A Closer Look at the Locky Poser, PyLocky Ransomware

blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/

September 10, 2018

Updated as of September 10, 2018, 6:40 PM PDT to update how PyLocky establishes C&C connection.

While ransomware has noticeably plateaued in today's threat landscape, it's still a cybercriminal staple. In fact, it saw a slight increase in activity in the first half of 2018, keeping pace by being fine-tuned to evade security solutions, or in the case of PyLocky (detected by Trend Micro as RANSOM_PYLOCKY.A), imitate established ransomware families and ride on their notoriety.

In late July and throughout August, we observed waves of spam email delivering the PyLocky ransomware. Although it tries to pass off as Locky in its ransom note, PyLocky is unrelated to Locky. PyLocky is written in Python, a popular scripting language; and packaged with PyInstaller, a tool used to package Python-based programs as standalone executables.

Ransomware written in Python isn't new — we've already seen CryPy (RANSOM_CRYPY.A) in 2016, and Pyl33t (RANSOM_CRYPPYT.A) in 2017 — but PyLocky features anti-machine learning capability, which makes it notable. Through the combined use of Inno Setup Installer (an open-source script-based installer) and PyInstaller, it posed a challenge to static analysis methods, including machine learning-based solutions — something we have already seen variants of Cerber do (although Cerber used NullSoft installer).

PyLocky's distribution also appears to be concentrated; we saw several spam emails targeting European countries, particularly France. And though the spam run started out small, its volume and scope eventually increased.

Figure 1: Distribution of PyLocky-related spam runs on August 2 (left) and August 24 (right)

Figure 2: PyLocky's ransom note pretending to be the Locky ransomware

Infection Chain

On August 2, we detected a spam run distributing PyLocky to French businesses, luring them with socially engineered subject lines such as those related to invoices. The email entices the user to click a link, which redirects users to a malicious URL containing PyLocky.

Figure 3: Spam email with the subject line, "Nous avons reçu votre paiement," which means "We have received your payment".

The malicious URL leads to a ZIP file (*Facture_23100.31.07.2018.zip*) that contains a signed executable (*Facture_23100.31.07.2018.exe*). When successfully run, the *Facture_23100.31.07.2018.exe* will drop malware components — several C++ and Python libraries and the Python 2.7 Core dynamic-link library (DLL) — along with the main ransomware executable (*lockyfud.exe*, which was created via PyInstaller) in C:\Users\{user}\AppData\Local\Temp\is-{random}.tmp.

Figure 4: The digital signature information of the ZIP file (top), and PyLocky-related malware components (bottom)

PyLocky encypts image, video, document, sound, program, game, database, and archive files, among others. Here's a list of file types PyLocky encrypts:

.dat, .keychain, .sdf, .vcf, .jpg, .png, .tiff, .gif, .jpeg, .jif, .jp2, .jpx, .j2k, .j2c, .fpx, .pcd, .bmp, .svg, .3dm, .3ds, .max, .obj, .dds, .psd, .tga, .thm, .tif, .yuv, .ai, .eps, .ps, .svg, .indd, .pct, .mp4, .avi, .mkv, .3g2, .3gp, .asf, .flv, .m4v, .mov, .mpg, .rm, .srt, .swf, .vob, .wmv, .doc, .docx, .txt, .pdf, .log, .msg, .odt, .pages., .rtf, .tex, .wpd, .wps, .csv, .ged, .key, .pps, .ppt., .pptx, .xml, .json, .xlsx, .xlsm, .xlsb, .xls, .mht, .mhtml, .htm, .html, .xltx, .prn, .dif, .slk, .xlam, .xla, .ods, .docm, .dotx, .dotm, .xps, .ics, .mp3., .aif, .iff, .m3u, .m4a, .mid, .mpa, .wav, .wma, .msi, .php, .apk, .app, .bat, .cgi, .com, .asp, .aspx, .cer, .cfm, .css, .js, .jsp, .rss, .xhtml, .c, .class, .cpp, .cs, .h, .java, .lua, .pl, .py, .sh, .sln, .swift, .vb, .vcxproj, .dem, .gam, .nes, .rom, .sav, .tgz, .zip, .rar, .tar, .7z, .cbr, .deb, .gz, .pkg, .rpm, .zipx, .iso, .ged, .accdb, .db, .dbf, .mdb, .sql, .fnt, .fon, .otf, .ttf, .cfg, .ini, .prf, .bak, .old, .tmp, .torrent

Figure 5: Code snippets showing PyLocky querying system properties (top), and being configured to sleep for a certain time to evade traditional sandbox solutions (bottom)

Encryption routine

PyLocky is configured to encrypt a hardcoded list of file extensions. PyLocky also abuses Windows Management Instrumentation (WMI) to check the properties of the affected system. For its anti-sandbox capability, PyLocky will sleep for 999,999 seconds — or just over 11.5 days — if the affected system's total visible memory size is less than 4GB. The file encryption routine executes if it is greater than or equal to 4GB.

After encryption, PyLocky will establish communication with its command-and-control (C&C) server. PyLocky implements its encryption routines using PyCrypto library – using the 3DES (Triple DES) cipher. PyLocky iterates through each logical drive, first generating a list of files before calling the 'efile' method, which overwrites each file with an encrypted version, then drops the ransom note.

PyLocky's ransom notes are in English, French, Korean, and Italian, which may suggest that it may also target Korean- and Italian-speaking users. It also sends the affected system's information to the C&C server via POST.

Figure 6: Code snippets showing PyLocky's C&C communication (top) and encryption routine (bottom)

Figure 7: PyLocky's ransom notes in different languages

Mitigation and Trend Micro Solutions

PyLocky's evasion techniques and abuse of legitimate tools typically reserved to administrators further exemplify the significance of defense in depth. For instance, machine learning is a valuable cybersecurity tool in detecting unique malware, but it is not a silver bullet. With today's threats, there are different vectors at the attackers' disposal, which makes a multi-layered approach to security important. Apply best practices: regularly back up files, keep the system updated, secure the use of system components, and foster a culture of cybersecurity awareness.

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. It features high-fidelity machine learning to secure the gateway and endpoint data and applications, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen™ protects against today's purpose-built threats that bypass traditional controls, exploit known, unknown, or undisclosed vulnerabilities, and either steal or encrypt personally-identifiable data. Smart, optimized, and connected, XGen™ powers Trend Micro’s suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Indicators of Compromise (IoCs)

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