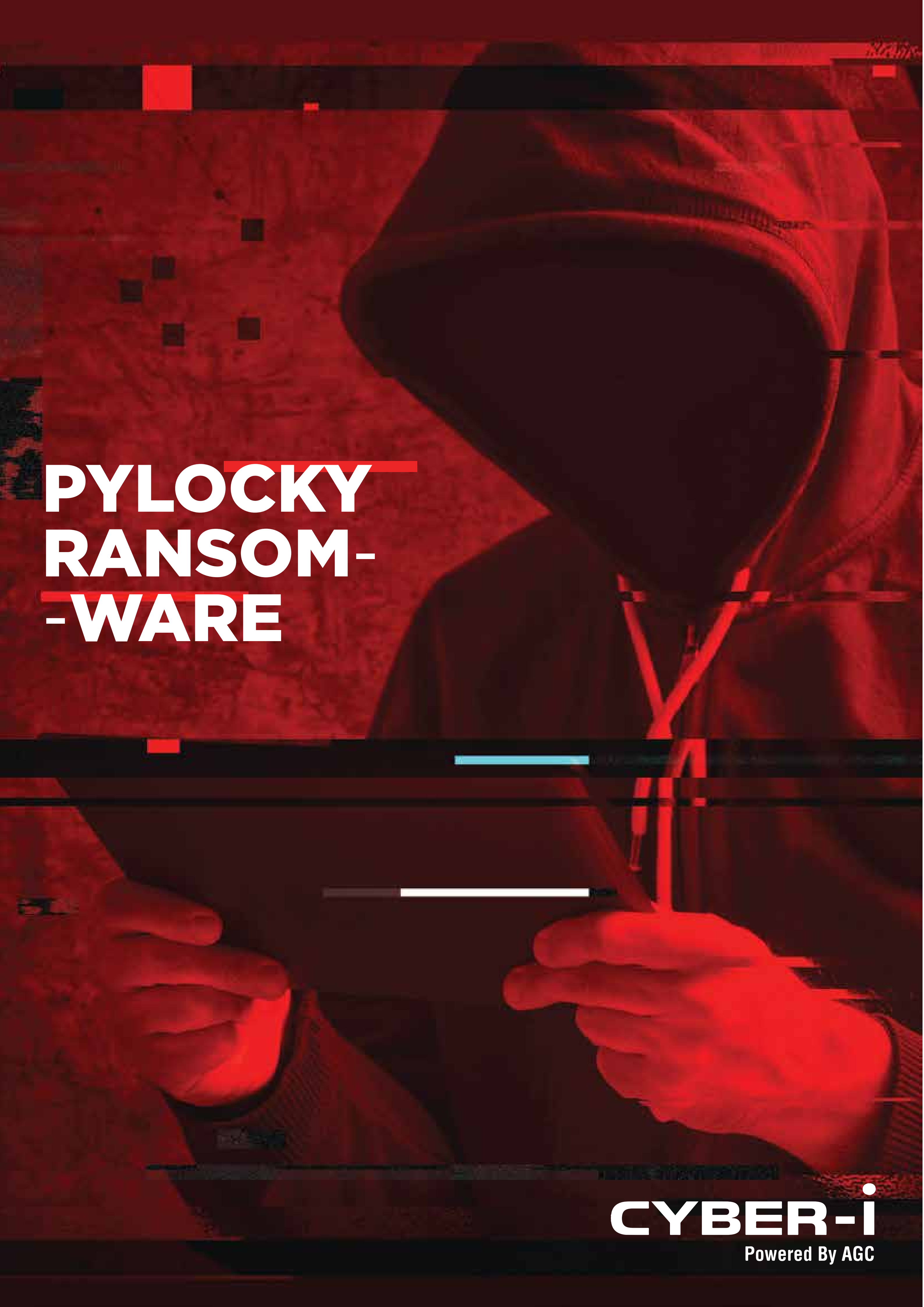


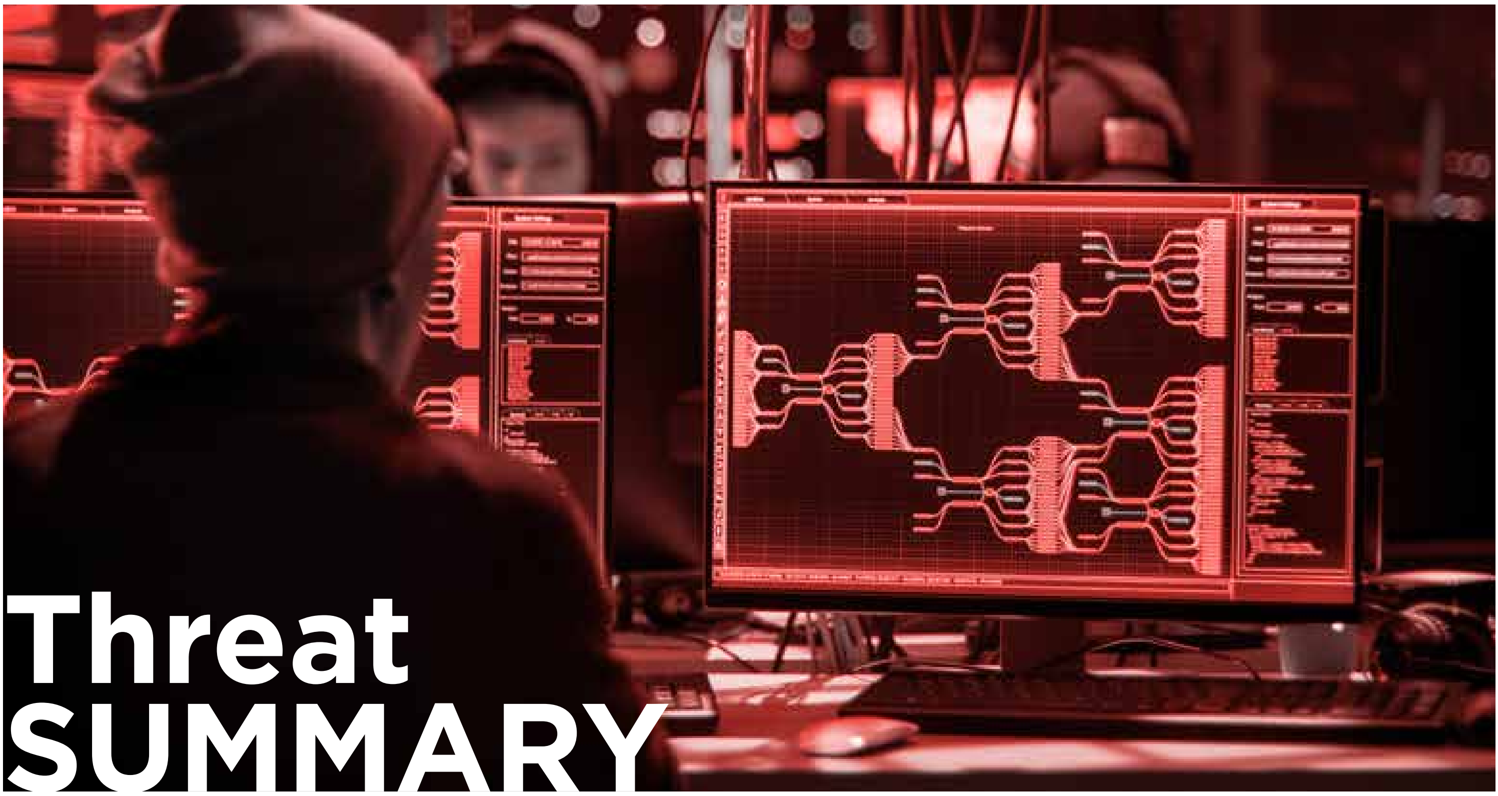
PYLOCKY RANSOMWARE

CYBER-i

Powered By AGC

VULNERABILITY SUMMARY

PyLocky ransomware written in python and packed with PyInstaller which helps to package the python based application as a stand-alone executable. Unlike other Ransomware, PyLocky contains anti-machine learning capability that makes very difficult for static analyses and it's very challenging one for researchers in depth analysis. Name itself claimed that, this ransomware belongs to Locky which is one of the most destructive malware in history that compromised various sector around the world but it doesn't have any relation with original Locky ransomware.



Threat SUMMARY

Name :	PyLocky
Type:	Ransomware, Cryptovirus
Symptoms :	The files on your computer have the .lockymap extension added to them and cannot be opened
Distribution Method :	Spam Emails, Email Attachments, Executable files.

TECHNICAL DETAILS

The initial stage of infection starts with a spam email campaign along with malicious attachment which distributed to the victims and trick them to click the link using social engineering techniques that drop PyLocky.

Once click the URL then drops a signed executable (Facture_23100.31.07.2018.exe) that eventually drops the Malware component that also contains the main ransomware executable (lockyfud.exe).

In addition to the main infection file, other files may also be dropped on the victim's computer and they are likely located in the following directories:

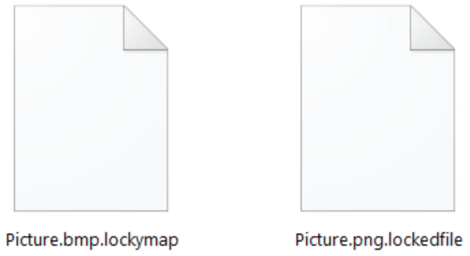
%Temp%
%AppData%
%Local%
%LocalLow%
%Roaming%

After completing its execution process, PyLocky encrypts more than 100 extension files including image, video, document, sound, program, game, database, and archive files, among others. once it completes the encryption process, PyLocky communicates with its command & control server and drops the ransom notes.

