Ransomware和启动过程

时间	作者	等级	Rank
2017-02-06 18:47:21	captain (/profile/1/)	低危	2

mbr勒索软件哟

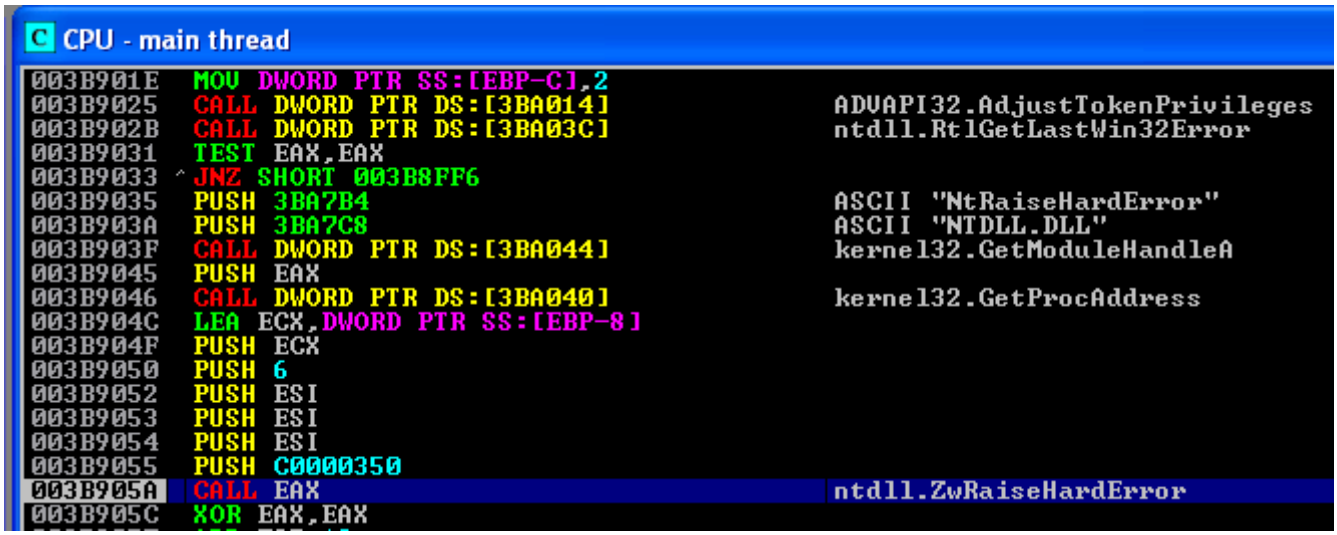
自从它在2016年初发现以来，我们跟踪了一些变种的Petya，一个勒索软件的多阶段加密，不仅锁定您的计算机，而且覆盖主引导记录。 在这个博客中，我们将更深入地了解它的更复杂的第二阶段的攻击。

Petya使用其引导代码和一个小内核代码覆盖主引导记录（MBR）及其相邻扇区。 MBR包含主引导代码，分区表和有关给定计算机系统的主盘的其他相关信息。

当您启动感染了Petya的计算机时，您会看到一个闪烁的颅骨ASCII图片。 有一些Petya的变化，通常基于所示的头骨的不同颜色来识别。 在原始版本中，头骨是红色的，而在一些变体中它是绿色的。

初始化

在初始阶段，Petya作为常规恶意软件到达，并尝试用其代码覆盖MBR和其他扇区。 然后使用NtRaiseHardError API触发重新启动以执行第二阶段，如图1所示。



