2017 年 1 月 31 日

思科对 Shamoon 2 的防护

Shamoon 是一种破坏性的恶意软件，攻击者曾利用该软件对沙特阿拉伯能源行业发起攻击。我们从 2012 年起便一直对该攻击事件进行跟踪。我们发现攻击者最近利用 Shamoon 的一个变体（识别为 Shamooon 2）侵入了几个组织和机构。Talos 意识到最近 Shamoon 2 攻击活动的增多，并已经做出回应以确保我们的客户得到保护。此外，Talos 将继续监控新进展，以确保我们的客户始终得到保护。

传播

据观察，Shamoon 2 瞄准非常具体的组织，并利用网络枚举和窃取的证书在网络中传播。有部分证书是从个人或共享帐户中盗取的特定组织的证书。其他的则是目标客户所使用产品的默认帐户。

防护

利用思科安全产品、服务和开源技术可对 Shamoon 2 进行防护。请注意，随着威胁的不断演变，我们可能会开发新的防护措施，并可能对现有防护措施进行改写或修改。因此，本文不应视为权威性文章。如需获取有关最新信息，请参阅您的 FireSIGHT 管理中心或 Snort.org。

Snort 规则

- 23893
- 23903
- 23905-23933
- 24127
- 40906

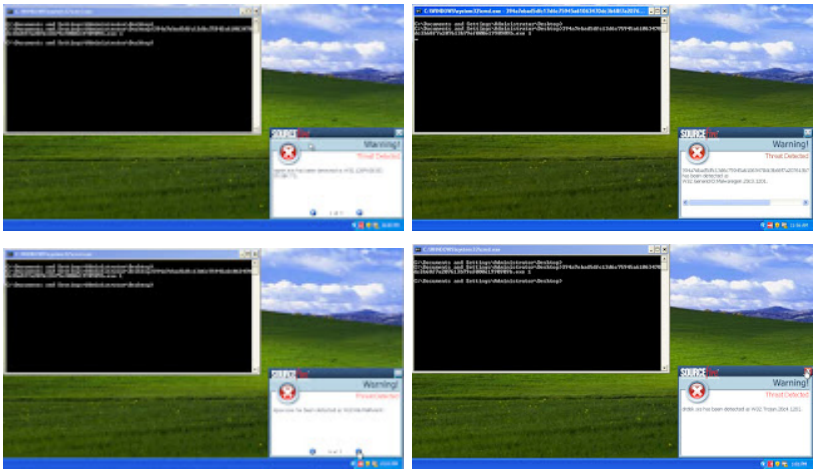
ClamAV 签名

- Win.Dropper.DistTrack-*
- Win.Trojan.DistTrack.*
- Win.Malware.DistTrack.*

AMP 测

- W32.GenericKD:Malwaregen.20c3.1201
- W32.Malwaregen.19nb.1201
- W32.47BB36CD28-95.SBX.TG

- W32.Malwaregen.19nb.1201
- W32.Generic:Malwaregen.20c3.1201
- Win.Malware.DistTrack
- W32.128FA5815C-95.SBX.TG
- W32.C7FC1F9C2B-95.SBX.TG
- W32.EFD2F4C3FE-95.SBX.TG
- W32.010D4517C8-95.SBX.TG
- Win.Malware.DistTrack.Talos



其他缓解策略

最近的 Shamoon 2 攻击活动有效地提醒了用户和组织必须制定全面的灾难恢复计划。没有人能够确定您是否会成为破坏性恶意软件的攻击对象，但我们可以百分之百肯定所有驱动器都会发生故障。如果没有适当的数据备份和恢复系统，则您将面临数据永远丢失的风险。有一点至关重要，即要确保对您的财产进行合理备份，使其可迅速恢复，以防 Shamoon、勒索软件或其他破坏性恶意软件的侵入或需要进行完全恢复的情况。

产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	N/A
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 的 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。

邮件安全功能可以拦截威胁源在攻击活动中发出的恶意邮件。

在 IPS 和 NGFW 的 网络安全保护功能中有最新的签名，可以检测威胁源的恶意网络活动。

AMP Threat Grid 有助于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。

发布者：ALEXANDER CHIU；发布时间：13:21
标签：AMP、CLAMAV、防护、SNORT 规则