An Analysis of the BabLock Ransomware

trendmicro.com/en_us/research/23/d/an-analysis-of-the-bablock-ransomware.html

April 18, 2023

Content added to Folio

Ransomware

An Analysis of the BabLock (aka Rorschach) Ransomware

This blog post analyzes a stealthy and expeditious ransomware called BabLock (aka Rorschach), which shares many characteristics with LockBit.

By: Don Ovid Ladores, Byron Gelera April 18, 2023 Read time: (words)

A ransomware called BabLock (aka Rorschach) has recently been making waves due to its sophisticated and fast-moving attack chain that uses subtle yet effective techniques. Although primarily based on LockBit, the ransomware is a hodgepodge of other different ransomware parts pieced together into what we now call BabLock (detected as Ransom.Win64.LOCKBIT.THGOGBB.enc). Note, however, that we do not believe that this ransomware originates from the threat actors behind LockBit, which is now in its third iteration.

In this blog entry, we look at its attack chain in detail and examine its likely origins.

Discovery

In June 2022, we discovered a ransomware (which turned out to be BabLock) using what appeared to be a unique style of appending extensions, where instead of the normal “one sample, one extension” method commonly used in ransomware attacks, we discovered that the attackers were appending numerical increments from 00-99 on top of the fixed ransomware extension for this specific infection. As a result, even on a single infected machine, there could be multiple extension variations from a single execution.

