DarkAngels Ransomware: Targeted Attack by Rebranded Babuk

By cybleinc

Published: 2022-05-06 · Archived: 2026-04-05 23:42:23 UTC

Rebranded Babuk Ransomware in Action: DarkAngels Ransomware Performs Targeted Attack

This deep-dive analysis of one of the DarkAngels ransomware samples presents recommendations on how to protect yourself/your organization from the malware.

Cyble Research Labs has identified a new ransomware malware known as DarkAngels. Analysis of the DarkAngels malware uncovered similarities between it and the Babuk Ransomware.

While executing the sample, we observed that the ransom note, and the TAs website, contain a specific organization’s name indicating that the malware sample may have been developed as part of a highly targeted attack.

This blog showcases the deep-dive analysis of one of the DarkAngels ransomware samples to identify their capabilities and the way to protect yourself/your organization from them.

Technical Analysis

Based on static analysis, we found that the malicious file is a 32-bit Graphical User Interface (GUI) based binary, as shown in Figure 1.

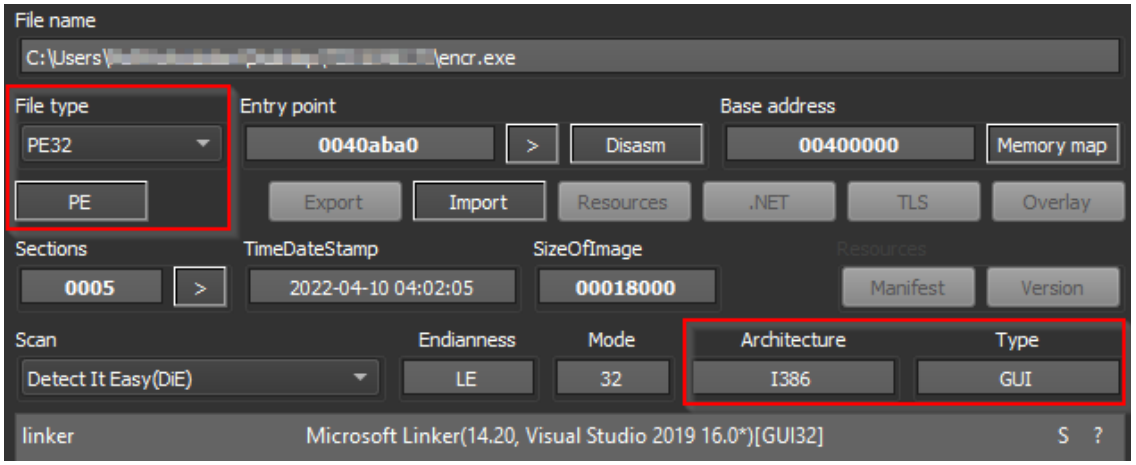

Figure 1 – Static File Information of DarkAngels Sample

Upon execution, the malware first changes the priority of the process i.e to zero by calling the *SetProcessShutdownParameters() API* so that the malware's activities can be terminated only before the system shutdown. This is a way to increase the amount of time the malware gets to execute in the compromised machine.

```
pNumArgs = 0;
CommandLineW = GetCommandLineW();
v20 = CommandLineToArgvW(CommandLineW, &pNumArgs);
SetProcessShutdownParameters(0, 0);
```

Figure 2 – Malware Changes the Priority of the Process

The malware tries to terminate the services before encrypting the system to ensure no interruption during its encryption process. To identify the services in the victim's machine, it calls the *OpenSCManagerA()* API, which establishes a connection to the service control manager and gives the malware access to the service control manager database, as shown in Figure 3.

```
result = OpenSCManagerA(0, 0, 0xF003Fu);
hSCManager = result;
if ( result )
{
  for ( i = 0; i < 0x2C; ++i )
  {
    hService = OpenServiceA(hSCManager, (&::lpServiceName)[i], 0x2Cu);
    if ( hService )
    {
      if ( QueryServiceStatusEx(hService, SC_STATUS_PROCESS_INFO, (LPBYTE)&Buffer,
        && Buffer.dwCurrentState != 1
        && Buffer.dwCurrentState != 3 )
      {
        if ( !EnumDependentServicesA(hService, 1u, lpServices, 0, &pcbBytesNeeded,
          && GetLastError() == 234 )
        {
          lpServices = (LPENUM_SERVICE_STATUSA)sub_412DE0(pcbBytesNeeded);
          if ( lpServices )
          {
            if ( EnumDependentServicesA(hService, 1u, lpServices, pcbBytesNeeded,
            {
              qmemcpy(lpServiceName, &lpServices[i], sizeof(lpServiceName));
              hSCObject = OpenServiceA(hSCManager, lpServiceName[0], 0x24u);
              if ( hSCObject )
              {
                if ( ControlService(hSCObject, 1u, &ServiceStatus) )
```

Figure 3 – Enumerates Services

After gaining access, the malware enumerates the services and fetches the service names in the victim's machines. The ransomware then checks the presence of the services such as VSS, SQL, Memtas, etc., and terminates them if the services are actively running on the victim's machine.

