登录

Linux勒索样本KillDisk分析报告

熊猫正正 / 2017-01-10 05:08:00 / 浏览数 7074 技术文章 技术文章 顶(0) 踩(0)

一、起因

在逛bleepingcomputer时，发现一个有趣的文章，链接：[https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-bo

顿时又勾起了我分析样本的欲望，其实很早之前我就分析过多款勒索类的软件，但都是基于window/Android等平台的，也接触过osx的一款开源勒索软件，对于Linux平台的

，样本是由ESET发现的，上面提供了样本的HASH值:8F43BDF6C2F926C160A65CBCDD4C4738A3745C0C，google搜了一大圈，没有找到下载链接，好可惜，于是在自

二、样本简介

KillDisk是一款之前比较有名的恶意软件，是由BlackEnergy组织攻击乌克兰电网以及新闻银行等系统的恶意软件，有要用于清除系统扇区，删除重要的系统文件，对特定类型

三、详细分析

首先查看文件类型，如下：

从图中我们可以得知，此样本为linux64位可执行程序，通过ida反编译程序，发现程序未加密，未加壳，main函数如下：

动态跟踪到main函数，如下所示：

样本首先为利用daemon函数创建一个单独的Linux守护进程执行恶意代码，参数为0,0，如下所示：

 动态调试main函数，创建daemon守护进程如下：

创建完守护进程之后，然后通过print_bnr修改Linux的grub项，导致系统bootloader启动发生异常，如下所示：

动态跟踪到print_bnr函数之后，如下所示：

函数拼接相应的字符串，做为grub启动项菜单显示，拼接字符串过程如下：

然后判断系统目录下的/etc/default/grub启动项文件是否存在，如果存在，则修改/boot/grub/menu.lst文件或者修改/boot/loader.rc配置文件（主要是为了兼容一些老的

然后遍历/etc/grub.d目录，将不是40_custom的文件全部删除，因为修改了grub启动项，需要执行update-grub命令，如下所示：

现在勒索样本已经成功修改了Linux系统的grub启动项，当系统重启之后，bootloader会显示我们刚刚写入的字符串菜单项，如下所示：

完成了grub的改写之后，后面的主要工作就是加密系统各个目录下的文件了，具体通过如下两个函数进行完成，加密工作完成之后，重启操作系统，进行勒索，如下所示：

 第一个加密函数，会对如下11个目录的文件进行加密，目录列表如下：

```
/boot
  /bin
  /sbin
  /lib/security
  /lib64/security
  /usr/local/etc
  /etc
  /mnt
  /share
  /media
  /home
```

第二个加密函数，会对如下5个目录的文件进行加密，目录列表如下：

```
/usr
  /tmp
  /opt
  /var
  /root
```

 由于两次使用的加密函数都是一样的，我们下面重点分析一下，它的加密过程，以及运用了哪些加密算法，加密函数如下：

 跟踪进入到bypass_dir函数，如下所示：

动态跟踪入进加密函数，加密/boot目录的文件，如下所示：

这个就和window上的目录遍历差不多了，当遍历到grub启动项文件时，则跳过，如果不是启动文件进调用crypt_file函数进行加密，crypt_file函数如下所示：

加密函数首先通过gen_key函数，生成三个密钥key,gen_key函数如下所示：

从代码可以看出，生成的三个密钥，对于每个文件来说都是随机生成的，然后对每个文件内容分成文件块加密，每个文件块的大小为4096字节，加密函数分别为crypt_all,cr