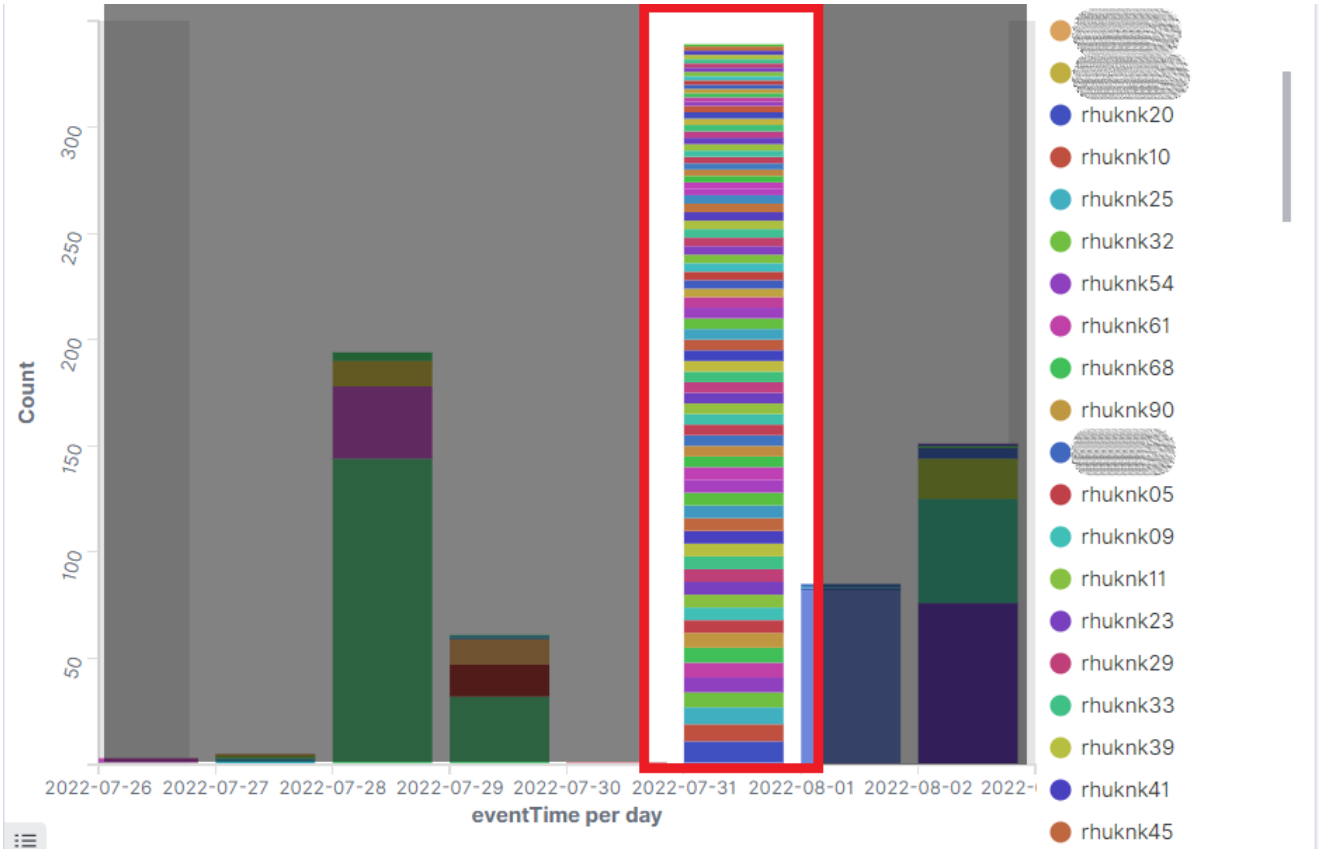

Figure 1. The ransomware's unique trait showing numerical increments for the extension

Our investigation found that the ransomware was always deployed as a multi-component package consisting mostly of the following files:

- The encrypted ransomware file, *config.ini*
- A malicious sideloaded DLL (DarkLoader, a *config.ini* decryptor and ransomware injector)
- A non-malicious executable used to load the malicious DLL
- A CMD file to execute the non-malicious binary using the correct password

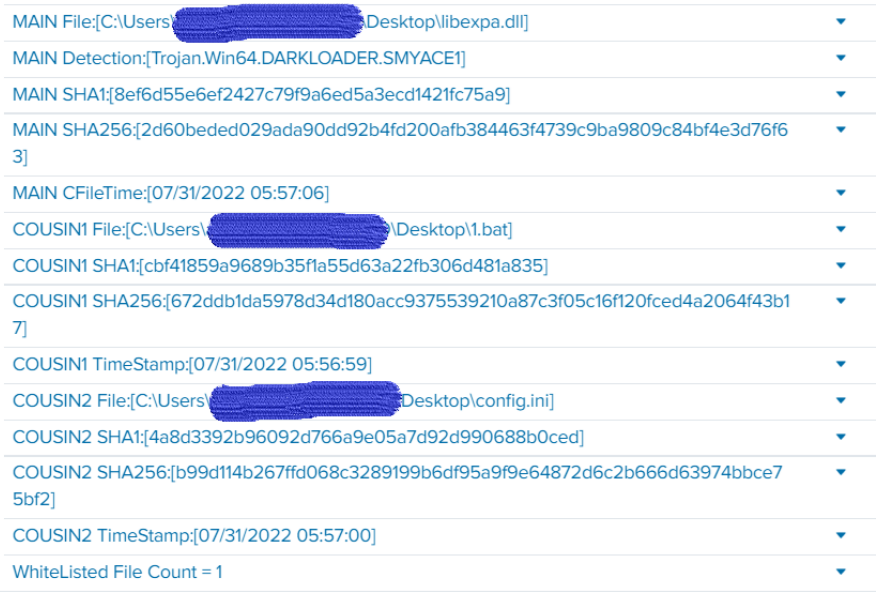

Figure 2. The main ransomware package found during one instance of infection

The DarkLoader DLL will check for specific commands, particularly ***--run***, which checks for the correct 4-digit password needed to start the encryption process. Although it bears little significance to the unpacking of the contents of *config.ini* itself, the DLL will execute the fundamental ransomware routine if supplied correctly.

