后门 FCKQ(CTB-Locker)的兴起

非官方中文译文·安天技术公益翻译组 译注

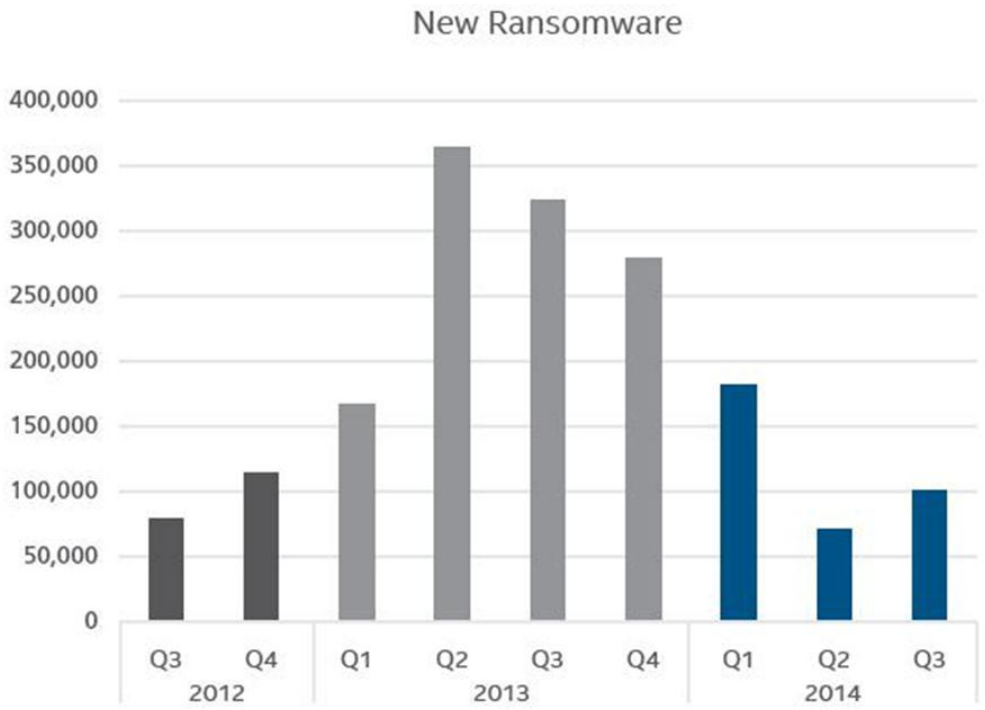
文档信息			
原文名称	The Rise of Backdoor-FCKQ (CTB-Locker)		
原文作者	Raj Samani	**原文发布日期**	2015 年 1 月 21 日
作者简介	Raj Samani 是迈克菲的副总裁和 EMEA 首席技术官。 uk.linkedin.com/pub/raj-samani/0/7b9/369 Christiaan Beek 是迈克菲实验室的威胁情报总监，其研究方向包括事件响应、逆向工程恶意软件、数字取证等。 www.linkedin.com/in/christiaanbeek		
原文发布单位	迈克菲实验室		
原文出处	https://blogs.mcafee.com/mcafee-labs/rise-backdoor-fckq-ctb-locker		
译者	安天技术公益翻译组	**校对者**	安天技术公益分析组
免责声明	本译文为安天实验室针对网络资料翻译而成，并未取得原作者授权，仅供内部学习和交流使用，安天实验室不对任何可能因此导致的版权问题承担责任。		

后门 FCKQ(CTB-Locker)的兴起

Raj Samani (@Raj_Samani) ， Christiaan Beek (@ChristiaanBeek)

2015 年 1 月 21 日

在迈克菲实验室 2014 年 11 月发布的报告中，高级副总裁 Vincent Weafer 指出 2014 年会作为“信用动荡年”被大家铭记。事实上，每一种威胁在第三季度都有明显增加，这也是对 2015 年的预兆。但也有例外：勒索软件。