EXTENSION FILES THAT ARE AFFECTED

PNG .PSD .PSPIMAGE .TGA .THM .TIF .TIFF .YUV .AI .EPS .PS .SVG .INDD .PCT .PDF .XLR .XLS .XLSX .ACCDB .DB .DBF .MDB .PDB .SQL .APK .APP .BAT .CGI .COM .EXE .GADGET .JAR .PIF .WSF .DEM .GAM .NES .ROM .SAV CAD Files .DWG .DXF GIS Files .GPX .KML .KMZ .ASP .ASPX .CER .CFM .CSR .CSS .HTM .HTML .JS .JSP .PHP .RSS .XHTML. DOC .DOCX .LOG .MSG .ODT .PAGES .RTF .TEX .TXT .WPD .WPS .CSV .DAT .GED .KEY .KEYCHAIN .PPS .PPT .PPTX .INI .PRF Encoded Files .HQX .MIM .UUE .7Z .CBR .DEB .GZ .PKG .RAR .RPM .SITX .TAR.GZ .ZIP .ZIPX .BIN .CUE .DMG .ISO .MDF .TOAST .VCD SDF .TAR .TAX2014 .TAX2015 .VCF .XML Audio Files .AIF .IFF .M3U .M4A .MID .MP3 .MPA .WAV .WMA Video Files .3G2 .3GP .ASF .AVI .FLV .M4V .MOV .MP4 .MPG .RM .SRT .SWF .VOB .WMV 3D .3DM .3DS .MAX .OBJ R.BMP .DDS .GIF .JPG .CRX .PLUGIN .FNT .FON .OTF .TTF .CAB .CPL .CUR .DESKTHEMEPACK .DLL .DMP .DRV .ICNS .ICO .LNK .SYS .CFG

After this, the ransomware may encrypt the files, setting two different file extensions – .lockedfile and .lockymap. The encrypted files start to appear like the following:



INDICATORS OF COMPROMISE

Hashes detected as RANSOM_PYLOCKY.A (SHA-256):

- c9c91b11059bd9ac3a0ad169deb513cef38b3d07213a5f916c3698bb4f407ffa
- 1569f6fd28c666241902a19b205ee8223d47cccdd08c92fc35e867c487ebc999

Related hashes (SHA-256):

- e172e4fa621845080893d72ecd0735f9a425a0c7775c7bc95c094ddf73d1f844 (Facture_23100.31.07.2018.zip)
- 2a244721ff221172edb788715d11008f0ab50ad946592f355ba16ce97a23e055 (Facture_23100.31.07.2018.exe)
- 87aadc95a8c9740f14b401bd6d7cc5ce2e2b9beec750f32d1d9c858bc101dffa (facture_31254872_18.08.23_{numbers}.exe)

Related malicious URLs:

- hxxps://centredentairenantes[.]fr (C&C server)
- hxxps://panicpc[.]fr/client[.]php?fac=676171&u=0000EFC90103
- hxxps://savigneuxcom[.]securesitefr[.]com/client.php?fac=001838274191030

SAMPLE REPORT FROM HYBRID ANALYSIS

https://www.hybrid-analysis.com/sample/2a244721ff221172edb788715d11008f0ab50ad946592f355ba16ce97a23e055?environmentId=100

https://www.hybrid-analysis.com/sample/95c6dee470e963ab9b7f92e122e04a3fcdc05b01455047218af7d23264b57561?environmentId=100

MITIGATION

With so many attack vectors available for the attackers, safeguarding your organization's assets requires you to establish a multi-layered approach to security. Apply best practices like regularly backing up files, keeping the system updated, securing the use of system components and promoting a culture of cybersecurity awareness. Moreover, the threat indicators may help in blocking out certain security threats if used correctly.

Removal steps:

- https://www.2-spyware.com/remove-pylocky-ransomware.html
- https://www.precisesecurity.com/virus/remove-pylocky-ransomware-lockedfile-files
- https://www.removeallvirus.com/remove-pylocky-ransomware-virus-from-computer-in-5-minutes-and-recover-locked-files
- https://malwareless.com/pylocky-ransomware-virus-free-removal-guide/

REFERENCE

- https://sensorstechforum.com/lockymap-files-virus-pylocky-ransomware-remove-restore-data/
- https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/
- http://www.rewterz.com/rewterz-news/rewterz-threat-advisory-pylocky-ransomware-using-unique-evasion-tactics

Let's ensure a Cyber Safe environment around us. Rely on AGC for all your Cyber Security concerns so that you can continue conquering organizations objectives

ABOUT AGC NETWORKS

AGC Networks (AGC) is a Global Solution Provider representing the world's best brands in Unified Communications, Data Center and Edge IT, Cyber Security (CYBER-i) and Digital Transformation & Applications to evolve the customer's digital landscape. AGC's ability to tailor solutions is strengthened by seamless services. For more details visit www.agcnetworks.com

info@agcnetworks.com
www.agcnetworks.com

32 Years of ICT Experience | 9 Global Locations | 3000+ Clients | Leading Technology Partners | Global Service Delivery