Bumblebee Loader on The Rise

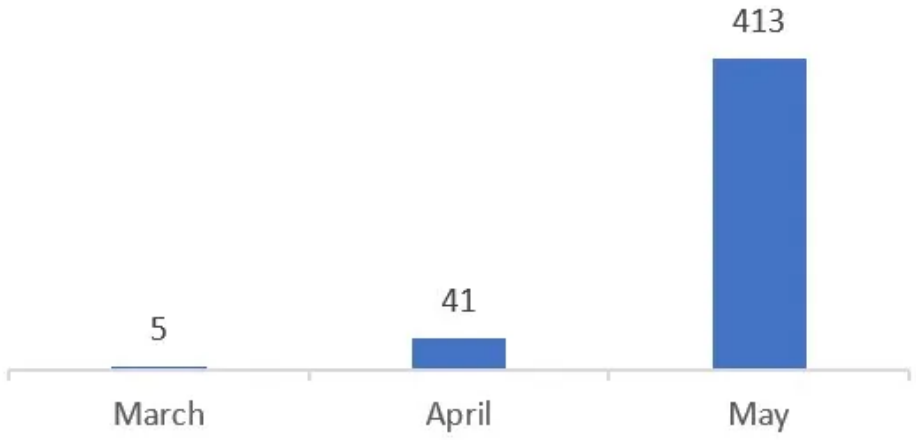
blog.cyble.com/2022/06/07/bumblebee-loader-on-the-rise/

June 7, 2022

Sophisticated loader delivers Cobalt-Strike Beacons

In March 2022, a new malware named “Bumblebee” was discovered and reportedly distributed via spam campaigns. Researchers identified that Bumblebee is a replacement for BazarLoader malware, which has delivered Conti Ransomware in the past. Bumblebee acts as a downloader and delivers known attack frameworks and open-source tools such as Cobalt Strike, Shellcode, Sliver, Meterpreter, etc. It also downloads other types of malware such as ransomware, trojans, etc.

Our intelligence indicates that the incidents of Bumblebee infection are on the rise, as shown below.



Rise of Bumblebee Malware

The Bumblebee infection starts through spam email. This email contains a link to further download an ISO file that eventually drops the malicious Dynamic Link Library (DLL) file. The DLL file further loads Bumblebee's final payload on the victim's machine.

ISO files are a type of archive file that contain an identical copy of data found on an optical disc, CDs, DVDs, etc. They are primarily used to back up optical discs or distribute large file sets intended to burn onto an optical disc.

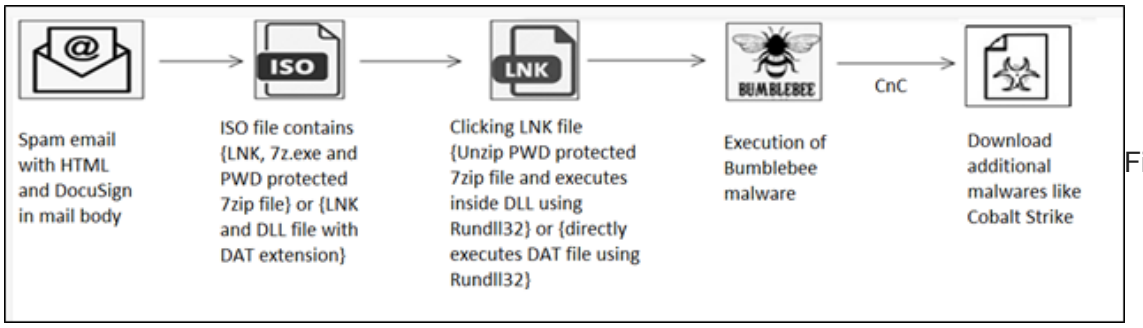


Figure 1 – Bumblebee Infection Vector

Technical Details:

The complete technical analysis of Bumblebee is mentioned in the following sections. Cyble Research Labs analysed the hash (SHA256), "*3e698d8d6e7820cc337d5e2eb3d8fbae752a4c05d11bcf00d3cb7d6dc45e1884*" for analysis.

