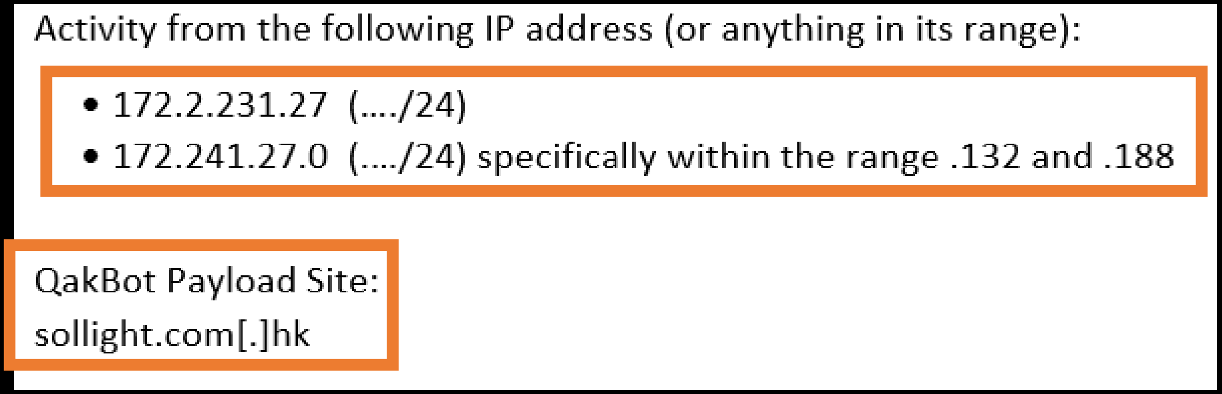
Examination of the document content 2/2

(hash 5267cc...)

- In addition to the Qakbot sample, the payload domain can also be found in the IOC document → **sollight.com[.]hk**
- Apparently, IP addresses of the range 172.x.x.x also showed malicious activity, which will be discussed later.



Activity from the following IP address (or anything in its range):

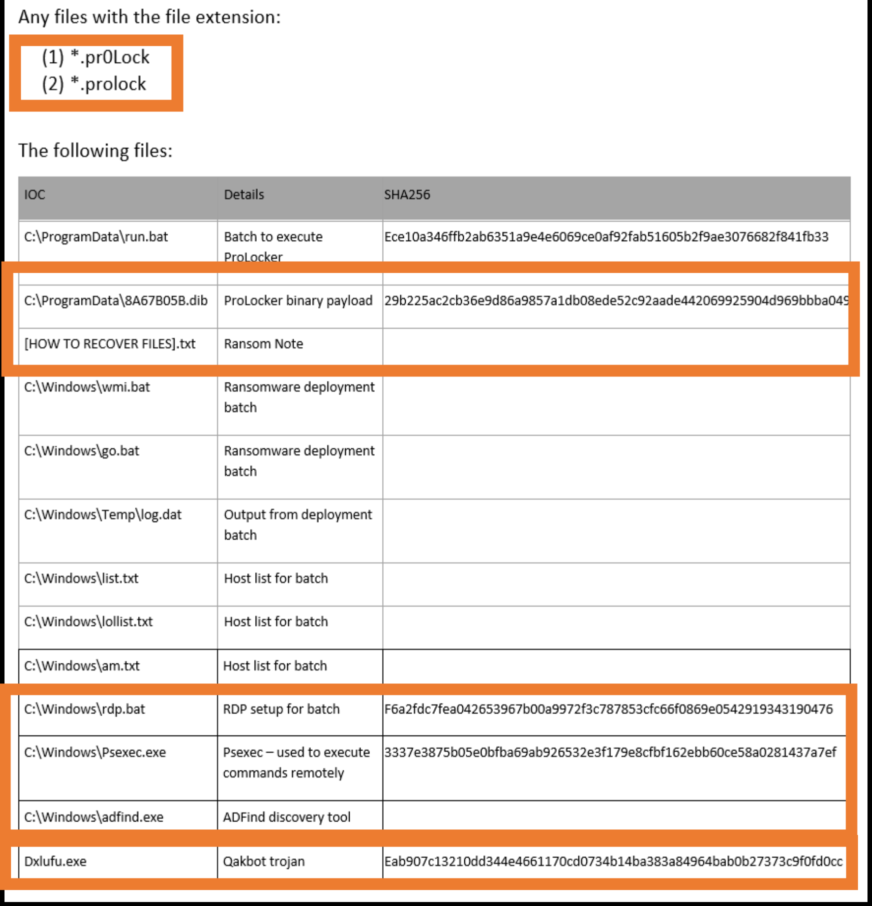
- 172.2.231.27 (..../24)
- 172.241.27.0 (..../24) specifically within the range .132 and .188

QakBot Payload Site:
sollight.com[.]hk

Examination of the document content 1/2

(hash 5267cc…)

- The forensic traces confirm the statements on Krebsonsecurity.com that files were encrypted with the **ProLock** ransomware.
- Another interesting IOC is the reference to a **Qakbot** payload.
  - On May 4, 2020 the FBI issued a security alert reporting the ProLock gang gains initial access to victim networks via the Qakbot trojan since March 2020.
- Files such as **rdp.bat**, **Psexec.exe** and **adfind.exe** were likely used for lateral movement to gain access to the domain controller or other interesting targets.



Any files with the file extension:

(1) *.pr0Lock
(2) *.prolock

The following files:

IOC	Details	SHA256
C:\ProgramData\run.bat	Batch to execute ProLocker	Ece10a346ffb2ab6351a9e4e6069ce0af92fab51605b2f9ae3076682f841fb33
C:\ProgramData\8A67B05B.dib	ProLocker binary payload	29b225ac2cb36e9d86a9857a1db08ede52c92aade442069925904d969bbba049
[HOW TO RECOVER FILES].txt	Ransom Note	
C:\Windows\wmi.bat	Ransomware deployment batch	
C:\Windows\go.bat	Ransomware deployment batch	
C:\Windows\Temp\log.dat	Output from deployment batch	
C:\Windows\list.txt	Host list for batch	
C:\Windows\lollist.txt	Host list for batch	
C:\Windows\am.txt	Host list for batch	
C:\Windows\rdp.bat	RDP setup for batch	F6a2fdc7fea042653967b00a9972f3c787853cfc66f0869e0542919343190476
C:\Windows\Psexec.exe	Psexec – used to execute commands remotely	3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
C:\Windows\adfind.exe	ADFind discovery tool	
Dxlufu.exe	Qakbot trojan	Eab907c13210dd344e4661170cd0734b14ba383a84964bab0b27373c9f0fd0cc