上图反应了勒索软件威胁的减少，但是如迈克菲实验室的威胁预测指出：勒索软件的传播、加密及目标搜索的方法将会不断进化。

对大多数人来说 ,后门 FCKQ (也就是 CTB-Locker)的出现使得这一预言听起来真实可靠。后门 FCKQ 是通过诸如 IRC、点对点网络、新闻组检索、垃圾邮件等多途径传播的。

细节

“后门-FCKQ”是一种新型加密恶意软件，通过电子邮件传播，旨在加密目标系统

中的文件。

它自我复制到以下文件：

%temp%< 7 random characters>.exe

%temp%\wkqifwe.exe

它也可以创建包含 7 个随机字符的工作任务：

%windir%\Tasks\cderkbm.job

它将以下注册表值添加到系统中：

%ALLUSERSPROFILE%\Application Data\Microsoft\<7 random characters>

它向 svchost.exe 注入代码，svchost.exe 会从以下目录启动文件：

%temp%\<7 random characters>.exe

注入 svchost.exe 的代码会用以下拓展名加密文件：

.pdf

.xls

.ppt

.txt

.py

.wb2

.jpg

.odb

.dbf

.md

.js

.pl

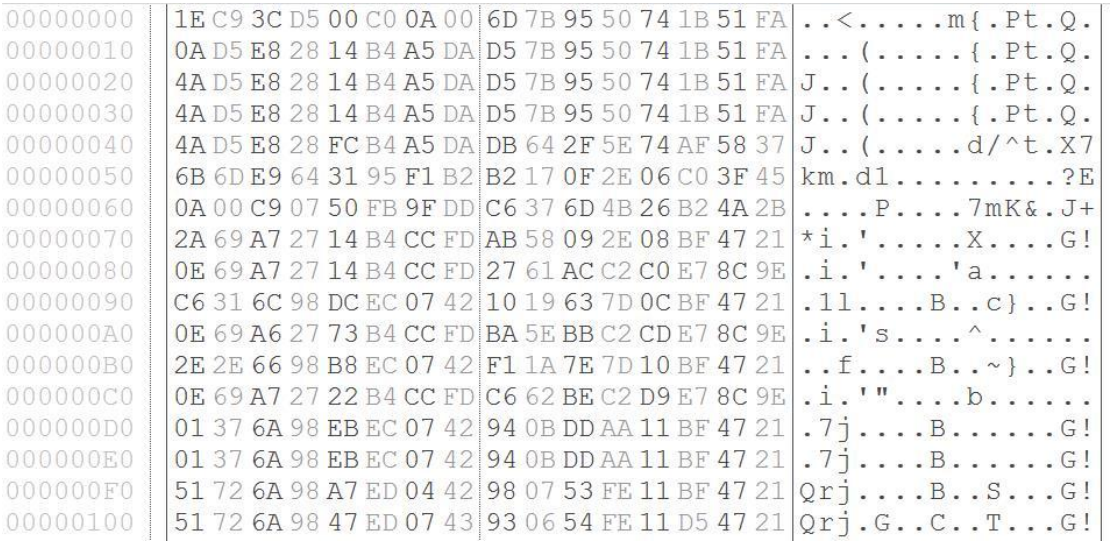
一旦被感染，该恶意软件就会在系统上显示如下图片：

新创建的进程会创建一个互斥体，名为：

\BaseNamedObjects\lyhrsugiwwnvnn

新一轮后门 FCKQ 的有趣之处是它使用了众所周知的下载器 Dalexis。这种下载器有几个版本，在内部数据库中进行简单搜索就会出现 900 多个该下载器及其变种的结果。为了绕过反反垃圾邮件工具，该下载器隐藏于一个 zip 文件中，最后解压为.scr （屏幕保护）文件。

该下载器的功能就是从特定位置下载其他的恶意软件，解压 Xor 编码的恶意代码并运行。这种情况下，下载的真正 CTB'恶意软件被打包在一个名为'pack.tar.gz'的文件中。

