑r
.idata:0041A05C ; int (__stdcall *GetDeviceCaps)(HDC hdc, int index)
.idata:0041A05C                 extrn __imp_GetDeviceCaps:dword
.idata:0041A05C                                         ; DATA XREF: GetDeviceCaps↑r
```

تصویر بالا مربوط به بخشی از کد باج‌افزار است که فرآیندهای مربوط به ساخت تصویری که بر روی دسکتاپ قرار می‌گیرد را نشان می‌دهد. با استفاده از gdi32.dll مشخصات صفحه نمایش سیستم قربانی گرفته می‌شود و نسبت به آن، متن با سایز و مکان درست برروی بک‌گراند مشکی جای می‌گیرد.

```
OSMajorVersion = v0->OSMajorVersion;
OSMinorVersion = v0->OSMinorVersion;
if ( OSMajorVersion == 5 && !OSMinorVersion || OSMajorVersion < 5 )
  return 0;
if ( OSMajorVersion == 5 && OSMinorVersion == 1 )
  return 51;
if ( OSMajorVersion == 5 && OSMinorVersion == 2 )
  return 52;
if ( OSMajorVersion == 6 && !OSMinorVersion )
  return 60;
if ( OSMajorVersion == 6 && OSMinorVersion == 1 )
  return 61;
if ( OSMajorVersion == 6 && OSMinorVersion == 2 )
  return 62;
if ( OSMajorVersion == 6 && OSMinorVersion == 3 )
  return 63;
if ( OSMajorVersion == 10 && !OSMinorVersion )
  return 100;
if ( OSMajorVersion == 10 && OSMinorVersion || OSMajorVersion > 0xA )
  return 0x7FFFFFFF;
return -1;
```

در بخش بالا نیز سیستم‌عامل سیستم هدف را برای اجرای برنامه بررسی می‌کند.

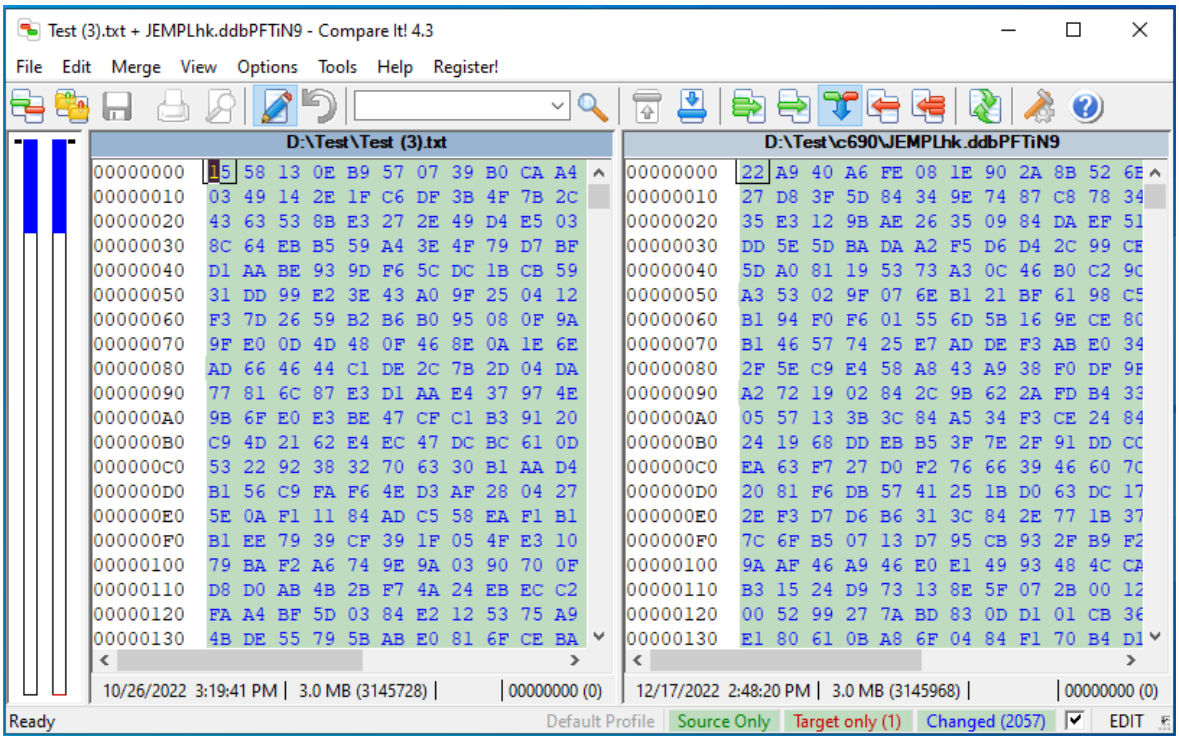
```
v2 = dword_4251F0;
