Look for a fix, get malware instead: examining the Cyrat ransomware

By Karsten Hahn

Published: 2021-06-22 · Archived: 2026-04-06 00:55:50 UTC

Encryption

Cyrat ransomware uses Fernet to encrypt files. This is a symmetric encryption method meant for small data files that fit into RAM. While Fernet is not unusual itself, it is not common for ransomware and in this case even problematic. This ransomware encrypts whole files regardless how big they are, whereas Fernet is unsuitable for big files.

A public RSA key is used to encrypt the Fernet key. This public key is downloaded from Mediafire instead of shipping it with the ransomware. This adds another dependency. The encrypted Fernet key is saved in **Desktop\EMAIL_US.txt**. A user with an infected system is required to send this file to the criminals.

Cyrat appends **.CYRAT** to encrypted files. It has a list of folders that it checks for target files. Those folders are 'Desktop', 'Downloads', 'Pictures', 'Music', 'Videos', and 'Documents'.

It targets files with the following extensions: 'doc', 'docx', 'xls', 'xlsx', 'ppt', 'pptx', 'boop', 'pst', 'ost', 'msg', 'eml', 'vsd', 'vsdx', 'txt', 'csv', 'rtf', '123', 'wks', 'wk1', 'pdf', 'dwg', 'onetoc2', 'snt', 'jpeg', 'jpg', 'docb', 'docm', 'dot', 'dotm', 'dotx', 'xlsm', 'xlsb', 'xlw', 'xlt', 'xlm', 'xlc', 'xltx', 'xltm', 'pptm', 'pot', 'pps', 'ppsm', 'ppsx', 'ppam', 'potx', 'potm', 'edb', 'hwp', '602', 'sxi', 'sti', 'sldx', 'sldm', 'sldm', 'vdi', 'vmdk', 'vmx', 'gpg', 'aes', 'PAQ', 'bz2', 'tbk', 'bak', 'tar', 'tgz', 'gz', '7z', 'rar', 'zip', 'backup', 'iso', 'vcd', 'bmp', 'png', 'gif', 'raw', 'tif', 'tiff', 'nef', 'psd', 'ai', 'svg', 'djvu', 'm4u', 'm3u', 'mid', 'wma', 'flv', '3g2', 'asf', 'mpeg', 'vob', 'mpg', 'swf', 'wav', 'mp3', 'sh', 'class', 'jar', 'java', 'rb', 'asp', 'php', 'jsp', 'brd', 'dch', 'dip', 'pl', 'vb', 'vbs', 'ps1', 'bat', 'cmd', 'asm', 'h', 'pas', 'c', 'cs', 'suo', 'sln', 'ldf', 'mdf', 'ibd', 'myi', 'myd', 'frm', 'odb', 'dbf', 'db', 'mdb', 'accdb', 'sql', 'sqlitedb', 'sqlite3', 'lay6', 'lay', 'mml', 'sxm', 'otg', 'odg', 'uop', 'std', 'sxd', 'otp', 'odp', 'wb2', 'slk', 'dif', 'stc', 'sxc', 'ots', 'ods', '3dm', 'max', '3ds', 'uot', 'stw', 'sxw', 'ott', 'odt', 'p12', 'csr', 'key', 'pfx', 'der', 'deb', 'mpeg', 'WEBM', 'MPG', 'MP2', 'MPEG', 'MPE', 'MPV', 'OGG', '3gp', 'mp3', 'json', 'css', 'html', 'py', 'exe', 'MP2', 'MPEG', 'MPE', 'MPV', 'OGG', '3gp', 'mp3'

The ransomware lists a few more extensions with a dot in them which is a bug: '.ARC', '.cpp', '.cgm', '.js', '.fla', '.asc', '.crt', '.sch'. These extensions will never be found by Cyrat because the file path is stripped from dots before it is compared with the target extension.

A ransom note named **RANSOME_NOTE.txt** is placed in every target folder. Furthermore a ransomware stock photo is downloaded from **images.idgesg.net** to **Documents\background_img.png** and set as wallpaper. The wallpaper does not contain any ransom message. In this state the stock photo's only purpose is to draw attention to the user.

Source: https://www.gdatasoftware.com/blog/cyrat-ransomware