Bumblebee Initial Access:

Bumblebee has been distributed through spear-phishing email messages that use different methods to trick users into downloading and opening the ISO files.

The spam email contains an HTML attachment as well as a hyperlink in the mail body to download the ISO file. Similarly, the HTML attachment contains a link that downloads the ISO file from Microsoft OneDrive.

Figure 2 shows the spam email that downloads ISO files from Microsoft OneDrive when users click on the "REVIEW THE DOCUMENT" hyperlink.

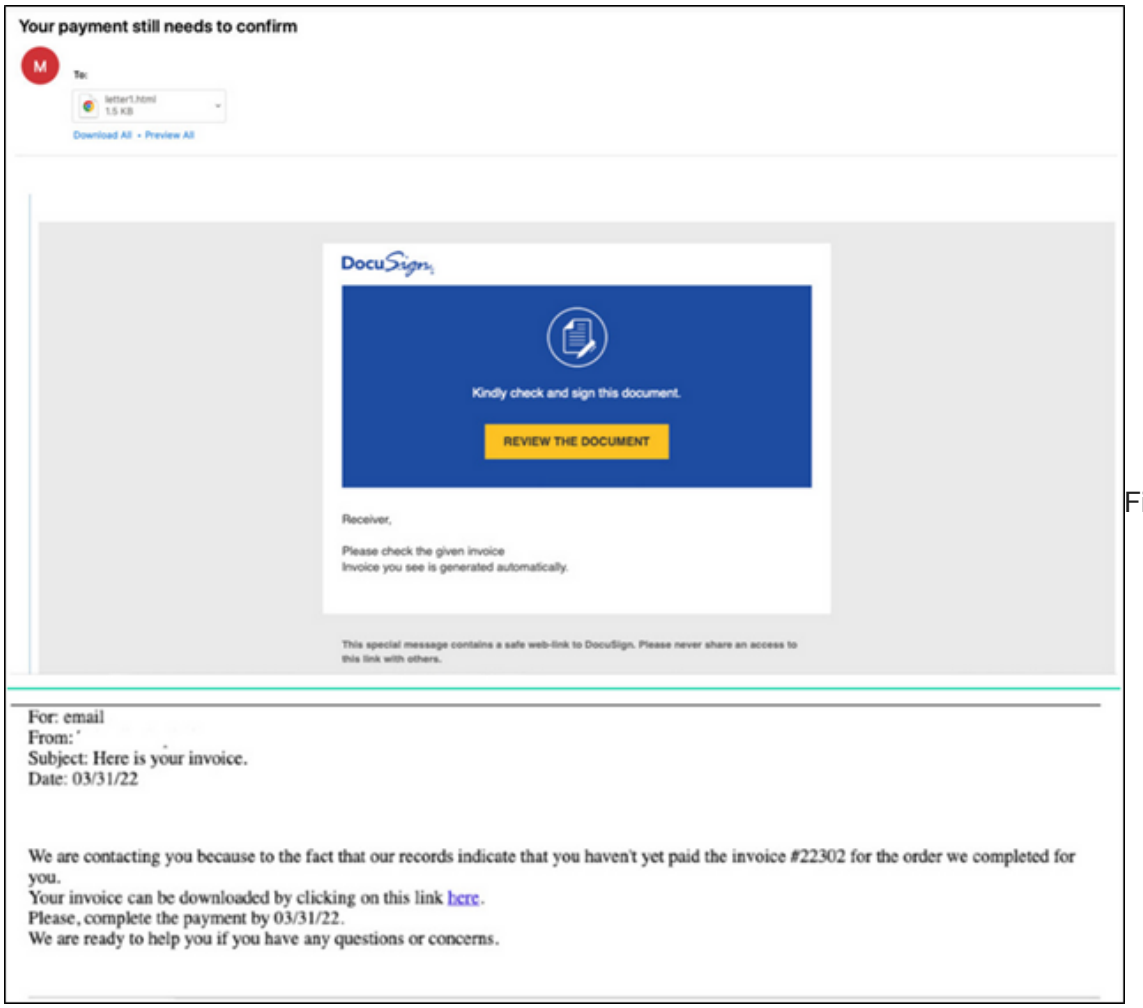


Figure 2 – Spam Email (Source – Proofpoint)