v12 = dword_4251F0[0] ^ _byteswap_ulong(*a1);
v11 = dword_4251F0[1] ^ _byteswap_ulong(a1[1]);
v10 = dword_4251F0[2] ^ _byteswap_ulong(a1[2]);
v9 = dword_4251F0[3] ^ _byteswap_ulong(a1[3]);
v3 = (unsigned int)dword_4253F0 >> 1;
while ( 1 )
{
  v8 = v2[4] ^ dword_403110[(unsigned __int8)v9] ^ dword_402D10[BYTE1(v10)] ^ dword_402910[BYTE2(v11)] ^ dword_402510[HIBYTE(v12)];
  v7 = v2[5] ^ dword_403110[(unsigned __int8)v12] ^ dword_402D10[BYTE1(v9)] ^ dword_402910[BYTE2(v10)] ^ dword_402510[HIBYTE(v11)];
  v6 = v2[6] ^ dword_403110[(unsigned __int8)v11] ^ dword_402D10[BYTE1(v12)] ^ dword_402910[BYTE2(v9)] ^ dword_402510[HIBYTE(v10)];
  v5 = v2[7] ^ dword_403110[(unsigned __int8)v10] ^ dword_402D10[BYTE1(v11)] ^ dword_402910[BYTE2(v12)] ^ dword_402510[HIBYTE(v9)];
  v2 += 8;
  if ( !--v3 )
    break;
  v12 = *v2 ^ dword_403110[(unsigned __int8)v5] ^ dword_402D10[BYTE1(v6)] ^ dword_402910[BYTE2(v7)] ^ dword_402510[HIBYTE(v8)];
  v11 = v2[1] ^ dword_403110[(unsigned __int8)v8] ^ dword_402D10[BYTE1(v5)] ^ dword_402910[BYTE2(v6)] ^ dword_402510[HIBYTE(v7)];
  v10 = v2[2] ^ dword_403110[(unsigned __int8)v7] ^ dword_402D10[BYTE1(v8)] ^ dword_402910[BYTE2(v5)] ^ dword_402510[HIBYTE(v6)];
  v9 = v2[3] ^ dword_403110[(unsigned __int8)v6] ^ dword_402D10[BYTE1(v7)] ^ dword_402910[BYTE2(v8)] ^ dword_402510[HIBYTE(v5)];
}