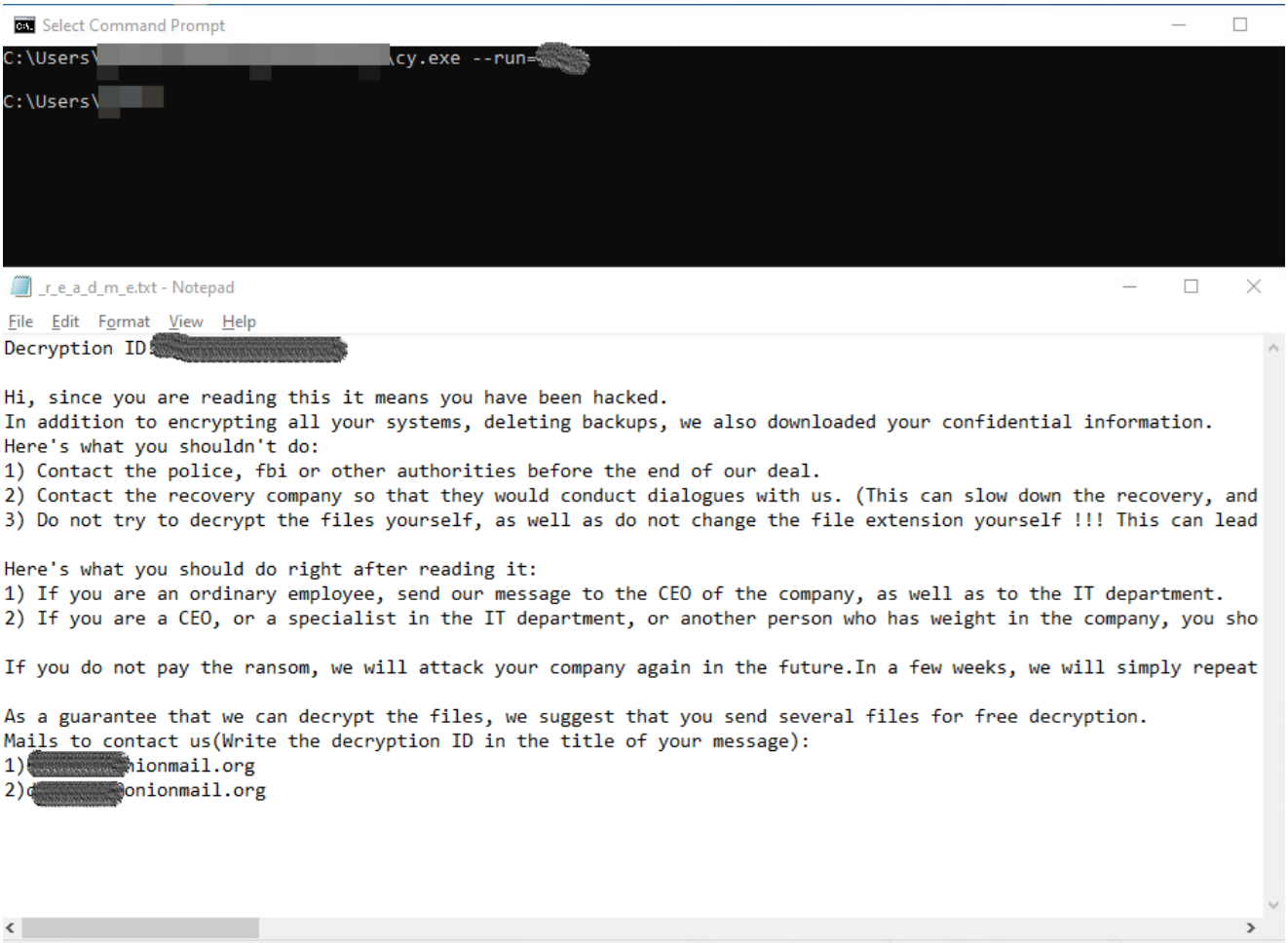

Figure 3. If the correct passcode is added to the command line, the ransomware will proceed

with the whole encryption process

Once the DLL component is loaded by the non-malicious executable, it will immediately look for the *config.ini* file in the current executable's path. Once this is found, the DLL decrypts *config.ini* and then executes *notepad.exe* with a certain set of command lines.

- For this particular campaign, we found a few notable and consistent patterns:
- The main ransomware binary is usually delivered as an encrypted *config.ini* file.
- DarkLoader is executed via DLL sideloadingusing legitimate executables.
- The *config.ini* file is decrypted by a specially crafted loader designed specifically for these campaigns (detected as Trojan.Win64.DarkLoader)
- BabLock appends a random number from 00 to 99 to the extension string per file within the same infected machine (for example, extn00-extn99 as extensions in the same infection).
- Any DarkLoader DLL can be used to decrypt any encrypted ransomware *config.ini*, with no specific binary pairing needed.
- The DarkLoader DLL uses Direct SysCall APIs to a select few, but important, calls to avoid API reading analysis.
- The decrypted BabLock ransomware is always packed with VMProtect for anti-virtualization.
- BabLock is loaded via the threat injection of a hooked API *Ntdll.RtlTestBit* to jump to memory containing the ransomware code.
- There have been a few variations of the passcode for *--run* across different attacks, but all of them are still within a certain range of each other.