通过分析my_ecb_crypt函数，我们可以得知，使用的加密算法为三重DES加密算法，三个密钥都是之前随机生成的，如下所示：

加密完成之后，可以看到所有的文件都已经被加密了，如下所示：

从上面的分析可以得出，勒索软件使用了三重DES加密算法，且对应的每个文件都是按照4096大小的文件块进行加密，文件加密密钥都是随机生成的，因此根本无法解密文

四、总结

好了，样本分析完了，再说说自己对勒索类样本的一点个人看法和经验，最近几年勒索软件是越来越流行，各大安全公司也在积极应对，同时随着各种物联网设备的兴起，可
FBI勒索样本之后，我又自己实现了一遍源代码，还蛮好玩的，这一两年各大安全公司都在花式炫耀自己捕获的各种平台下的勒索软件，如Maktub,Locker,Petya,Locky,Nan
Locker,Chimera,PowerWare,Tesalcrypt,Linux.Encoder.1等以及它们的变种，其实这些勒索样本都还比较容易实现，技术手段也都不太高明，从PC平台端的勒索从简单的加
下面给大家介绍几款开源的勒索软件，供大家参考研学习： https://github.com/eyecatchup/Critroni-php
https://github.com/PanagiotisDrakatos/JavaRansomware
https://github.com/NTNUCIC/ransomware
https://github.com/Monkey-D-Groot/Ransomware
https://github.com/gdbinit/gopher
https://github.com/NullArray/Cypher
https://github.com/qnighy/ransomware-demo
https://github.com/alextspy/Ransomware
https://github.com/CHRISTOPHERDIEHL/Ransomware
https://github.com/ultra723/ransomware
https://github.com/tfairane/AndroMalware
https://github.com/AlphaDelta/DUMB
https://github.com/mymortal/Ransomware
https://github.com/brucecio9999/CryptoWire-Advanced-AutoIt-ransomware-Project
https://github.com/lucdew/goransomware
https://github.com/zongyuwu/RansomRB
https://github.com/SadFud/GG-Ransomware
https://github.com/marcosValle/RansPy

从上面的开源代码可以看出，勒索类的软件已经运作在了各个平台，以及可以使用各种不同的语言进行编写:C/C++,Java,JavaScript,Python,Go,C#,VB.Net,PHP,Ruby等，随

五、样本的发展趋势预测

KillDisk是由一个叫[TeleBots]的团队开发的，该团队也开发了同名的后门木马，并为2016年破坏乌克兰公司【电力系统，银行系统】的网络攻击负责。除此之外，乌克兰银

可以得出KillDisk之前是[TeleBots]团队开发的专门针对乌克兰的网络攻击样本，在2017/01/05，ESET才捕抓到一个
KillDisk的样本，具体的染感量未知，这款变种样本应该也是[TeleBots]团队开发的，由于样本刚刚出来就被ESET捕获到了，新本较新，暂未对影响量以及传播渠道进行批漏

能过微步在线平台查找Hash值，上面显示样本发现时间为：2017/01/05,相关的IOC列表如下：

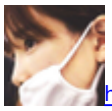
```
26633a02c56ea0df49d35aa98f0fb538335f071c
    84a2959b0ab36e1f4e3abd61f378dc554684c9fc
    8f43bdf6c2f926c160a65cbcdd4c4738a3745c0c
    95fc35948e0ce9171dfb0e972add2b5d03dc6938
    92fe49f6a758492363215a58d62df701afb63f66
    b2e566c3ce8da3c6d9b4dc2811d5d08729dc2900
    2379a29b4c137afb7c0fd80a58020f5e09716437
    25074a17f5544b6f70ba3e66ab9b08adf2702d41
```

（由于ESET并未对样本的捕获来源以及样本的感染进行过多的详细说明，以上纯属个人想法，有不对的地方，请大牛多多指教，欢迎交流）

六、参考

https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/
http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/
https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/
http://www.linuxidc.com/Linux/2017-01/139254.htm
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
https://x.threatbook.cn/
http://blog.nsfocus.net/analysis-ukrenergo-blackout-event-ukraine/

1. 7 条回复


hades 2017-01-10 06:33:19

少点传播渠道、影响范围这方面的分析，主要内容都主要是对木马逆向分析

0 回复Ta


笑然 2017-01-10 09:28:00

首篇通过审核的勒索软件文章，四倍奖励妥妥的！

0 回复Ta


r4bb1t_ 2017-01-10 10:17:17

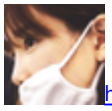
文件加密密钥都是随机生成的根本没办法解这真心不道德，这篇质量可以，同时希望进行相关研究的大佬们也多投稿交流呀：)

0 回复Ta


hades 2017-01-10 13:25:03

哈哈 马爸爸不差钱。。

0 回复Ta


hades 2017-01-11 02:35:14

主要是样本数量没有途径。。

0 回复Ta


熊猫正正 2017-01-11 03:38:07

引用第5楼hades于2017-01-11 10:35发表的 回 3楼(r4bb1t_) 的帖子：
主要是样本数量没有途径。。 [url=https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=632&pid=1264][/url]

是的，主要是样本是ESET在1月5号第一手发现的，他们也没公布他们的捕获来源，以及感染数量，估计现在还没有大面积应用到Linux服务器攻击中，不过针对Linux/Io

0 回复Ta


helloworld 2017-01-13 09:38:38

看来勒索软件要爆发了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板