*a2 = _byteswap_ulong(*v2 ^ (unsigned __int8)dword_403510[(unsigned __int8)v5] ^ dword_403510[BYTE1(v6)] & 0xFF00 ^ dword_403510[BYTE2(v7)] & 0xFF0000 ^
a2[1] = _byteswap_ulong(v2[1] ^ (unsigned __int8)dword_403510[(unsigned __int8)v8] ^ dword_403510[BYTE1(v5)] & 0xFF00 ^ dword_403510[BYTE2(v6)] & 0xFF000
a2[2] = _byteswap_ulong(v2[2] ^ (unsigned __int8)dword_403510[(unsigned __int8)v7] ^ dword_403510[BYTE1(v8)] & 0xFF00 ^ dword_403510[BYTE2(v5)] & 0xFF000
result = _byteswap_ulong(v2[3] ^ (unsigned __int8)dword_403510[(unsigned __int8)v6] ^ dword_403510[BYTE1(v7)] & 0xFF00 ^ dword_403510[BYTE2(v8)] & 0xFF00

000046D8 sub_405248:21 (4052D8)
```

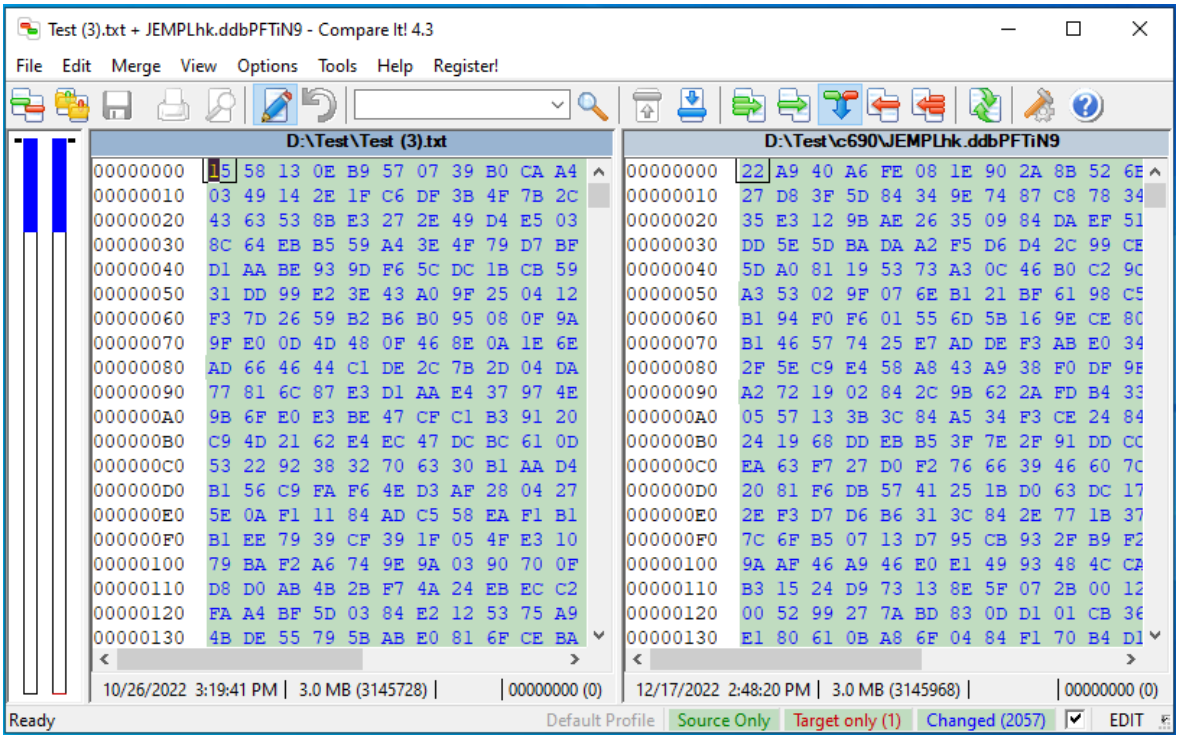
در این بخش نیز به نظر می‌رسد که عملیاتی مربوط به کلید Salsa20 که در آن ماتریسی ساخته می‌شود و باج‌افزار با آن کار می‌کند، در حال انجام است.

```
00000000 ; Ins/Del : create/delete structure
00000000 ; D/A/*   : create structure member (data/ascii/array)
00000000 ; N       : rename structure or structure member
00000000 ; U       : delete structure member
00000000 ; -------------------------------------------------------------------
00000000
00000000 _PEB            struc ; (sizeof=0x248, align=0x8, copyof_1)
00000000 InheritedAddressSpace db ?
00000001 ReadImageFileExecOptions db ?
00000002 BeingDebugged   db ?
00000003 anonymous_0     _PEB::$D57935FE5756AF9F9B84A66E67E8019A ?