The ISO file contains two files called *Attachments.lnk* and *Attachments.dat*. This malicious link file contains the parameters to execute *"Attachments.dat,"* which is the Bumblebee payload, using Windows' *rundll32.exe* service.

Figure 3 shows the contents of the ISO file and properties of the .lnk file.

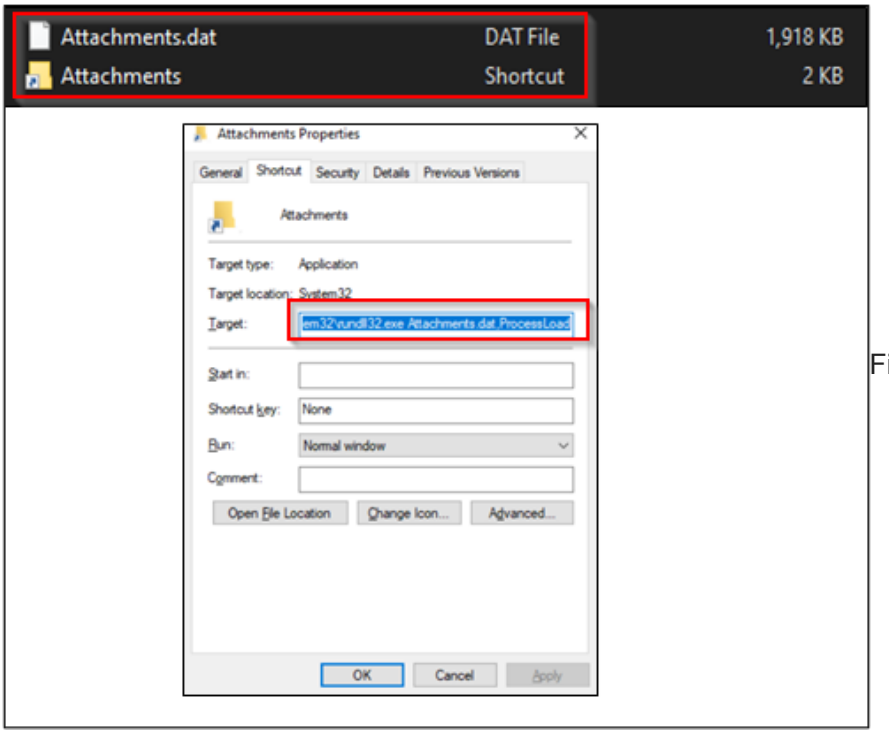


Figure 3 – Contents of the ISO File and Properties of Malicious .lnk File

Target command line:

> *cmd.exe /c start /wait "" "C:\Users\Admin\Local\Temp\Attachments.lnk" rundll32.exe "C:\Windows\System32\rundll32.exe" Attachments.dat,ProcessLoad*

In another case of infection, the ISO file contains three files, namely *New Folder.LNK*, *7z.exe,* and *arch.7z*. The shortcut file *New Folder.LNK* launches powershell.exe and extracts the password-protected file *arch.7z* by using *7z.exe*.

The *arch.7z* file contains a 64-bit DLL file named "arch.dll," which is a Bumblebee loader. The PowerShell command extracts the *arch.dll* file into the location *C:\ProgramData* and executes it using *rundll32.exe.*

Figure 4 shows the contents of the ISO file and properties of the .lnk file.