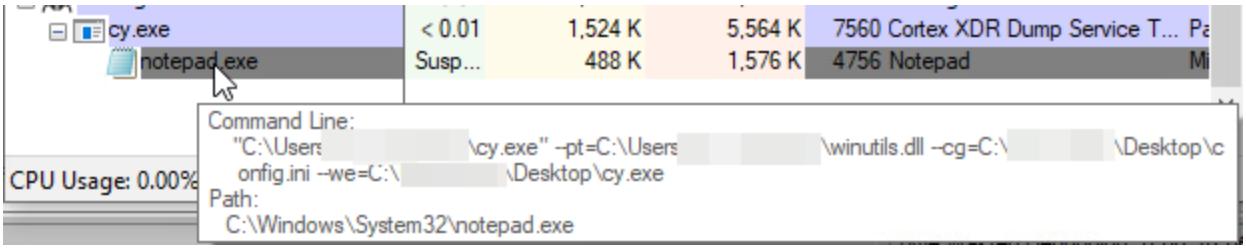

Figure 4. The command line argument supplied to notepad.exe to load and execute the ransomware on recent attacks.

Figure 5. DLL using several direct SysCall instructions to avoid API reading techniques

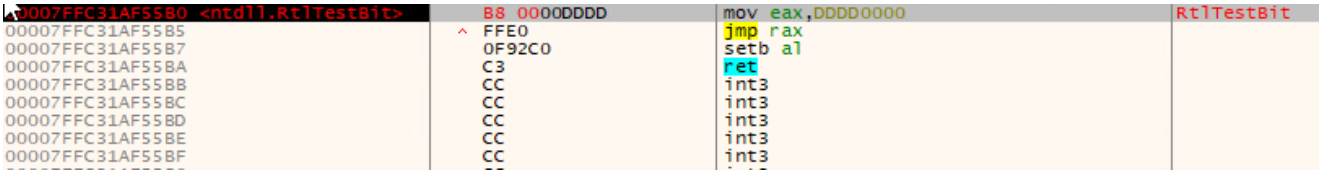

Figure 6. The notepad.exe file is injected with an API call thread to RtlTestBit, which has been patched/hooked to jump to the malicious routine

Subtle but sophisticated

Throughout our initial encounter with BabLock in June 2022, we searched for similar files and found that the earliest record of these files dated back to March 2022. After discovering this, we wanted to find out how it managed to stay under the radar for so long.

Since June 2022, there have only been a handful of recorded incidents involving the ransomware, including the most recent one. Due to a low number count, no notable statistics involving region, industry, or victim profile have stood out as of the time of writing.