00000004 Mutant          dd ?                    ; offset
00000008 ImageBaseAddress dd ?                   ; offset
0000000C Ldr             dd ?                    ; offset
00000010 ProcessParameters dd ?                  ; offset
00000014 SubSystemData   dd ?                    ; offset
00000018 ProcessHeap     dd ?                    ; offset
0000001C FastPebLock     dd ?                    ; offset
00000020 AtlThunkSListPtr dd ?                   ; offset
00000024 IFEOKey         dd ?                    ; offset
00000028 anonymous_1     _PEB::$9091FB23ACFC48B9D2023E9670FB1584 ?
0000002C anonymous_2     _PEB::$6F1CA9A36B21C857AE5467E073440320 ?
00000030 SystemReserved  dd ?
00000034 AtlThunkSListPtr32 dd ?
00000038 ApiSetMap       dd ?                    ; offset
```

در تصویر بالا مشاهده می‌شود که باج‌افزار با تعدادی کلید مربوط به PEB و همینطور FastPebLock از پروسس خود محافظت می‌کند تا روند اجرای صحیح باج‌افزار، بدون اختلال توسط پروسس‌های دیگر صورت پذیرد.

پس از بررسی چند نمونه فایل سالم با نمونه رمزشده مشخص گردید که تنها ۵۱۲ کیلوبایت از ابتدای هرفایل رمزگذاری می‌شود و مابقی فایل دست نخورده باقی می‌ماند. همچنین برای فایل‌های کوچکتر از ۵۱۲ کیلوبایت نیز تمام فایل رمز می‌شود؛ و در انتهای هر فایل با هر حجمی نیز ۲۴۳بایت اضافه می‌نماید که در تصویر زیر مشخص شده است.





طبقه‌بندی: عادی

۶-۲ تحلیل ترافیک شبکه

پس از بررسی ترافیک شبکه ضبط شده حین اجرای باج‌افزار و همچنین بررسی نتایج سندباکس‌های آنلاین، موردی در ارتباط با باج‌افزار مشاهده نشد و به نظر می‌رسد این سمپل کاملاً آفلاین فعالیت می‌کند.

۶-۳ رمزنگاری و رمزگشایی

خانواده باج‌افزار LockBit 3.0 با الگوریتم Salsa20 فایل‌ها را با سرعتی بسیار بالا رمزگذاری کرده و کلیدی را در انتهای فایل ذخیره می‌کند.

در نهایت باتوجه به رمزگذاری صورت گرفته توسط الگوریتم Salsa20 در حال حاضر هیچ‌گونه ابزار رایگانی جهت رمزگشایی فایل‌های رمزشده توسط این باج‌افزار، ارائه نشده است.

۷ شناسه‌های تهدید (IOCs)

نمونه فایل‌های اجرایی:

80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce
a56b41a6023f828cccaaef470874571d169fdb8f683a75edd430fbd31a2c3f6e
d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee
5063b12853375a1fbbf85c82ddf13341cf941c5acd4a39a51d6addf145a7a51
c597c75c6b6b283e3b5c8caeee095d60902e7396536444b59513677a94667ff8
917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2

فایل‌های دراپ شده:

BC21.tmp
917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
ddbPFTiN9.bmp
f778ddee4515e5ab34972951a7d6a27cfa129a85b29d36df527c0f1e9bc5cafe
ddbPFTiN9.ico
95e059ef72686460884b9aea5c292c22917f75d56fe737d43be440f82034f438

۸ شناسایی (Detection)

با توجه به اینکه باج‌افزار LockBit 3.0 بلافاصله پس از اجرا، فضای VSS را حذف می‌کند، با استفاده از رول زیر در اسپلانک می‌توان انتشار باج‌افزار در شبکه را شناسایی کرد:

```
((EventCode="4688" OR EventCode="1") (CommandLine="*vssadmin* *delete* *shadows*" OR CommandLine="*wmic* *shadowcopy* *delete*" OR CommandLine="*vssadmin* *resize* *shadowstorage*")) OR (EventCode="5857" ProviderName="MSVSS__PROVIDER") OR (EventCode="5858" Operation="*Win32_ShadowCopy*")
```