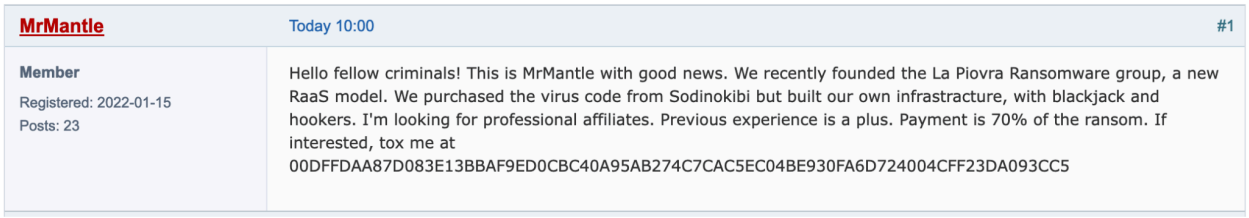
Dissecting La Piovra Ransomware

Executive Brief

The “La Piovra Ransomware” is the new kid on the block, however, it brings nothing new compared to REvil / Sodinokibi ransomware family. Our research shows that this new group potentially bought the original code from the REvil gang, powered up their own backend infrastructure and went to business.

For those of you who don’t know, La Piovra means octopus, and probably this group is inspired from the La Piovra tv show, about the italian mafia. They even have their own soundtrack: https://www.youtube.com/watch?v=wtng11JJaac.

Affiliate Portal: http://wx3djgl4cacl6y4x7r4e4mbqrrub24ectue7ixyix2du25nfowtvfiyd.onion
Extorsion Blog: http://h3txev6jev7rcm6p2qkxn2vctybi4dvochr3inymzgif53n2j2oqviqd.onion
PayPage: http://et22fibzuzfyzgurm35sttm52qbzvdgzy5qhzy46a3gmkrrht3lec5ad.onion
Forum where I saw them advertising their services: http://lk6myerfewzsn5niicgmxsjo7qld2xrrc36lz7yjshpgr54wviqlwvyd.onion/viewtopic.php@id=2177.html



MrMantle	Today 10:00	#1
Member Registered: 2022-01-15 Posts: 23	Hello fellow criminals! This is MrMantle with good news. We recently founded the La Piovra Ransomware group, a new RaaS model. We purchased the virus code from Sodinokibi but built our own infrastracture, with blackjack and hookers. I'm looking for professional affiliates. Previous experience is a plus. Payment is 70% of the ransom. If interested, tox me at 00DFFDAA87D083E13BBAF9ED0CBC40A95AB274C7CAC5EC04BE930FA6D724004CFF23DA093CC5	

The group initially offered tech support over email at “lapiovra.oficial@protonmail.com” but it seems they no longer do that and now they use tox chat, advertising the following ID:

00DFFDAA87D083E13BBAF9ED0CBC40A95AB274C7CAC5EC04BE930FA6D724004CFF23DA093CC5

Technical Analysis

The malware stores encrypted configuration data with RC4 encryption in the .grrr. The name differs among various malware variants:

#	Name	Ratio	Virtual Size	Virtual Address	Physical Size	Offset to Raw Data	Entropy	Flags
1	.text	24%	0x9974	0x1000	0x9A00	0x400	6.58	0x60000020, Cod
2	.rdata	39%	0xF760	0xB000	0xF800	0x9E00	6.45	0x40000040, Initi
3	.data	3%	0x1330	0x1B000	0x1200	0x19600	7.49	0xC0000040, Initi
4	.grrr	32%	0xC800	0x1D000	0xC800	0x1A800	4.37	0xC0000040, Initi
5	.reloc	1%	0x50C	0x2A000	0x600	0x27000	6.05	0x42000040, Initi