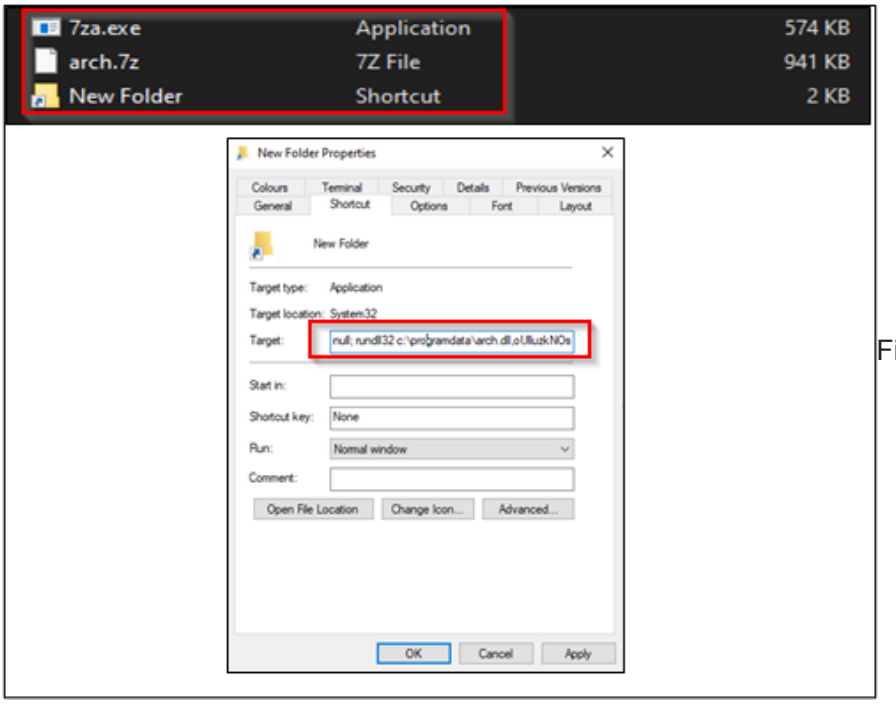


Figure 4 – Contents of Malicious ISO and Properties of .lnk file

Target command line:

> *C:\Windows\System32\cmd.exe /c powershell -WindowStyle Hidden -Command ".\7za.exe x arch.7z -p434330cf2449 -o\"c:\programdata\" -y > $null; rundll32 c:\programdata\arch.dll,oUlluzkNOs*

Defensive Evasion:

Bumblebee downloads and executes the other payloads on victim machines without being detected by any antivirus programs. Bumblebee uses various techniques to inject and attach the payloads into the running process.

The Bumblebee loader has a list of process names related to tools used by security researchers to identify if the malware is debugged or running in a virtual environment. The malware terminates its execution if it identifies any of these processes running on the victim's machine. The figure below shows the list of process names.

Figure 5 – List of the Security Tools

The malware terminates its execution if it is identified to be running in a sandbox environment. The malware calls the *Wine_get_unix_file_name()* API to identify the sandbox machine, as shown below.

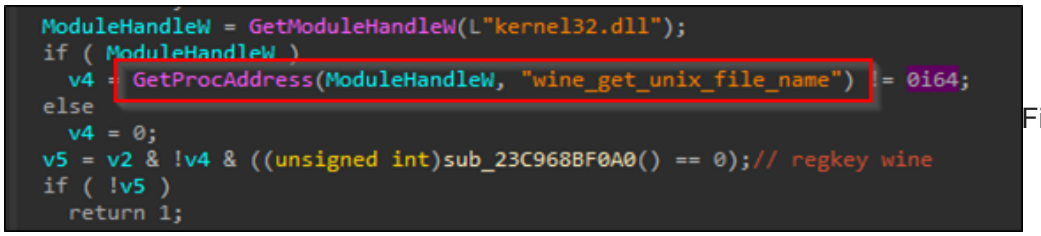


Figure 6 – Sandbox Detection using GetProcAddress()

Bumblebee also avoids running in the sandbox environment by comparing the victim's specific usernames with a list of hard-coded usernames. The hard-coded names are commonly-used sandbox usernames seen in the wild.