The ransomware also enumerates the running processes using *CreateToolhelp32Snapshot(), Process32FirstW(), and Process32NextW()* APIs, checks the process names such as sql.exe,oracle.exe, powerpnt.exe, etc., and terminates them if they are actively running.

```
    if ( !lstrcmpW((&lpString1)[j], pe.szExeFile) )
    {
      hProcess = OpenProcess(1u, 0, pe.th32ProcessID)
      if ( hProcess )
      {
        TerminateProcess(hProcess, 9u);
        CloseHandle(hProcess);
      }
      break;
    }
  }
}
return CloseHandle(hSnapshot);
```

Figure 4 – Terminates Active Processes

Furthermore, we noticed that the binary launches the vssadmin.exe process to delete all Shadow Copy, as shown in figure 5. The malware deletes shadow copies to avoid recovery of the system after encrypting the files.

```
ShellExecuteW(0, L"open", L"cmd.exe", L"/c vssadmin.exe delete shadows /all /quiet"
result = (FARPROC)sub_404AB0();
```

Figure 5 – Deletes All Shadow Copies

The malware deletes all items from the Recycle Bin by calling the "*SHEmptyRecycleBinA()* API to ensure no deleted files are restored after encryption.

```
.text:0040AC43                  push    7               ; dwFlags
.text:0040AC45                  push    0               ; pszRootPath
.text:0040AC47                  push    0               ; hwnd
.text:0040AC49                  call    ds:SHEmptyRecycleBinA
```

Figure 6 – Deletes Items from Recycle Bin

After execution, DarkAngels Ransomware tries to get system information using *GetSystemInfo() API*, which extracts information such as NumberOfProcessors.

```
.text:0040AC4F                  lea     ecx, [ebp+SystemInfo]
.text:0040AC55                  push    ecx             ; lpSystemInfo
.text:0040AC56                  call    ds:GetSystemInfo
.text:0040AC5C                  mov     edx, [ebp+SystemInfo.dwNumberOfProcessors]
.text:0040AC5F                  mov     [ebp+var_5C], edx
```

Figure 7 – DarkAngels Ransomware Collect System Info

The malware then creates a thread for all CPUs that it encounters, creates ransom notes named *How_To_Restore_Your_Files.txt*, and encrypts the files present in the victim's machine.

The malware enumerates the system and excludes the folders such as AppData, Boot, Windows, Windows.old, etc., from the encryption process.

The ransomware specifically excludes files such as autorun.inf, boot.ini,bootfont.bin, etc., from encryption.

The ransomware also excludes file extensions such as .exe, .dll, and .babyk. The .babyk is a well-known extension for Babuk ransomware which indicates the DarkAngels is linked to Babuk ransomware.

Like Babuk ransomware, the DarkAngels appends a signature "choung dong looks like hot dog" at the end of the encrypted file, indicating the ransomware is linked to Babuk.

```
v51 = 0;
v63 = 1;
qmemcpy(v36, "choung dong looks like hot dog!!", sizeof(v36));
```

Figure 8 – Appends Signature at the end of an encrypted file

The below figure demonstrates the ransom note dropped by the malware with the name "*How_To_Restore_Your_Files.txt*" to instruct the victims to pay the ransom money for the decryption tool.

