2017 年 1 月 6 日，星期五

思科对“灰熊草原”(GRIZZLY STEPPE) 网络攻击活动的防护

在过去几周，人们对攻击多个美国政治、政府和私营实体的网络攻击活动进行了一些讨论。这些讨论主要指控这些网络攻击活动的目的是干扰 2016 年美国联邦大选，以及确定这些高调入侵活动的负责人。2016 年 12 月 29 日，美国国土安全部 (DHS) 和联邦调查局 (FBI) 发布了一份联合分析报告，详细介绍了攻击者用来入侵这些机构的部分工具和基础设施。DHS-FBI 联合报告将此次攻击活动称为“灰熊草原”(GRIZZLY STEPPE)。Talos 了解这些有关“灰熊草原”(GRIZZLY STEPPE) 恶意攻击活动的讨论和报告，并积极作出了响应，确保我们的客户已受到保护。

思科安全产品、服务和开源技术可提供针对“灰熊草原”(GRIZZLY STEPPE) 攻击活动的防护。思科已对 DHS-FBI 报告中列出的 IP 地址进行了评估，并将其列入了黑名单。请注意，Talos 将继续监控新发展，确保我们的客户始终受到保护。

AMP 保护

- W32.55058D3427-95.SBX.TG
- W32.9ACBA7E5F9-95.SBX.TG
- PHP.2D5AFEC034.backdoor.DRT
- W32.AC30321BE9-95.SBX.TG
- W32.9F918FB741-95.SBX.TG
- PHP.0576CD0E94.backdoor.DRT
- W32.Auto.0fd050.182066.in01
- PHP.1343C905A9.backdoor.DRT
- PHP.20F76ADA17.backdoor.DRT
- PHP.249EE04814.backdoor.DRT
- PHP.2D5AFEC034.backdoor.DRT
- PHP.3BD682BB78.backdoor.DRT
- PHP.449E7A7CBC.backdoor.DRT
- PHP.6FAD670AC8.backdoor.DRT
- PHP.7B28B9B85F.backdoor.DRT
- PHP.7DAC01E818.backdoor.DRT
- PHP.9376E20164.backdoor.DRT
- PHP.A0C00ACA2F.backdoor.DRT
- PHP.AE67C121C7.backdoor.DRT
- PHP.BD7996752C.backdoor.DRT

- PHP.D285115E97.backdoor.DRT
- PHP.DA9F2804B1.backdoor.DRT

Web 信誉/DNS 保护

- efax.pfdregistry.net
- private.directinvesting.com
- www.cderlearn.com
- ritsoperrol.ru
- littjohnwilhap.ru
- wilcarobbe.com
- one2shoppee.com
- insta.reduct.ru
- editprod.waterfilter.in.ua
- mymodule.waterfilter.in.ua
- efax.pfdregistry.ne

Snort 规则

41122-41136

ClamAV 签名

- Win.Trojan.OnionDuke-5486244-0
- Win.Trojan.Agent-5486255-0
- Win.Trojan.OnionDuke-5486245-0
- Php.Malware.Agent-5486261-0
- Win.Trojan.Agent-5486256-0

请注意，Talos 未来可能会发布更多规则、签名和其他检测，当前规则会根据未来得到的更多信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心或 Snort.org。

产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
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 的网络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。

邮件安全设备可以拦截威胁发起者在攻击活动中发出的恶意邮件。

网络安全设备（如 IPS 和 NGFW）拥有最新的签名库，可以检测威胁发起者的恶意网络活动

发布者：ALEXANDER CHIU；发布时间：11:30

标签：AMP、攻击活动、CLAMAV、防护、DNS、“灰熊草原”、SNORT 规则、WEB 信誉