我们不打算讨论Petya在这个博客的初始阶段，但是，因为有很多文章已经写了。 相反，我们将从调试器中仔细看看它的实际启动代码。

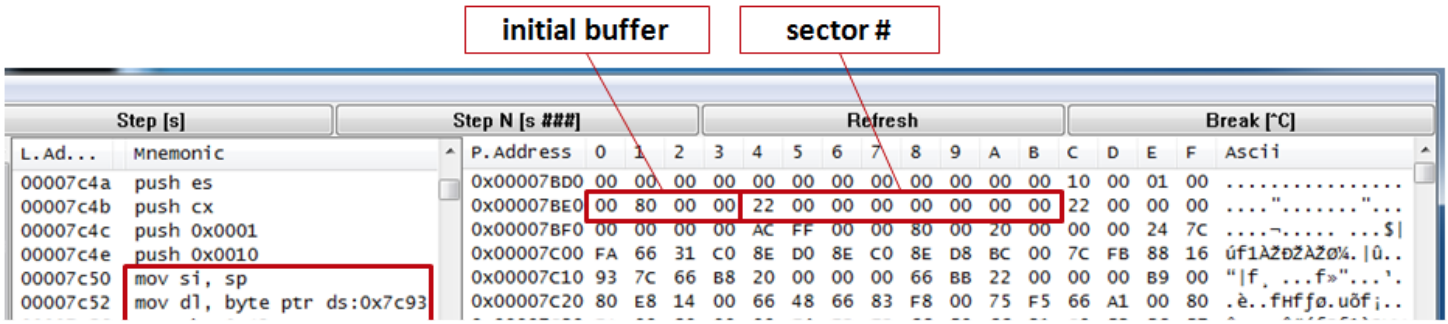
第二阶段

一旦在初始攻击阶段触发重新启动，Petya会显示一个假的CHKDSK，它实际上是加密例程的一部分。 在对相邻扇区的其余部分进行加密时，屏幕显示一个假计表，显示正在检查的磁盘的百分比。 之后，它会显示一个闪烁的ASCII头骨图片（我们的示例是红色的，表明它是原始变体之一。）

在调试器中启动代码

让我们通过将它加载到调试器中来仔细看看第二个阶段。 在调试器中分析被感染的MBR不容易，但它是可能的。 一旦被感染的MBR被加载，Petya将0x20扇区的恶意软件代码复制到内存位置，从0x8000开始，只是离开始启动代码几百个字节。

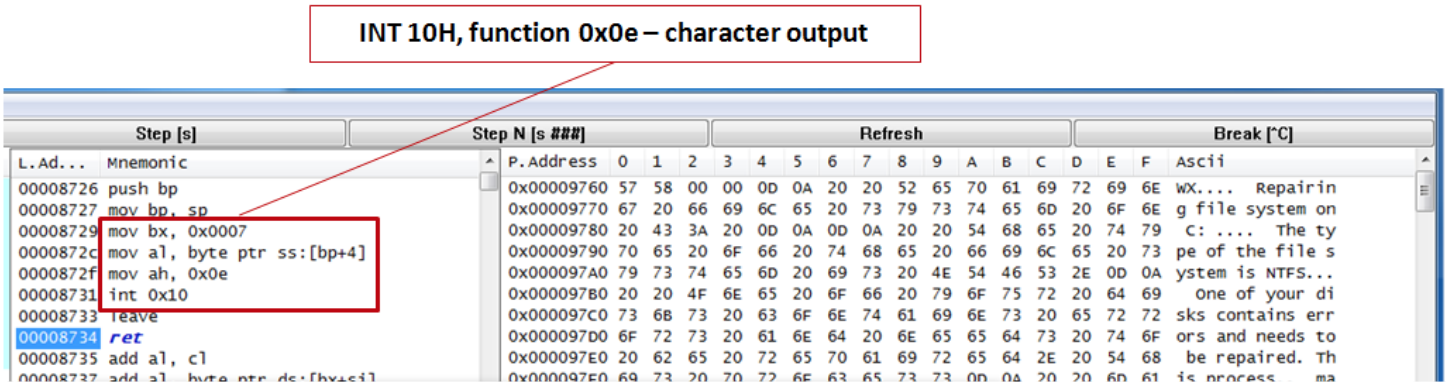
在引导过程中，计算机尚不知道要加载哪个操作系统。 因此，目前没有Windows API可用。 恶意软件依赖于原始INT 13H。 恶意软件使用它来执行其基本功能，例如将扇区（功能0x42，INT 13H）读取到不同的存储器位置。 下面的图2示出了用于读取扇区的指令以及磁盘地址分组（DAP）的结构.DAP包含用于传送扇区的内容的缓冲器的地址，以及要被传送的扇区读。



