2016 年 10 月 13 日，星期四

LockyDump - 我们掌握所有配置信息

作者：Warren Mercer 和 Matthew Molyett

摘要

自从在 2016 年 2 月出现以来，Locky 不断演变。由于该恶意软件本身具有的一些特征以及散布方式不断改变，跟踪它有时变得非常困难。负责 Locky 的人员着眼于跟踪使用该勒索软件的联属机构，尝试不断改善运营安全 (OPSEC)。本文介绍 Talos 发布的一个新 Locky 配置提取程序，名为“LockyDump”。这是首个可转储目前已知的所有 Locky 变体（例如基于 .locky、.zepto 和 .odin 的勒索软件）使用的配置参数的开源工具。

利用 LockyDump，您可以在虚拟环境中运行已知的 Locky 样本，从而提取和提供该样本的所有配置信息，包括与该样本相关联的 AffilID。Locky 的最新变体让此提取过程变得越来越难以完成。此配置提取过程发生变化后，Talos 希望能够通过反向处理更多 Locky 样本，尝试获取所有重要 AffilID 信息。获取每个样本的联属信息后，能够实现跟踪 Locky 联属的历史信息，从而确定每个联属的趋势和其他特征，比如确定首选的主要散播方式（例如通过使用漏洞攻击包 [EK] 或通过垃圾邮件/网络钓鱼邮件）。

配置提取详细信息

Talos 制作了一个适用于 Locky 的配置提取工具（支持 Locky 现有的所有版本，即 Zepto/Odin）。利用该工具，您可以提取硬编码到恶意二进制文件中的以下配置参数。

affilID	在 Locky 二进制文件中指定的联属 ID。我们观察到的值有 1、3、4、5、8、D、E、F、13、15
dga_seed	由各版本 Locky 使用，依靠域生成算法 (DGA) 实现命令与控制 (C2) 通信的种子值。
persist_svhost	“0” 或 “1” 标志设置，用于实现另存为操作和运行 %temp%\svchost.exe。
persist_registry	“0” 或 “1” 标志设置，用于通过受害计算机注册表中的 run 项获得持久性。
ignore_russian	“0” 或 “1” 标志设置，用于使用俄语语言包在系统上终止执行。
callback_path	其中包含 Locky 向 C2 服务器回发 HTTP POST 请求所用的 URL 路径。该值在 Locky 演变过程中改变过多次，之前曾包含过 /asache_handler.php 和 /data/info.php 等路径。
C2_servers	Locky 样本获取 DGA 信息所用的 C2 服务器的硬编码 IP。
rsa_key_id	在加密过程中使用的 RSA 秘钥 ID。
rsa_bits	在加密过程中使用的 RSA 秘钥大小。
rsa_exponent	RSA 在加密过程中使用的质数。
ransom	二进制文件在成功感染系统后显示的勒索信。
onion_addr	指示用户按恶意软件要求支付勒索金额的付费网关地址。这些地址位于 Tor 网络上。

LOCKYDUMP 要求

LockyDump 是 PE32 Windows 二进制应用，用于提取 Locky 系列恶意软件中嵌入的配置。恶意软件必须执行，LockyDump 才能从内存中提取这些值。分析环境因此被限制为 Windows 系统且应能受到 Locky 危害。

LOCKYDUMP 过程方法

Locky 以 Win32 可执行文件和 DLL 形式散播。因此，我们制作的 LockyDump 利用两种单独的分析方法。DLL 文件开头使用 LoadLibrary 启用脱壳程序，从而显示 Locky 代码并让初始化代码解密配置。配置解密后，LockyDump 会找到解密的配置并将其打印到标准输出。

以 EXE 文件形式提供的 Locky 版本需要使用不同的分析方法，其实现形式是通过配置为用于调试的 LockyDump 执行恶意软件。LockyDump 在检测到真正的代码之前允许恶意软件运行，并在检测到真正的代码之时冻结恶意软件。然后，LockyDump 找到配置信息并将其打印到标准输出。

可选功能：

通过启用下列可选功能，在运行 LockyDump 时可以从 Locky 样本中提取更多信息。这些可选功能使用 Windows 环境变量配置，您可以在执行 LockyDump 之前设置：

set LOCKY_DUMP_VERBOSE=1

set LOCKY_DUMP_SAVE=1

详细输出 - Locky 配置包含两个模板：一个用于勒索信图像，一个用于勒索信 HTML。默认情况下，LockyDump 不会打印这些字段，因为这会显著增加输出的大小。如果存在环境变量 LOCKY_DUMP_VERBOSE，两个勒索模板都会打印到标准输出。

Locky 脱壳 - Locky 二进制文件受多种加壳程序保护，这让静态分析变得难以进行。设置环境变量 LOCKY_DUMP_SAVE 后，已脱壳的 Locky 文件会在当前工作目录中被另存为 DUMPED_IMAGE.DLL。该进程文件将始终为“DUMPED_IMAGE.DLL”。