If user account names match with the names on the list, the malware terminates itself. A list of user account names is shown in the figure below.

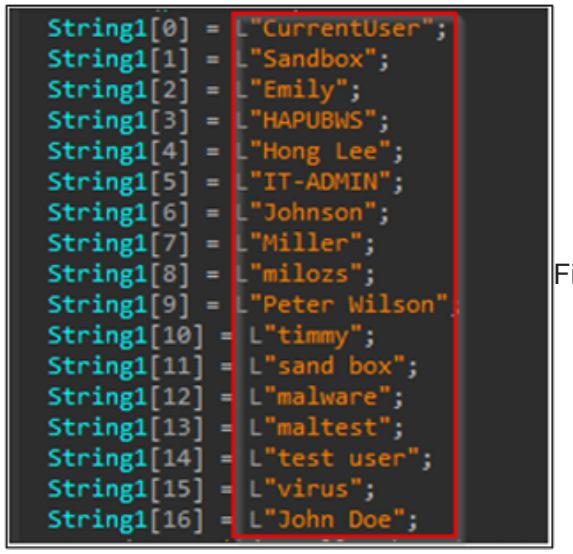


Figure 7 – List of Hardcoded User Accounts

The malware performs additional checks to identify the virtual environment, such as Wine, Vbox, and VMware. To identify the virtual environment, the malware performs the following actions:

- Queries registry keys related to Virtual Machine-related software
- Executes WMI queries to identify them
- Identifies emulator by reading the respective registry keys
- Identify the window name of the running process

This technique used by malware is highlighted in the figure below.

Figure 8 – Additional Defence Evasion Techniques

After the evading detection, Bumblebee resolves its function names at runtime and creates a unique event name, *3C29FEA2-6FE8-4BF9-B98A-0E3442115F67.*

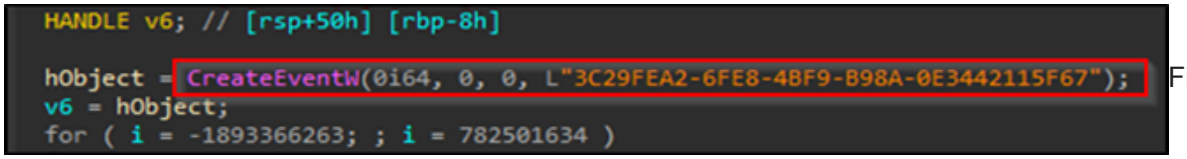


Figure 9 – Bumblebee Creating Unique Event

The malware uses WMI queries to collect details such as system details, adapter details, etc., from the victim's machine. After that, it sends the stolen information to the Command and Control (C&C) server.

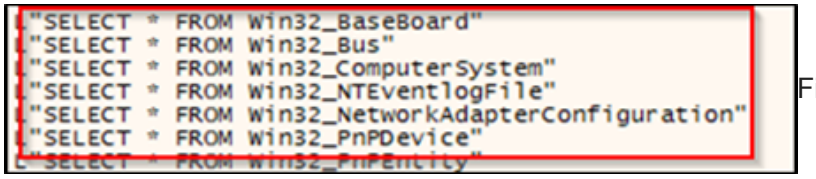


Figure 10 – WMI Queries

The Bumblebee Loader uses various commands to perform malicious activities such as DLL injection, downloading executables, uninstalling loaders, and enabling persistence. The commands used by the malware are mentioned below.