假CHKDSK

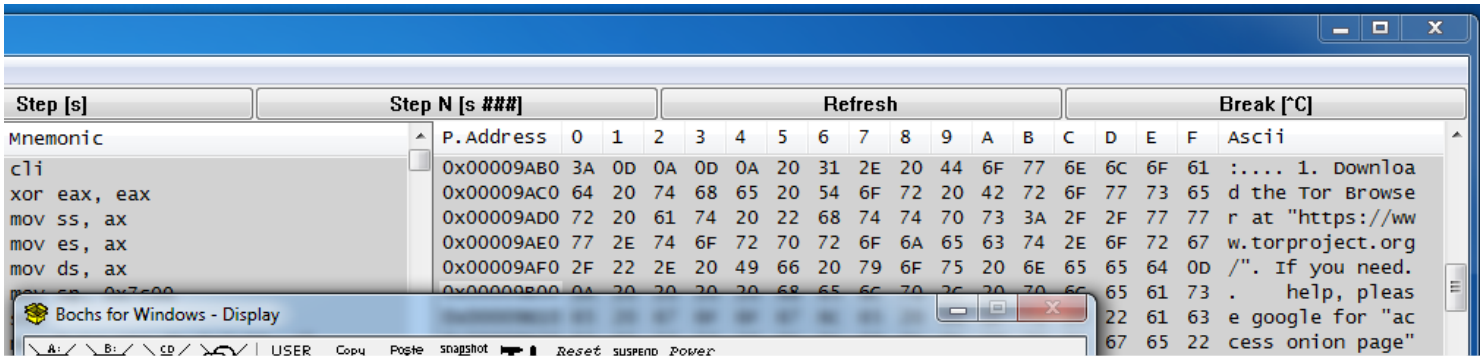
读取启动代码后，将显示假的CHKDSK，随后是加密过程。

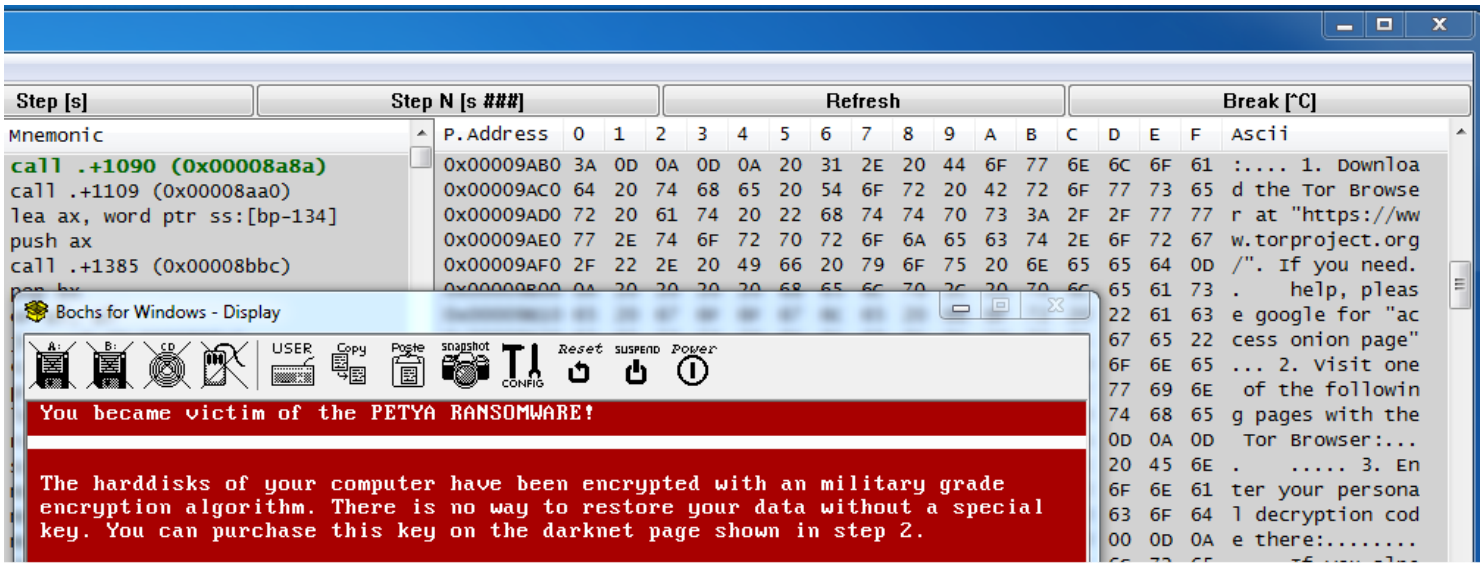
伪CHKDSK显示的初始警告消息使用另一个INT 10H（功能0x0E）逐个字符打印，如图3所示。