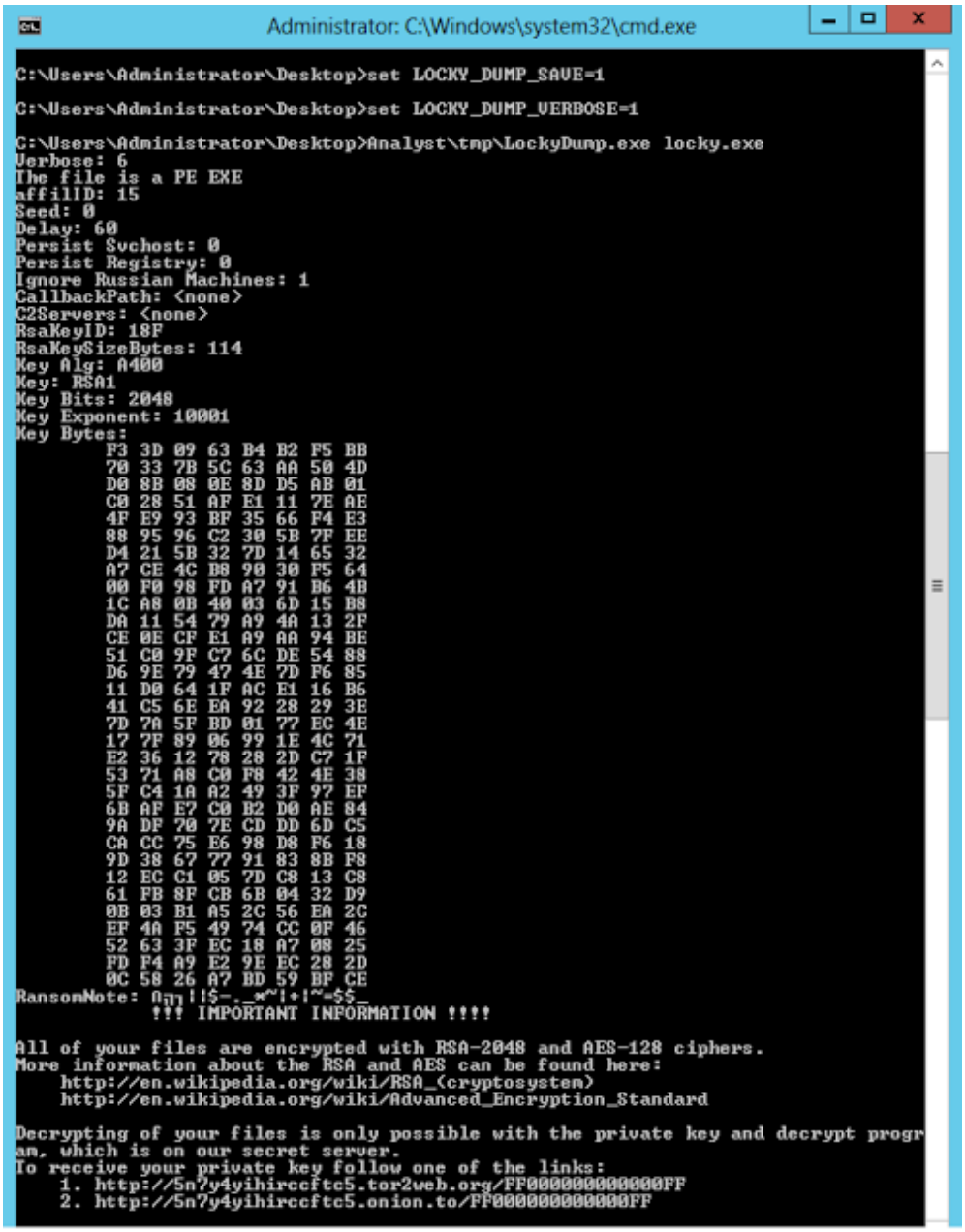
执行说明

利用 LockyDump，用户可以创建 Microsoft Windows 虚拟实例，在其中置入已知 Locky 样本，然后针对该样本运行 LockyDump。强烈建议使用虚拟环境，因为 LockyDump 需要执行 Locky 才能从内存中提取配置信息。

通过命令行执行 LockyDump 所用的语法如下：

LockyDump.exe sample.exe [样本参数]

该命令将针对您指定的样本运行 LockyDump。通过用“set”命令配置本地环境变量，可以设置上文介绍的可选功能。根据需要设置任意可选功能后，只需照常运行 LockyDump 即可



源代码

可从我们的 GitHub 上获取 LockyDump 源代码。为方便用户使用，我们既提供源代码，也提供编译的二进制文件。

LockyDump.10122016.exe SHA256：
d49fd9fb7d290a530c292f451c32e558f6f5797944ecb2d6b73e151f450fc43c

请在执行前验证散列。

总结

Talos 在开源社区中发布此工具是为了方便其他研究人员自行对 Locky 做历史分析。Fortinet Virus Bulletin 会议上的信息足以展示我们向其他人发布此工具的必要性，因为尚不清楚 Fortinet 配置提取工具是否会公开。

根据我们在过去一周的观察，基于垃圾邮件的 Locky 传播大幅下降，该工具正是在这个时机发布。请注意，Locky 会不断演变，它迟早会通过其他配置方法卷土重来，这可能会致使该工具失效。在这种情况下，我们会努力发布更新版本，让该工具能继续使用并发挥预期的作用。

发布者：WARREN MERCER；发布时间：11:07
标签：配置提取程序、LOCKY、恶意软件、ODIN、开源、勒索软件、TALOS、ZEPTO