- “dij”
- “dex”
- “sdl”
- “ins”

DLL Injection:

The malware receives the “dij” command for DLL and Shellcode injection. As shown in Figure 11, it injects Shellcode into legitimate processes using the APC routine. It specifically injects code into the below processes:

- *\\Windows Photo Viewer\\ImagingDevices.exe*
- *\\Windows Mail\\wab.exe*
- *\\Windows Mail\\wabmig.exe*

```
if ( a2 )
{
  v15 = GetModuleHandleW(L"ntdll.dll");
  v16 = v19;
  NtQueueApcThread = GetProcAddress(v15, "NtQueueApcThread");
  ((void (__fastcall *)(HANDLE, __int64, _QWORD, _QWORD, _DWORD))NtQueueApcThread)(a2, v16, 0i64, 0i64, 0);
  CloseHandle(a2);
}
```

Figure 11 – Process injection via Asynchronous Procedure Calls (APC)

The loader then creates two new sections within the target process and copies the Shellcode to the newly created sections to properly inject the Shellcode. Then it invokes the Shellcode in the target executable via a dynamically resolved *NtQueueApcThread()*.

Downloading Additional Payloads:

The malware receives the “dex” command for downloading and executing additional payloads. After receiving this command along with payload data, it writes the file into a disk using the *CreateFileA()* and *WriteFile()* functions and executes it via the COM object.

In this example, the malware uses the hardcoded name “wab.exe” to store the payload.

```
if ( (!v77 || !memcmp(v76, "dex", v77)) && v67 == 3 )
{
  SHGetSpecialFolderPathA(0i64, &String1, 28, 0);
  lstrcatA(&String1, "\\wab.exe");
  v78 = v167;
  if ( v169 >= 0x10 )
    v78 = (__int64 *)v167[0];
  if ( (unsigned int)sub_23C968BA838(&String1, v78, v168) )
  {
    sub_23C968BB380(&String1);
    *(_DWORD *)(v44 + 136) = 1;
  }
  goto LABEL_261;
}
```

Figure 12 – The dex command operation

Persistence:

The *Ins* command helps enable persistence by copying *the Bumblebee malware*DLL into the *%appdata%* directory and creating a VBS script that loads the malicious DLL using a scheduled task.
The *sdl* command uses PowerShell to delete files from the infected system without prompting the user.
The PowerShell command used by the malware is:

PS C:\> Remove-item -Path "filepath" -Force

C&C Communication:

The figure below shows the COBALT STRIKE traffic from the malware.