sections of the REvil / Sodinokibi payload

The configuration file contains information about which folders, files, and file extensions to exclude from encrypting. It also contains information on which processes to kill, which services to delete, how to escalate privileges with CVE-2018-8453, how to communicate with C2s, and ransom note to display:


```
{"pk":"M4O6efUNv8nZ38UjEZa5t0O4JprZSEOksh1dmd1lC1c=",
"pid":"21",
"sub":"707",
"dbg":false,
"fast":true,
"wipe":false,
"wht":{
    "fld":["windows.old","system volume information","$windows.~ws","google","boot","tor browser","programdata","
        $windows.~bt","program files (x86)","program files","windows","intel","msocache","$recycle.bin","mozilla","
        perflogs","appdata","application data"],

    "fls":["desktop.ini","ntuser.dat","autorun.inf","ntldr","boot.ini","ntuser.ini","iconcache.db","ntuser.dat.log",
        "bootfont.bin","thumbs.db","bootsect.bak"],

    "ext":["rom","ani","cab","mpa","diagpkg","drv","exe","bat","key","shs","idx","msc","wpx","cpl","ps1","nls","
        diagcfg","ics","lnk","cur","sys","com","scr","mod","msi","adv","msstyles","hta","ldf","lock","themepack","
        msu","spl","nomedia","rtp","386","bin","icns","cmd","ocx","diagcab","ico","prf","hlp","theme","msp","dll","
        deskthemepack","icl"]},
"wfld":["backup"],
"prc":["ocomm","excel","dbsnmp","onenote","firefox","xfssvccon","infopath","wordpa","isqlplussvc","dbeng50","mspub",
    "mydesktopqos","ocautoupds","thunderbird","encsvc","outlook","oracle","mydesktopservice","thebat","agntsvc","
    steam","ocssd","sql","tbirdconfig","synctime","visio","sqbcoreservice","winword","msaccess","powerpnt"],
"net":true,
"svc":["backup","mepocs","memtas","veeam","svc$","vss","sophos","sql"],
"exp":false,
```


configuration file for REvil / Sodinokibi

The configuration file for REvil / Sodinokibi.

REvil / Sodinokibi identifies which keyboard languages are configured using GetKeyboardLayoutList. It checks the primary language ID with a switch case. If one of the chosen languages is configured, the malware shuts down. The malware authors do not want to ransom files from the specific set of countries seen in the switch case below.

In this REvil / Sodinokibi variant, a check for Syrian was added, along with new checks for the system language using GetSystemDefaultUILanguage and GetUserDefaultUILanguage:

```
undefined4 __cdecl FUN_00403d32(undefined prim_lang_id)

{
  switch(prim_lang_id) {
  case 0x18:     LANG_ROMANIAN
  case 0x19:     LANG_RUSSIAN
  case 0x22:     LANG_UKRAINIAN
  case 0x23:     LANG_BELARUSIAN
  case 0x25:     LANG_ESTONIAN
  case 0x26:     LANG_LATVIAN
  case 0x27:     LANG_LITHUANIAN
  case 0x28:     LANG_TAJIK
  case 0x29:     LANG_PERSIAN
  case 0x2b:     LANG_ARMENIAN
  case 0x2c:     LANG_AZERI
  case 0x37:     LANG_GEORGIAN
  case 0x3f:     LANG_KAZAK
  case 0x40:     LANG_KYRGYZ
  case 0x42:     LANG_TURKMEN
  case 0x43:     LANG_UZBEK
  case 0x44:     LANG_TATAR
    return 1;    If one of the languages, return True
  default:
    return 0;    Else, return False
  }
}
```

Sodinokibi / REvil switch case for the primary language ID

Once the language checks pass, the malware continues its execution. It deletes shadow copies from the machine with vssadmin.exe to make file recovery more difficult:

```
"C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

Shadow copy deletion with vssadmin.exe.

The ransomware iterates through all folders on the machine, encrypts all files, and drops a ransom note in each folder. Once it has finished encryption, it changes the desktop wallpaper to help inform the user of the attack:

Sodinokibi / REvil new wallpaper after the ransomware encrypts the files

The new wallpaper after the ransomware encrypts the files.

```
------ Welcome. Again. ------

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your computer has extension s8rw9hj520.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities -
nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private
key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/A308E070B855E7B6

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/A308E070B855E7B6

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:
```

The ransom note for the ransomware.

After the malware encrypts the files on the target machine, it tries to establish communication with a C2 server. In order to generate the URL for the C2, it iterates through a list of domains configured in the previously decoded configuration file:

Sodinokibi domain list from the configuration file