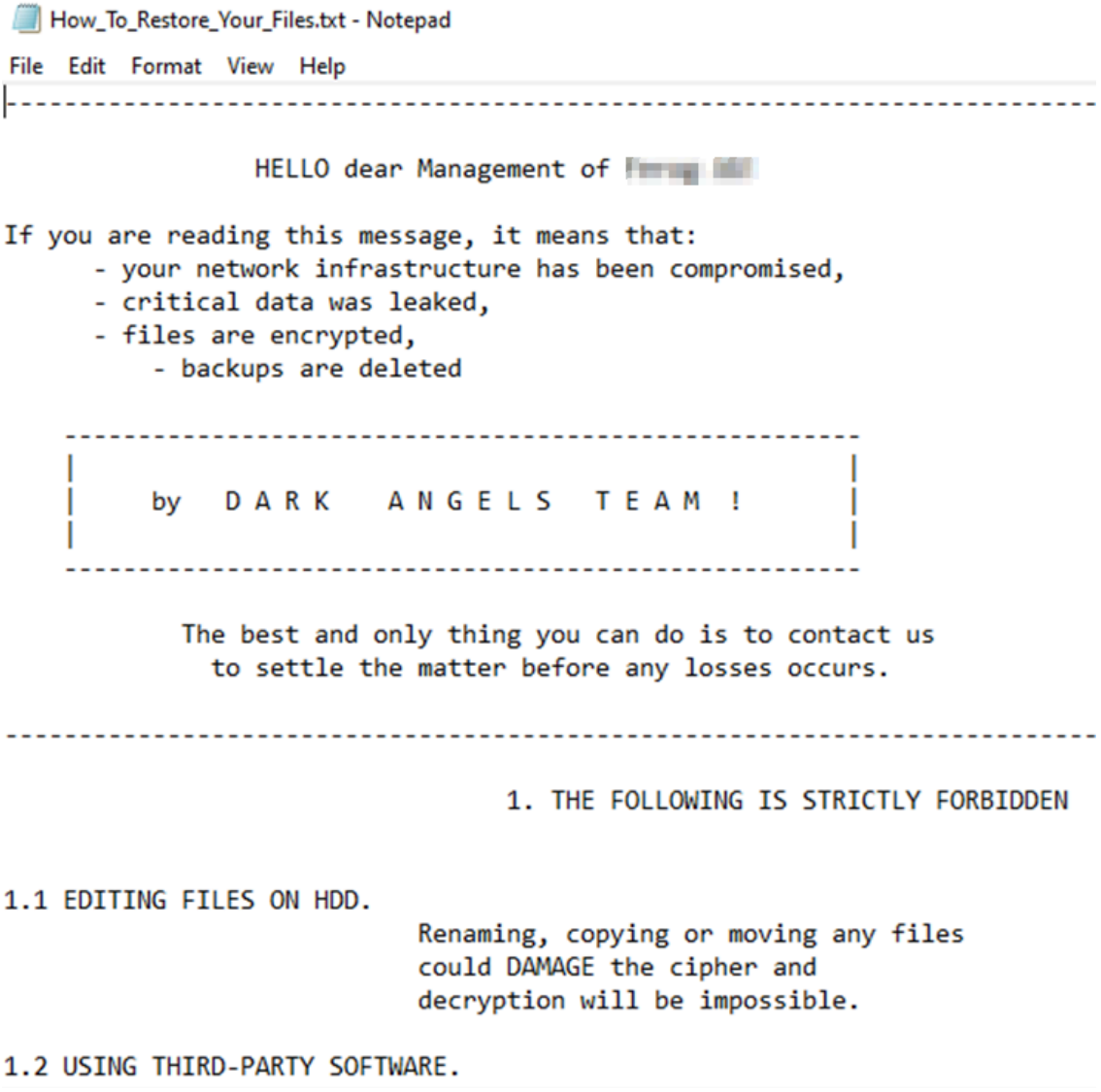

Figure 9 – Ransom note

In their ransom note, the TAs have instructed victims to contact them through their TOR website. In addition, the TAS threatens the victims to disclose their data if they do not respond within four days after the attack and notify government supervision agencies, competitors, and clients.

After dropping the ransom notes, the malware encrypts the files on the victim's machine and appends the extension with ".crypt," as shown in the below figure.