红色头骨

一旦加密过程完成，恶意软件触发另一个引导加载程序，此时显示红色头骨（见图4）。 从那时起，每次重新启动受感染的机器时，都会显示红色头骨，按任意键将显示警告和付款提示（参见图5）


Step [s]
Step N [s ###]
Refresh
Break [^C]
Mnemonic
cli
xor eax, eax
mov ss, ax
mov es, ax
mov ds, ax
P.Address 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii
0x00009AB0 3A 0D 0A 0D 0A 20 31 2E 20 44 6F 77 6E 6C 6F 61 :.... 1. Downloa
0x00009AC0 64 20 74 68 65 20 54 6F 72 20 42 72 6F 77 73 65 d the Tor Browse
0x00009AD0 72 20 61 74 20 22 68 74 74 70 73 3A 2F 2F 77 77 r at "https://ww
0x00009AE0 77 2E 74 6F 72 70 72 6F 6A 65 63 74 2E 6F 72 67 w.torproject.org
0x00009AF0 2F 22 2E 20 49 66 20 79 6F 75 20 6E 65 65 64 0D /". If you need.
Bochs for Windows - Display
USER Copy Paste snapshot Reset suspend Power


Step [s]
Step N [s ###]
Refresh
Break [^C]
Mnemonic
call .+1090 (0x00008a8a)
call .+1109 (0x00008aa0)
lea ax, word ptr ss:[bp-134]
push ax
call .+1385 (0x00008bbc)
P.Address 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii
0x00009AB0 3A 0D 0A 0D 0A 20 31 2E 20 44 6F 77 6E 6C 6F 61 :.... 1. Downloa
0x00009AC0 64 20 74 68 65 20 54 6F 72 20 42 72 6F 77 73 65 d the Tor Browse
0x00009AD0 72 20 61 74 20 22 68 74 74 70 73 3A 2F 2F 77 77 r at "https://ww
0x00009AE0 77 2E 74 6F 72 70 72 6F 6A 65 63 74 2E 6F 72 67 w.torproject.org
0x00009AF0 2F 22 2E 20 49 66 20 79 6F 75 20 6E 65 65 64 0D /". If you need.
Bochs for Windows - Display
USER Copy Paste snapshot CONFIG Reset suspend Power
You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

Wrap Up

大多数勒索软件仍然允许您使用受感染的机器支付赎金。 但Petya不给你这个机会。 您必须使用不同的计算机上线，支付赎金，并获得解密密钥。 但请注意，如果您支付赎金，不能保证您将恢复您的受感染的系统。

用户版本的勒索软件比像Petya的MBR版本更容易分析。 有趣的是，注意勒索软件的不同策略和部署如何对不同的受害者构成不同的威胁。 修改MBR或硬盘驱动器中的其他扇区需要提升的特权。 这意味着有效避免类似恶意软件或勒索软件感染的一种方法是降低您的计算机系统的权限级别。 我们的建议是始终使用非管理员帐户登录到您的计算机。

始终遵循最佳安全实践，以避免被感染，包括定期安装修补程序和更新，计划的驱动器扫描与更新的AV文件，过滤您的Web和电子邮件流量，扫描链接和附件，然后单击它们。 而对于勒索软件，一致的备份策略将为您节省许多头痛。

评论