```
"dmn":
    "lyricalduniya.com;theboardroomafrica.com;chris-anne.com;ownidentity.com;web865.com;paradigmlandscape.co
    m;envomask.com;scentedlair.com;jlgraphisme.fr;andrealuchesi.it;mursall.de;letterscan.de;metcalfe.ca;dent
    ourage.com;chomiksy.net;yayasanprimaunggul.org;opticahubertruiz.com;affligemsehondenschool.be;zealcon.ae
    ;craftingalegacy.com;jimprattmediations.com;gosouldeep.com;innovationgames-brabant.nl;pisofare.co;coachp
    reneuracademy.com;goodherbalhealth.com;grafikstudio-visuell.de;advance-refle.com;placermonticello.com;am
    elielecompte.wordpress.com;bodet150ans.com;alnectus.com;strauchs-wanderlust.info;khtrx.com;latableacrepe
    s-meaux.fr;precisetemp.com;nicksrock.com;loparnille.se;narca.net;silkeight.com;bescomedical.de;sealgrind
    erpt.com;hospitalitytrainingsolutions.co.uk;fanuli.com.au;augen-praxisklinik-rostock.de;trevi-vl.ru;kira
    ribeaute-nani.com;skoczynski.eu;kellengatton.com;greatofficespaces.net;sytzedevries.com;jayfurnitureco.c
    om;rozmata.com;kenmccallum.com;texanscan.org;landgoedspica.nl;amorbellezaysalud.com;bagaholics.in;a-zpap
```

The domain list from the configuration file.

The malware creates several random URLs using the domains with a combination of hard-coded and randomly generated strings. A recent report by Tesorion covers the similarities in the way REvil / Sodinokibi and GandCrab generate random URLs, which further strengthens suspicions of a potential shared author:

```
aAdmin:                                 ; DATA XREF: create_rand_url+80↑o
                text "UTF-16LE", 'admin',0
aImages:                                ; DATA XREF: create_rand_url+A0↑o
                text "UTF-16LE", 'images',0
                align 4
aPictures:                              ; DATA XREF: create_rand_url+A7↑o
                text "UTF-16LE", 'pictures',0
                align 10h
aImage:                                 ; DATA XREF: create_rand_url+AE↑o
                text "UTF-16LE", 'image',0
aTemp:                                  ; DATA XREF: create_rand_url+B5↑o
                text "UTF-16LE", 'temp',0
                align 4
aTmp:                                   ; DATA XREF: create_rand_url+BC↑o
                text "UTF-16LE", 'tmp',0
aGraphic:                               ; DATA XREF: create_rand_url+C3↑o
                text "UTF-16LE", 'graphic',0
aAssets:                                ; DATA XREF: create_rand_url+CA↑o
                text "UTF-16LE", 'assets',0
                align 10h
aPics:                                  ; DATA XREF: create_rand_url+D1↑o
                text "UTF-16LE", 'pics',0
                align 4
aGame:                                  ; DATA XREF: create_rand_url+D8↑o
                text "UTF-16LE", 'game',0
                align 4
```

The hard-coded strings for random URL generation.

Once the URLs are generated, the malware sends encrypted machine information to each of the domains including usernames, machine name, domain name, machine language, operating system type, and CPU architecture:

Address	UNICODE
01CFE430	{"ver":256,"pid":"10","sub":"7","pk":"GadtWz2QBTacskL+55Wpo65Ikw
01CFE4B0	Y28qJOxHoe4Xte81M=","uid":"A308E070B855E7B6","sk":"llRpuwUdZa4pf
01CFE530	1KE6Mb3SOzxm32avoz7KIhvscS+KhzquTdHswJtebU5pQBqseS2EnpmEQgIzuPY6
01CFE5B0	S+NUatHsPVB72YARMQyMr+UT7xMLTfVXkWXHx7n5w==","unm":"Malware","ne
01CFE630	t":"MALWARE-PC","grp":"WORKGROUP","lng":"he-IL","bro":false,"os"
01CFE6B0	:"Windows 7 Ultimate","bit":64,"dsk":"QwADAAAAAPCf+RMAAAAAMAwrCg
01CFE730	AAAA=="}....

The data sent to the C2 server before encryption.

When the user clicks on the ransom note and enters the key, a page appears that lists the price they must pay in bitcoin to retrieve their files:

CONCLUSION

In this blog, we took a deep dive into the REvil / Sodinokibi ransomware infection process, and showed that even though the obfuscation techniques used by the ransomware authors are quite simple, they are still proving to be very effective in bypassing most antivirus vendors.

Our analysis further supports the suspicion that the threat actors behind the REvil / Sodinokibi ransomware are the same allegedly retired authors who created the GandCrab ransomware, based on findings detailed in this report, such as: similarities in the language and countries whitelist (Russian-speaking countries and even Syrian Arabic), the “revengeful” targeting of an Ahnlab product for process injection, and the similarities in the URL-generation routine.

Since April 2019, the REvil / Sodinokibi ransomware has become very prolific and has become the 4th most common ransomware within less than 4 months after its first appearance. It has since gone through several minor updates, and it is our assessment that its industrious authors will continue to develop the ransomware, adding more features and improving its evasive capabilities.