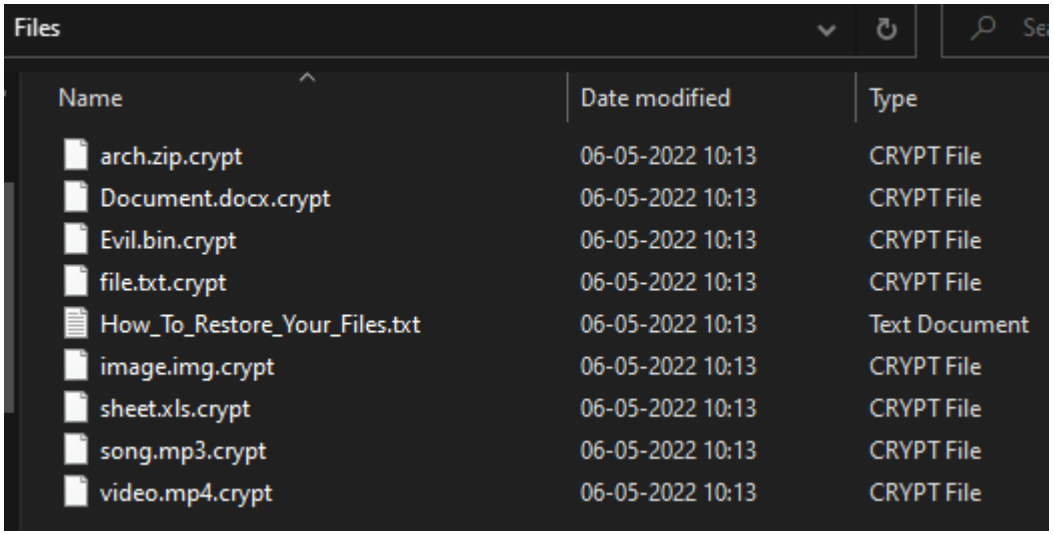

Figure 10 – Encrypted Files on the Machine

DarkAngels has the capability to be spared through network shares and paths of the infected machine, as shown in Figure 11.

```
lpString = sub_404C00(pNumArgs, (int)v19, L"shares");
lpString2 = sub_404C00(pNumArgs, (int)v19, L"paths");
```

Figure 11 – Checks for Network shares and paths

If the given command-line argument is “shares,” then the ransomware finds Network shares and retrieves information about each shared resource on a server using *NetShareEnum*() API. Furthermore, it checks for $ADMIN share and starts encrypting the files.

```
if ( lpString )
{
  v22 = 1;
  v9 = lstrlenW(lpString);
  for ( j = 0; j < v9; ++j )
  {
    if ( lpString[j] == 44 )
    {
      lpString[j] = 0;
      ++v22;
    }
  }
  do
  {
    v3 = lstrlenW(lpString);
    lpString1 = (LPWSTR)sub_412DE0(2 * v3 + 2);
    lstrcpyW(lpString1, lpString);
    sub_40A980(lpString1);
    sub_412E10(lpString1);
    v4 = lstrlenW(lpString);
    lpString += v4 + 1;
    --v22;
if ( lstrcmpW(*(LPCWSTR *)v9, L"ADMIN$")
{
  lstrcpyW(String1, L"\\\\");
  lstrcatW(String1, servername);
  lstrcatW(String1, L"\\");
  lstrcatW(String1, *(LPCWSTR *)v9);
  sub_40A5C0(String1);
```

Figure 12 – Enumerate Shares and Encrypt Files

If the given command-line argument is “paths,” then the ransomware calls *GetDriveTypeW()* API to find out the network drive connected to the infected machine. Once the network drive is identified, the ransomware starts encrypting the files.

```
if ( lpString2 )
{
  v20 = 1;
  v8 = lstrlenW(lpString2);
  for ( k = 0; k < v8; ++k )
  {
    if ( lpString2[k] == 44 )
    {
      lpString2[k] = 0;
      ++v20;
    }
  }
  do
  {
    v5 = lstrlenW(lpString2);
    v28 = (LPWSTR)sub_412DE0(2 * v5 + 2);
    lstrcpyW(v28, lpString2);
    if ( lstrlenW(v28) == 2 && v28[1] == 58 )
      sub_40AAB0(*v28);
    else
      sub_40A5C0(v28);
    sub_412E10(v28);
```

```
lstrcpyW(lpString1, L"\\\\?\\");
lstrcpyW(lpString1 + 5, L":");
lpString1[4] = a1;
DriveTypeW = GetDriveTypeW(lpString1);
if ( DriveTypeW && DriveTypeW != 5 )
{
  if ( DriveTypeW == 4 )
  {
    nLength = 260;
    lpRemoteName = (LPWSTR)sub_412DE0(520);
    if ( lpRemoteName )
    {
      if ( !WNetGetConnectionW(lpString1 + 4, lpRemoteName, &nLength)
        sub_40A5C0(lpRemoteName);
      sub_412E10(lpRemoteName);
```

Figure 13 – Enumerate Drives and Encrypt Files

When the command line arguments “-paths” and “-shares” are not provided, and also no mutex named “DarkAngels” opened in the infected machine then, the ransomware recursively traverses through all local drives and encrypts the files.

```
LogicalDrives = GetLogicalDrives();
if ( LogicalDrives )
{
  for ( m = 65; m <= 0x5Au; ++m )
  {
    if ( (LogicalDrives & 1) != 0 )
      sub_40AAB0(m);
    LogicalDrives >>= 1;
```

Figure 14 – Enumerates Local Drives

The below image shows the warning message to a victim company.