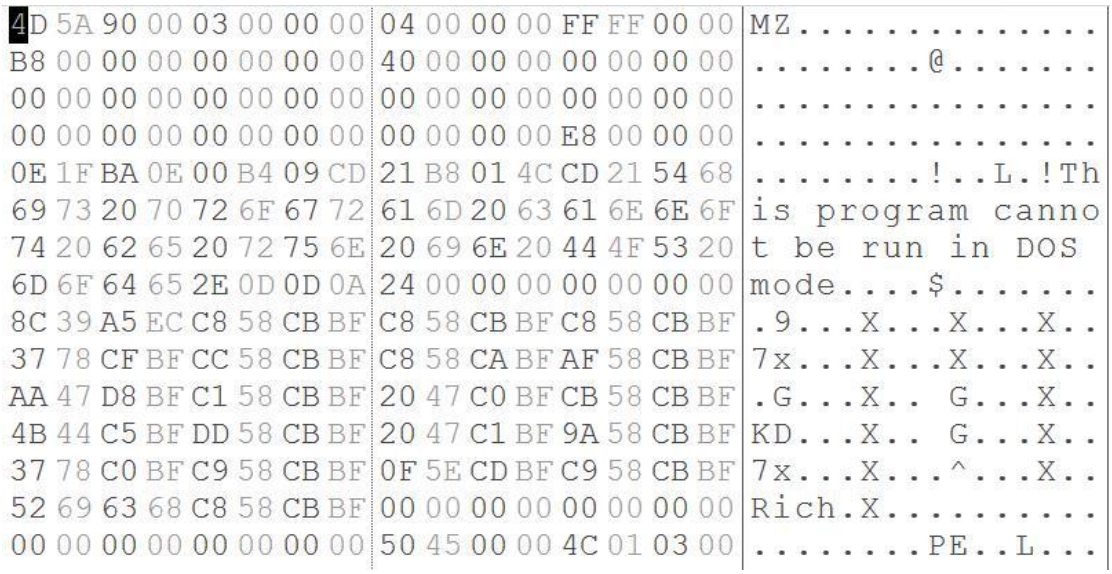


```
00000000 | 1E C9 3C D5 00 C0 0A 00 | 6D 7B 95 50 74 1B 51 FA | ..<.....m{.Pt.Q.
00000010 | 0A D5 E8 28 14 B4 A5 DA | D5 7B 95 50 74 1B 51 FA | ...(.....{.Pt.Q.
00000020 | 4A D5 E8 28 14 B4 A5 DA | D5 7B 95 50 74 1B 51 FA | J..(.....{.Pt.Q.
00000030 | 4A D5 E8 28 14 B4 A5 DA | D5 7B 95 50 74 1B 51 FA | J..(.....{.Pt.Q.
00000040 | 4A D5 E8 28 FC B4 A5 DA | DB 64 2F 5E 74 AF 58 37 | J..(.....d/^t.X7
00000050 | 6B 6D E9 64 31 95 F1 B2 | B2 17 0F 2E 06 C0 3F 45 | km.d1.........?E
00000060 | 0A 00 C9 07 50 FB 9F DD | C6 37 6D 4B 26 B2 4A 2B | ....P....7mK&.J+
00000070 | 2A 69 A7 27 14 B4 CC FD | AB 58 09 2E 08 BF 47 21 | *i.'.....X....G!
00000080 | 0E 69 A7 27 14 B4 CC FD | 27 61 AC C2 C0 E7 8C 9E | .i.'....'a......
00000090 | C6 31 6C 98 DC EC 07 42 | 10 19 63 7D 0C BF 47 21 | .1l....B..c}..G!
000000A0 | 0E 69 A6 27 73 B4 CC FD | BA 5E BB C2 CD E7 8C 9E | .i.'s....^......
000000B0 | 2E 2E 66 98 B8 EC 07 42 | F1 1A 7E 7D 10 BF 47 21 | ..f....B..~}..G!
000000C0 | 0E 69 A7 27 22 B4 CC FD | C6 62 BE C2 D9 E7 8C 9E | .i.'"....b......
000000D0 | 01 37 6A 98 EB EC 07 42 | 94 0B DD AA 11 BF 47 21 | .7j....B......G!
000000E0 | 01 37 6A 98 EB EC 07 42 | 94 0B DD AA 11 BF 47 21 | .7j....B......G!
000000F0 | 51 72 6A 98 A7 ED 04 42 | 98 07 53 FE 11 BF 47 21 | Qrj....B..S...G!
00000100 | 51 72 6A 98 47 ED 07 43 | 93 06 54 FE 11 D5 47 21 | Qrj.G..C..T...G!
```