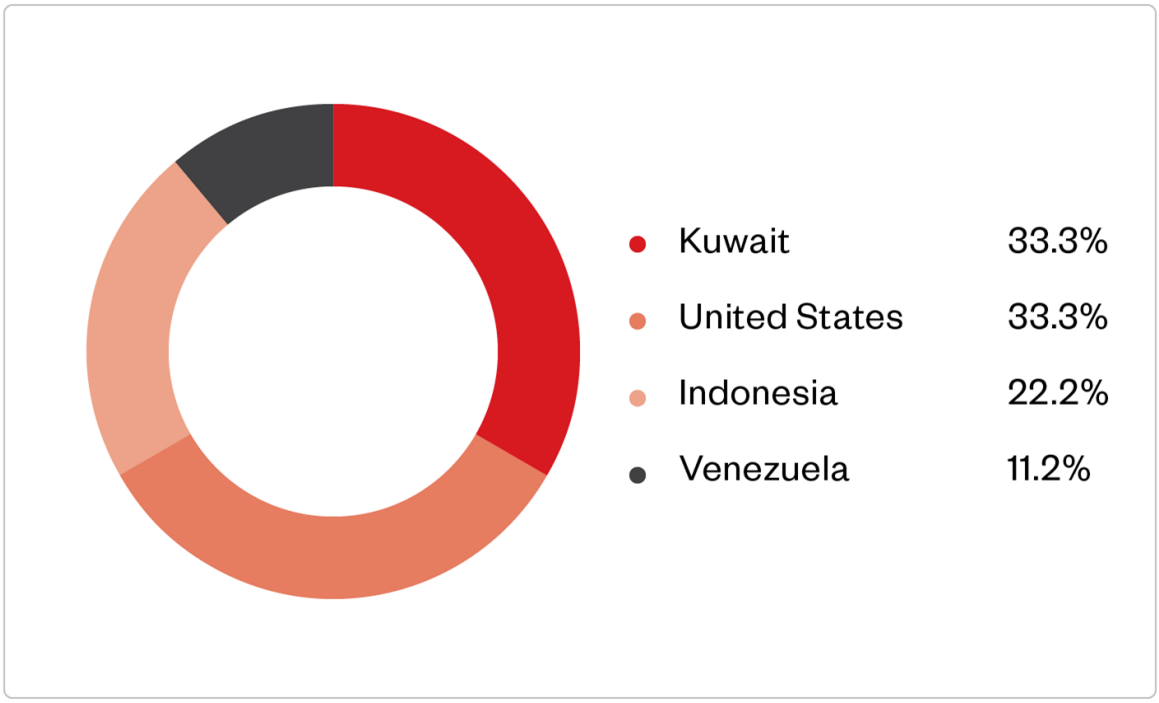

Figure 7. Distribution of incidents involving the BabLock ransomware

However, due to its notable features and characteristics, attacks related to BabLock can be easily identified. As we've already mentioned, after every file encryption, the ransomware appends a random number string between 00-99 to its hardcoded extension. This results in up to 100 different variations of the same ransomware extension.

```
sub_7FEEF395420(v45, 20i64, L"%02d", (rand_val % 99));
v34 = _mm_load_si128(&xmmword_7FEEF3C9D40);
for ( j = 0i64; j < 0xE; ++j )    // .rhuknk
```

Figure 8. Code snippet showing a random number string between 00-99 being appended to encrypted files

It also has a fairly sophisticated execution routine:

- It uses a specific number code to execute properly.
- It splits the package into multiple components.
- It separates and hides the actual payload into an encrypted file.
- It uses normal applications as loaders

Finally, BabLock employs publicly available tools as part of its infection chain. We found that the most used tools were the following:

- Chisel - A transmission control protocol (TCP) and user datagram protocol (UDP) tunnel
- Fscan - A scanning tool

By using these two tools — combined with BabLock/LockBit possessing the capability to set active directory (AD) Group Policies for easier propagation — it's possible for a malicious actor to navigate around a network without much effor

Comparing and contrasting BabLock to LockBit and other ransomware

From our investigation, most of the routines used by BabLock are more closely related to Lockbit (2.0) than any other ransomware. Other researchers also mention similarities to ransomware such as Babuk, Yanluowang and others.

Initially, we suspected it to be related to the DarkSide ransomware due to ransom note similarities. However, unlike the DarkSide ransomware, BabLock removes shadow copies by executing the following command lines:

> *vssadmin.exe delete shadows /All /Quiet*

Therefore, we immediately ruled this relationship out since it's different to the way DarkSide does things, which is deleting shadow copies through Windows Management Instrumentation (WMI) and PowerShell (which is technically more sophisticated and difficult to detect through standard monitoring tools).

```
do
{
  *((_BYTE *)&v771 + v3 + 1313) ^= v1447;
  *((_BYTE *)&v771 + v3 + 1314) ^= v1447;     // Delete Shadows /All /Quiet
  v3 += 2i64;
}
while ( v3 < 0x34 );
v1452 = 0;
LODWORD(v4) = sub_7FEED93FFD0(&v1526, &v1447 + 1);
v5 = v4;
_mm_storeu_si128((__m128i *)&v1375, _mm_load_si128((const __m128i *)&xmmword_7FEED96BFB0));
v1376 = 0x187D537D;
v1377 = 0x187D057D;
v1378 = 0x7D;
v1379 = 0;
v6 = 0i64;
do
  *((_BYTE *)&v771 + v6++ + 801) ^= v1375;    // vssadmin.exe
while ( v6 < 0x18 );
```

Figure 9. The ransomware binary decrypts and executes the command line to delete shadow copies.

One of its common characteristics to Lockbit (2.0) would be the use of the same group policy to generate a desktop drop path. Similarly, the use of vssadmin for deleting shadow copies is also a routine heavily used in LockBit attacks (albeit also a common routine for many modern ransomware). Still, the resemblance is uncanny. Furthermore, it is running the same commands to execute GPUpdate for the AD. Due to this, our detection for this ransomware is still under the LockBit family.

