2017 年 5 月 22 日，星期一

针对 Adylkuzz、Uiwix 和 EternalRocks 的思科防护

一周多以前出现的 WannaCry 攻击是首批利用 Shadow Brokers 泄露数据的大规模攻击之一。当时，我们最为担忧的是会很快发现其他威胁开始利用相同的漏洞。在过去数周，Talos 观察到其他恶意软件变种也在利用 Shadow Brokers 在其攻击活动中释放的 ETERNALBLUE 和 DOUBLEPULSAR 漏洞。这些恶意软件变种包括 Adylkuzz、Uiwix 和 EternalRocks。

Adylkuzz 是一种恶意软件，它利用 ETERNALBLUE 和 DOUBLEPULSAR 在受感染系统中安装加密货币挖矿软件。实际上，这种攻击出现在 WannaCry 攻击之前，到目前为止一直在持续传播加密货币挖矿程序。

Uiwix 使用类似的技术在受感染系统中安装勒索软件。当文件加密后，文件名会添加“UIWIX”作为文件扩展名的一部分。这种恶意软件的主要独特之处在于，勒索软件“自身不进行蠕虫传播”（这有别于 WannaCry），它只是将自己安装在系统中。

我们发现攻击者利用的另一个恶意软件变种名为 EternalRocks。在此类攻击活动中，该恶意软件使用 ETERNALBLUE 和 DOUBLEPULSAR 获取系统访问权限，但之后只将该权限用作后门，以在受感染系统中安装其他恶意软件。该恶意软件的一个显著特征是，它在下载最终有效负载（包括 Shadow Brokers 放出的多个其他漏洞）之前有 24 小时的休眠/延迟。这可以有效避开沙盒环境等防护措施。

在 WannaCry 勒索软件成功得手后，有关它的新闻时常见诸各媒体，我们必然会看到攻击活动使用类似的技术攻击易受攻击的操作系统，并传播其他类型的恶意软件。

Adylkuzz、Uiwix 和 Eternalrocks 只是模仿者的首批例子，在不久的将来，我们可能会看到更多攻击使用相同的感染媒介。攻击者可以结合使用漏洞 (ETERNALBLUE) 和后门程序 (DOUBLEPULSAR)，在受感染系统中安装和运行任意代码。

在降低风险时应务必牢记的一点是，要阻止攻击利用 Microsoft 安全公告 MS17-010 中所述的 CVE-2017-0143 到 CVE-2017-148 漏洞，最有效的方法是尽快为您的组织应用安全更新。

防护

Talos 发现利用这些漏洞的恶意软件正在增加。最终有效负载与防御这些攻击毫无关系。只要它们利用的是 Shadow Brokers 披露的漏洞和工具，基于网络的检测就可以阻止它们。

这些攻击利用的漏洞早在至少两个月之前就已经被发现，根据具体的漏洞，我们已在 2017 年 3 月中旬利用 NGIPS 和 NGFW 技术采取防护措施。

Snort 规则：42329-42332、42340、41978、42256

开源 Snort 用户规则集客户可以在 Snort.org 上下载出售的最新规则包，保持最新状态。

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	生产
AMP	✔
CloudLock	不适用
CWS	✔
邮件安全	不适用
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

网络安全设备（例如 NGFW、NGIPS 和 Meraki MX）可以检测与此威胁相关的恶意活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella 可防止对与恶意活动相关的域进行 DNS 解析。

StealthWatch 可以检测网络扫描活动、网络传播和与 CnC 基础设施的连接，从而与此活动建立联系，通知管理员。

发布者：ALEXANDER CHIU；发布时间：18:14

标签：ADYLKUZZ、防护、ETERNALROCKS、SNORT 规则、UIWIX