图 1： ‘pack.tar.gz’

如上述截图所示，并不存在代表已知文件类型的文件标头。例如，如果这是一个可执行文件，前两个字符（即魔数）就应该是 “MZ”。这便是恶意软件编写者试图规避恶意软件网关检测的方法之一。最近，我们看到多次的伎俩就是将恶意软件的有效负载荷置于 Pastebin 或 Github 上。

在这种情况下，‘pack.tar.gz’ 文件用不同的 XOR 密钥来加密部分文件，一旦破解了这个谜团，后门 FCKQ 的解压代码就呈现出来了。



```
4D 5A 90 00 03 00 00 00 | 04 00 00 00 FF FF 00 00 | MZ..............
B8 00 00 00 00 00 00 00 | 40 00 00 00 00 00 00 00 | ........@.......
00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | ................
00 00 00 00 00 00 00 00 | 00 00 00 00 E8 00 00 00 | ................
0E 1F BA 0E 00 B4 09 CD | 21 B8 01 4C CD 21 54 68 | ........!..L.!Th
69 73 20 70 72 6F 67 72 | 61 6D 20 63 61 6E 6E 6F | is program canno
74 20 62 65 20 72 75 6E | 20 69 6E 20 44 4F 53 20 | t be run in DOS
6D 6F 64 65 2E 0D 0D 0A | 24 00 00 00 00 00 00 00 | mode....$.......
8C 39 A5 EC C8 58 CB BF | C8 58 CB BF C8 58 CB BF | .9...X...X...X..
37 78 CF BF CC 58 CB BF | C8 58 CA BF AF 58 CB BF | 7x...X...X...X..
AA 47 D8 BF C1 58 CB BF | 20 47 C0 BF CB 58 CB BF | .G...X.. G...X..
4B 44 C5 BF DD 58 CB BF | 20 47 C1 BF 9A 58 CB BF | KD...X.. G...X..
37 78 C0 BF C9 58 CB BF | 0F 5E CD BF C9 58 CB BF | 7x...X...^...X..
52 69 63 68 C8 58 CB BF | 00 00 00 00 00 00 00 00 | Rich.X..........
00 00 00 00 00 00 00 00 | 50 45 00 00 4C 01 03 00 | ........PE..L...
```

图 2：后门-FCKQ 的解压代码

有大量后门-FCKQ（CTB-Locker）的样本作为对比资料，我们能够迅速识别各个代码部分。

快速的 Yara 检测规则，如下所示：

```
rule Backdoor-FCKQ : CTB_Locker,Ransomware

{
meta:
author = "ISG"
date = "2015-01-20"
description = "CTB_Locker"

strings:
$string0 =
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA"
$string1 =
"RNDBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA"
$string2 = "kernel32.DLL"
$string3 = "klospad.pdb"

condition:
3 of them
}
```

比特币踪迹

当追踪比特币的踪迹及可能发生的交易时，账户上没有发现任何价值，也没有与其他账户的交易。

清除

所有用户：使用当前的“引擎和 DAT 文件”进行检测和清除。

如果使用推荐的引擎和 DAT 文件（或更高版本的），就可以成功清除为了挂钩系统启动而做出的系统注册表及/或 INI 文件修改。

特别感谢 Sanchit Karve 先生的分析援助。