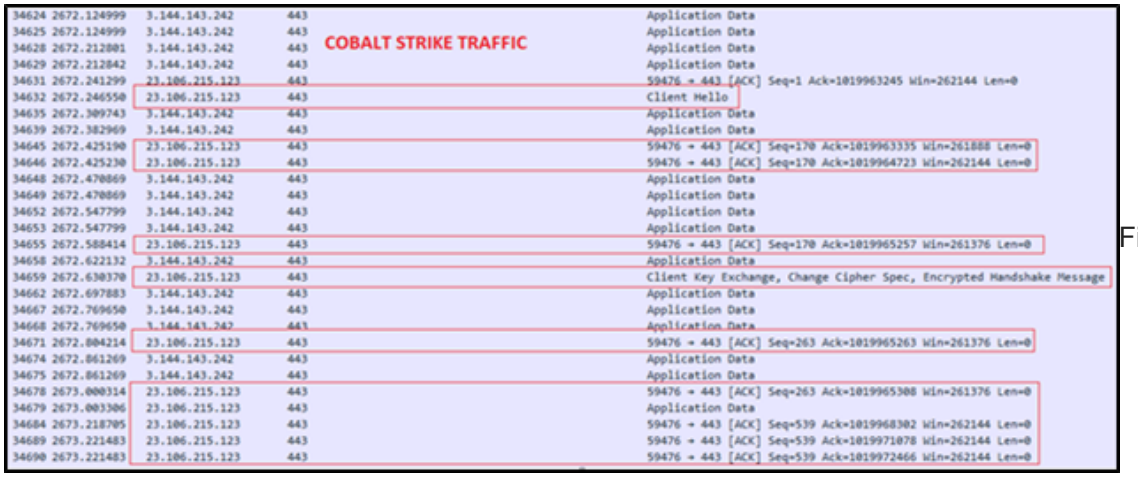


Figure 13 – Cobalt Strike Network Traffic of Bumblebee Malware

Conclusion

Bumblebee is a new and highly sophisticated malware loader that employs extensive evasive maneuvers and anti-analysis tricks, including complex anti-virtualization techniques. To make the Bumblebee malware's activity stealthier and harder to detect, its Threat Actors frequently update these capabilities.

Bumblebee loader can be deployed to facilitate initial access and deliver payloads such as Cobalt Strike, ransomware, etc. It is likely to become a popular tool for ransomware groups to deliver their payload.

Cyble Research Labs closely monitors the BumbleBee malware group and other similar Threat Actor activities and analyzes them to better understand their motivations and keep our readers well-informed.

Our Recommendations

- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Avoid downloading files from unknown websites.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed antivirus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Block URLs that could spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on the employees' systems.

MITRE ATT&CK® Techniques:

Tactic	Technique ID	Technique Name
Initial Access	T1566 T1190	Phishing Exploit Public-Facing Application.
Execution	T1059	Command and Scripting Interpreter
Defence Evasion	T1497	Virtualization/Sandbox Evasion
Persistence	T1053	Scheduled Task/Job
Discovery	T1012 T1082	Query Registry System Information Discovery
Credential Access	T1552	Unsecured Credentials
Lateral Movement	T1021	Remote Services
Impact	T1496	Resource Hijacking

Indicators Of Compromise:

Indicators	Indicator Type	File name
7092d2c4b041db8009962e865d6c5cd7 11838141f869e74225be8bd0d4c866cb46ef0248 0e859acbd03e59eae287b124803ec052cf027b519e608c7ccfd920044b9ee1c7	MD5 SHA1 Sha256	New-Folder-00519.img
42badc1d2f03a8b1e4875740d3d49336 cee178da1fb05f99af7a3547093122893bd1eb46 c136b1467d669a725478a6110ebaaab3cb88a3d389dfa688e06173c066b76fcf	MD5 SHA1 Sha256	7z.exe
310803b7d4db43f2bd0040e21a4ef9fc f42c381524b5f52f0e1a5a8c60d62464b8644968 b091415c1939d1da9a7d07901dd3d317a47b2a8ccc9c666d8cf53a512a80b8d6	MD5 SHA1 Sha256	arch.7z
fd21be3db76b714cb4dfae779d1ada1f 8157b198c00de0a19b1d02ae7b76c78857baccd2 315b3d80643da454b40cc938a0e8794f90ccbd05868e55b4848cacbf047850ae	MD5 SHA1 Sha256	New Folder.LNK
16da4284ab7ab9d5669c34c339132ed6 34dc625fc243d06cbc33d403ac7ee05edfd32819 1249075a0c4af8ecfeb4a3ab1e9ef692cb8876591d73f3470106402ab1592717	MD5 SHA1 Sha256	arch.dll
c9cf08565a10f4c46308037bd31a7f46 17752edb2473b4a246d6a6980375bd87133e7514 3e698d8d6e7820cc337d5e2eb3d8fbae752a4c05d11bcf00d3cb7d6dc45e1884	MD5 SHA1 Sha256	LdrAddx64.dll
33e03ca5dd9a8f85fdcf091a97312e45 186981f889ad88a0d5f21c18adb8b35c78851c74 64c299dc88a35d4ef551516be4f7ed95ae568a6ee0b66a1fcfc3f68bf80d87fe	MD5 SHA1 Sha256	wab.exe
23.254.229[.]131	IP	C&C

79.110.52[.]71	IP	C&C
51.75.62[.]99	IP	C&C
23.106.215[.]123	IP	C&C