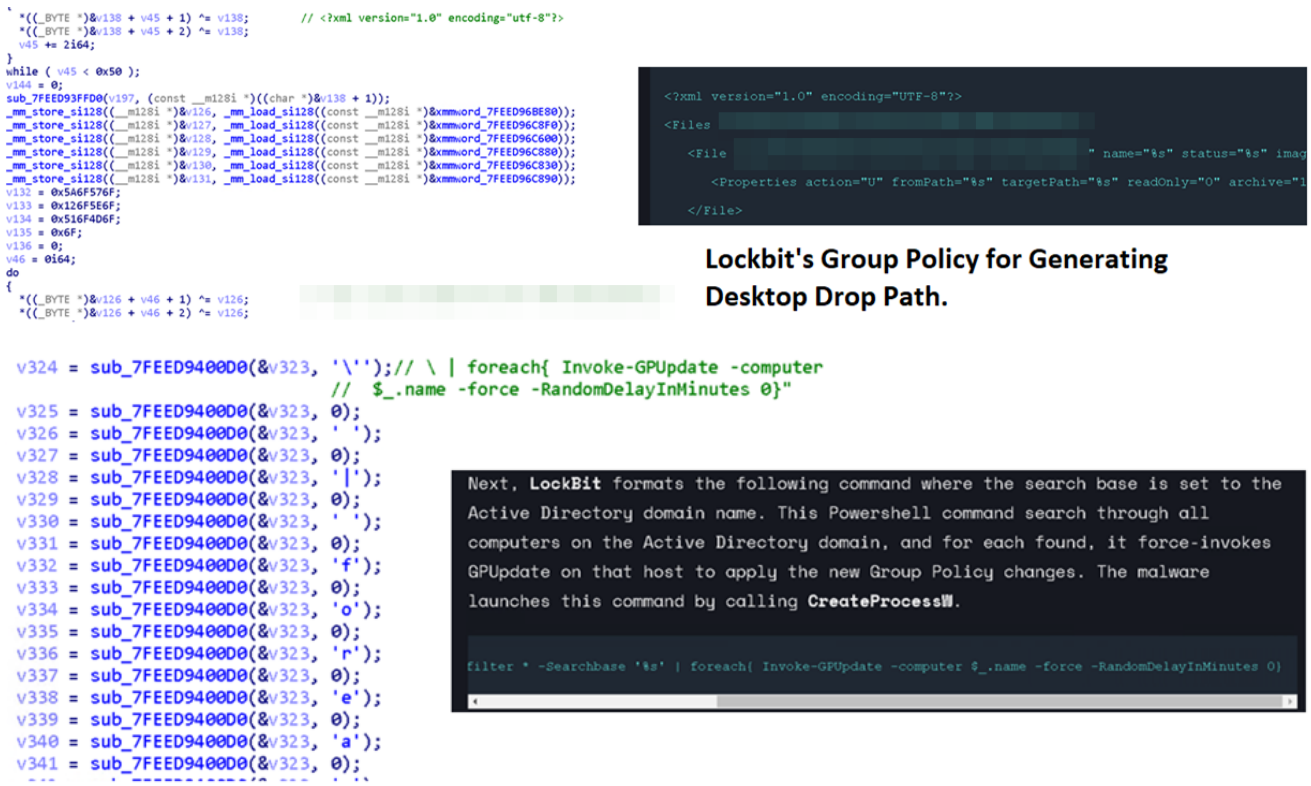

Figure 10. Comparing BabLock's group policy for generating the desktop drop path (left) with that of LockBit (right)

From what we can tell, BabLock looks like a Frankenstein-like creation that is stitched together from different known ransomware families.