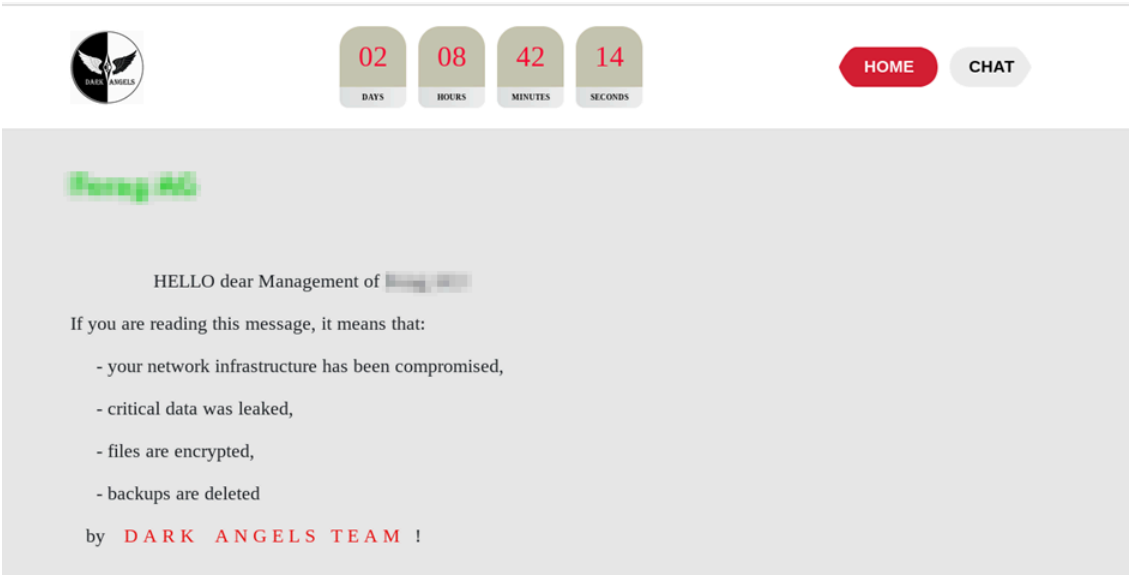

Figure 15 – Warning message to a Victim Company

The below image shows the financial transactions of over $1M to the TAs BTC address.

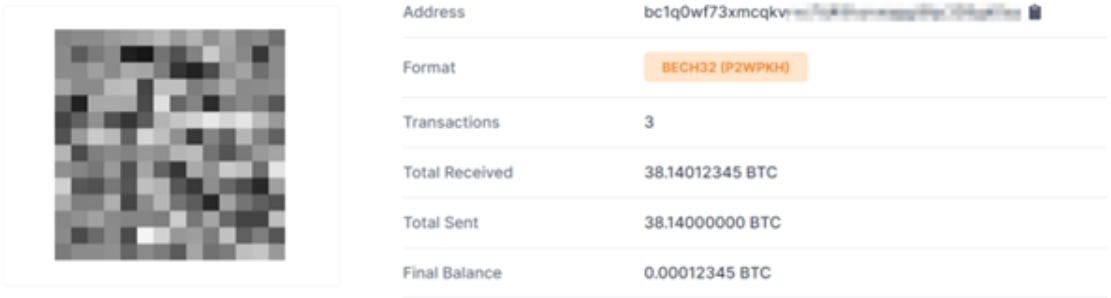

Figure 16 – Financial Transactions

Conclusion

There is a strong correlation between the DarkAngels malware and the existing Babuk ransomware code. It is common for threat actors to leverage existing code, modifying it, and rebranding it. Unlike Babuk ransomware, the Dark Angels are using the malware to target specific organizations. This approach shows some TAs are specifically selecting their targets. Thus far no DarkAngels leak site has been identified. However, considering the targeted attacks one might appear soon.

We will continue to monitor DarkAngels' extortion campaigns and update our readers with the latest information.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety measures needed to prevent ransomware attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Users should take the following steps after the ransomware attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impacts and cruciality Of DarkAngels Ransomware:

- Loss of Valuable data.
- Loss of organization's reliability or integrity.
- Loss of organization's business information.
- Disruption in organization operation.
- Economic loss.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Discovery	T1082	System Information Discovery
Impact	T1490 T1489 T1486	Inhibit System Recovery Service Stop Data Encrypted for Impact

---

Source: https://blog.cyble.com/2022/05/06/rebranded-babuk-ransomware-in-action-darkangels-ransomware-performs-targeted-attack/