WannaCry和Lazarus攻击组织——缺失的关联？

2017-05-17 卡巴斯基

几个小时前，一名来自Google的叫做Neel Mehta的研究人员在Twitter发布了一条标签为#WannaCryptAttribution的神秘信息：

事实上，这段加密信息说的是两个样本在代码上存在相同之处。Neel所说的两个样本为：

- 一个来自2017年2月的WannaCry勒索软件样本，该样本看上去是非常早期的变种
- 一个来自2015年2月的Lazarus APT攻击组织所使用的样本

两者的相似之处见下图，其中一致的代码被框出：

那么，这意味着着什么呢？以下是一些我们想到的问题和答案。

我们曾经详细研究和报道过Lazarus攻击组织，并且同来自BAE和SWIFT的同事在卡巴斯基安全专家峰会（SAS 2017）上进行过专题演示。

此外，Lazarus攻击组织还是索尼影业攻击、孟加拉银行失窃案以及DarkSeoul行动的幕后黑手。

我们认为，Lazarus并不是一个普通的APT攻击组织。Lazarus发动的攻击行动在规模上令人感到震惊。该攻击组织从2011年起就一直处于活跃状态。该组织最早是通过Novetta发布的有关Operation Blockbuster的研究结果而被发现的。我们也参与了相关研究，并且在研究过程中，收集到数百个来自Lazarus的样本，表明Lazarus在运营一个恶意软件工厂，同行多个输送机制造大量最新的恶意软件。

理论上来说，一切都是可能的，尤其考虑到2017年2月发现的WannaCry样本可能是抄袭了2015年后门程序的代码。但是，这些代码似乎在之后版本的WannaCry样本中

都被删除。2017年2月的样本似乎是非常早期的WannaCry变种。我们认为伪旗行动理论上是可以的，但是应当不大可能。

目前来说，需要对WannaCry较早版本的变种进行进一步研究。我们认为这些研究可能是解开WannCry攻击行动谜团的钥匙。有一点可以确认——Neel Mehta的发现是迄今为止揭开WannaCry起源的最重要线索之一。

是的，它们使用相同的目标加密文件扩展名列表。但是，在2017年5月的变种中，添加了更多扩展名：

> .accdb
> .asm
> .backup
> .bat
> .bz2
> .cmd
> .der
> .djvu
> .dwg
> .iso
> .onetoc2
> .pfx
> .ps1
> .sldm
> .sldx
> .snt
> .sti
> .svg
> .sxi

> .vbs

> .vcd

此外，攻击者还删除了较旧的扩展名：“. tar.bz2” ，将其替换为 “ “.bz2” 。

我们坚信，2017年2月的样本和2017年5月大规模WannaCry勒索软件攻击中所使用的样本是同一批人编译的，或者是能够访问同样的源代码的人所编译的。

我们认为重要的是，全球其他研究人员也应该对这些恶意软件的相似之处开展调查，发现更多有关WannaCry起源的线索。回顾孟加拉银行失窃案，最初时，只有很少的证据指向这些攻击同Lazarus组织有关。但是随着时间推移，越来越多的证据出现，让我们和其他研究人员可以将这些证据联系起来，得出结论。所以，进一步研究对于将这些点连接起来至关重要。

是的，来自Coma Technologies的Matt Suiche确认Neel 提供的样本之间存在相似之处：

当然可以。

您可以从这里下载the “lazaruswannacry”的Yara规则。
下载链接：https://cdn.securelist.com/files/2017/05/lazaruswannacry.zip

还包括便于阅读的信息：

rule lazaruswannacry {

meta:

description = “Rule based on shared code between Feb 2017 Wannacry sample and Lazarus backdoor from Feb 2015 discovered by Neel Mehta”
date = “2017-05-15”

```
reference =  “https://twitter.com/neelmehta/status/864164081116225536”
author =  “Costin G. Raiu, Kaspersky Lab”
version =  “1.0”
hash =  “9c7c7149387a1c79679a87dd1ba755bc”
hash =  “ac21c8ad899727137c4b94458d7aa8d8”

strings:

$a1={
51 53 55 8B 6C 24 10 56 57 6A 20 8B 45 00 8D 75
04 24 01 0C 01 46 89 45 00 C6 46 FF 03 C6 06 01
46 56 E8
}

$a2={
03 00 04 00 05 00 06 00 08 00 09 00 0A 00 0D 00
10 00 11 00 12 00 13 00 14 00 15 00 16 00 2F 00
30 00 31 00 32 00 33 00 34 00 35 00 36 00 37 00
38 00 39 00 3C 00 3D 00 3E 00 3F 00 40 00 41 00
44 00 45 00 46 00 62 00 63 00 64 00 66 00 67 00
68 00 69 00 6A 00 6B 00 84 00 87 00 88 00 96 00
FF 00 01 C0 02 C0 03 C0 04 C0 05 C0 06 C0 07 C0
08 C0 09 C0 0A C0 0B C0 0C C0 0D C0 0E C0 0F C0
10 C0 11 C0 12 C0 13 C0 14 C0 23 C0 24 C0 27 C0
2B C0 2C C0 FF FE
}

condition:

((uint16(0) == 0x5A4D)) and (filesize < 15000000) and
all of them
}
```

长按二维码关注卡巴斯基
获取最新鲜专业的国际安全资讯和分析