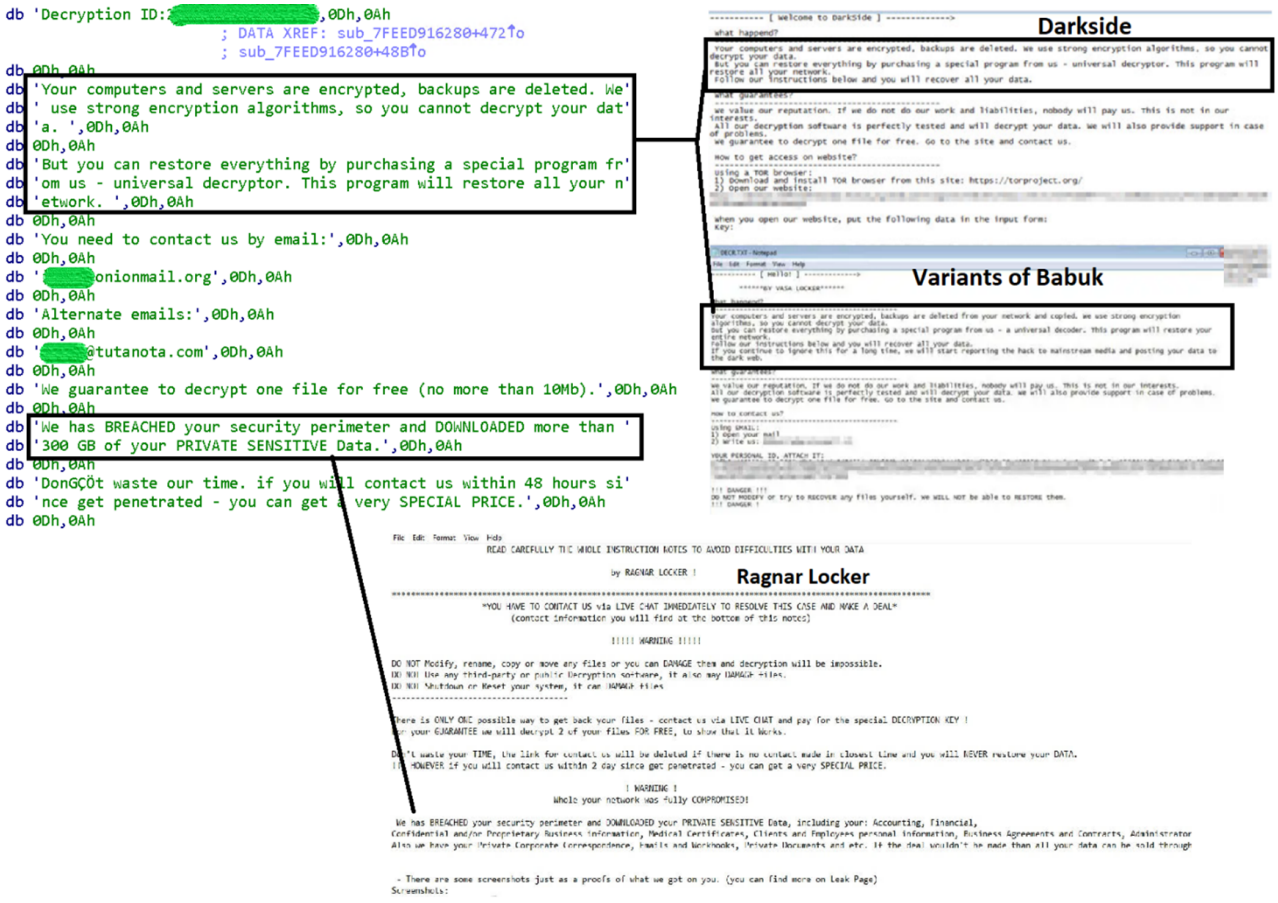

Figure 11. Similarities between BabLock and other ransomware families

Insights and conclusion

Our first encounter with BabLock almost coincided with the release of Lockbit v3.0. However, since most of its structure still resembles Lockbit v2.0, we surmise that this may be from another affiliate or group. With nearly a year since the release of LockBit v3.0, we have found no changes to the payload of the BabLock even with recent attacks, further solidifying our stance that they are neither connected nor closely affiliated with the actual LockBit group. What we do know is that the threat actor behind BabLock managed to take many of the base capabilities of LockBit v2.0 and added bits and pieces of different ransomware families to create their own unique variant, which could possibly be enhanced further in the future.

Recommendations

Organizations can implement security frameworks to safeguard their systems from similar attacks, which systematically allocate resources to establish a robust defense strategy against ransomware. Below are some recommended guidelines that organizations may want to consider:

- Taking an inventory of assets and data

- Identifying authorized and unauthorized devices and software
- Auditing event and incident logs
- Managing hardware and software configurations
- Granting admin privileges and access only when necessary to an employee's role
- Monitoring network ports, protocols, and services
- Establishing a software allowlist that only executes legitimate applications
- Implementing data protection, backup, and recovery measures
- Enabling multifactor authentication (MFA)
- Deploying the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Watching out for early signs of an attack such as the presence of suspicious tools in the system

Implementing a multi-faceted approach can aid organizations in securing potential entry points into their systems such as endpoint, email, web, and network. With the help of security solutions that can identify malevolent elements and questionable activities, enterprises can be safeguarded from ransomware attacks.

Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.

Trend Micro Cloud One™ – Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.

Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.

Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found here.

sXpIBdPeKzI9PC2p0SWMpUSM2NSxWzPyXTMLIbXmYa0R20xk