2017 年 2 月 16 日，星期四

# 思科有效防护“Magic Hound”攻击

“Magic Hound”是代码名称，用于代指一系列表面看似有限的恶意软件传播活动（这些活动的攻击目标是沙特阿拉伯的组织以及在沙特阿拉伯有商业利益的组织）。Magic Hound 与 Talos 发现并记录的其他恶意软件传播活动相似，都使用带链接的网络钓鱼邮件，而邮件中提供的链接指向攻击者所控制服务器上托管的恶意 Word 文档。恶意文档在打开后会提示用户启用宏，企图诱导收件人执行攻击者的脚本，并下载其他恶意软件，从而导致收件人的系统被感染。“Magic Hound”与当前存在的一些更复杂的攻击活动有所不同，Magic Hound 攻击者采用的是商业恶意软件和工具。这其中包括 IRC 僵尸程序和 Metasploit Meterpreter 负载以及开源远程管理工具 (RAT) 等工具。

Talos 了解此项针对性的攻击活动，并已经做出响应以确保在“Magic Hound”和其他类似的攻击活动被识别以及不断变化的过程中，我们的客户都能始终得到保护。

## 防护

利用思科安全产品、服务和开源技术可有效防护 Magic Hound 攻击。请注意，随着此威胁的不断演变，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调整或修改。因此，本文不应被视为权威版本。如需获取最新信息，请参阅您的 FireSIGHT 管理中心或 Snort.org。

## Snort 规则

- 41655-41659

## AMP 检测

- W32.C21074F340.magichound.hunt.talos
- W32.EA139A73F8.magichound.hunt.talos
- W32.DA2ABDC951.magichound.hunt.talos
- W32.0D3AE68286.magichound.hunt.talos
- W32.F0ECC4388F.magichound.hunt.talos
- W32.860F4CD443.magichound.hunt.talos
- W32.B42B118621.magichound.hunt.talos
- W32.4BEEE6E7AA.magichound.hunt.talos
- W32.5E0E09C986.magichound.hunt.talos
- W32.3161F9087D.magichound.hunt.talos
- W32.B6C159CAD5.magichound.hunt.talos
- W32.6A7537F2CE.magichound.hunt.talos
- W32.16D87FBD86.magichound.hunt.talos

- W32.92BC7D0444.magichound.hunt.talos
- W32.86D3409C90.magichound.hunt.talos
- W32.C3A8F51763.magichound.hunt.talos
- W32.A390365DDF.magichound.hunt.talos
- W32.D2FFC757A1.magichound.hunt.talos
- W32.79C9894B50.magichound.hunt.talos
- W32.2F7F358250.magichound.hunt.talos
- W32.8C2E4AA8D7.magichound.hunt.talos
- W32.ABE8E86B78.magichound.hunt.talos
- W32.9E4D2E983F.magichound.hunt.talos
- W32.E57F77CC3D.magichound.hunt.talos
- W32.CA6E823DED.magichound.hunt.talos
- W32.EAAECABB43.magichound.hunt.talos
- W32.1C3E527E49.magichound.hunt.talos
- W32.29A659FB0E.magichound.hunt.talos
- W32.218FAC3D06.magichound.hunt.talos
- W32.E5B643CB6E.magichound.hunt.talos
- W32.71E584E7E1.magichound.hunt.talos
- W32.388B26E22F.magichound.hunt.talos
- W32.33EE8A57E1.magichound.hunt.talos
- W32.5469FACC26.magichound.hunt.talos
- W32.528714AAAA.magichound.hunt.talos
- W32.66D24A5293.magichound.hunt.talos
- W32.CFCE482710.magichound.hunt.talos
- W32.68DB2B363A.magichound.hunt.talos
- W32.E837F6B814.magichound.hunt.talos
- W32.F912D40DE9.magichound.hunt.talos
- W32.AF0AE0FA87.magichound.hunt.talos
- W32.6D1A50CA3E.magichound.hunt.talos
- W32.6C195EA18C.magichound.hunt.talos
- W32.97943739CC.magichound.hunt.talos
- W32.7E57E35F8F.magichound.hunt.talos
- W32.DB453B8DE1.magichound.hunt.talos
- W32.82779504D3.magichound.hunt.talos
- W32.1C550DC73B.magichound.hunt.talos
- W32.7CDBF5C035.magichound.hunt.talos
- W32.B2EA3FCD2B.magichound.hunt.talos
- W32.3F23972A0E.magichound.hunt.talos
- W32.133959BE83.magichound.hunt.talos
- W32.BA3560D3C7.magichound.hunt.talos
- W32.D8731A94D1.magichound.hunt.talos
- W32.D08D737FA5.magichound.hunt.talos

## 域/IP 地址检测

- analytics-google[.]org
- microsoftexplorerservices[.]cloud
- msservice[.]site
- service.chrome-up[.]date
- service1.chrome-up[.]date
- servicesystem.serveirc[.]com
- syn.timezone[.]live
- timezone[.]live
- www.microsoftsubsystem.com-adm[.]in
- www1.chrome-up[.]date
- www3.chrome-up[.]date
- www5.chrome-up[.]date
- www7.chrome-up[.]date
- 104.218.120[.]128
- 104.238.184[.]252
- 139.59.46[.]154
- 45.56.123[.]129
- 45.58.37[.]142
- 45.76.128[.]165
- 69.87.223[.]26
- 89.107.60[.]11
- 89.107.62[.]39

## 其他缓解策略

“Magic Hound”攻击者依然企图通过网络钓鱼邮件和社交工程在组织网络中找到立足点。此攻击活动突显出制定应对垃圾邮件和网络钓鱼邮件的全面策略以及安全意识计划的重要性。绝对不要访问未知或未验证发件人的电子邮件中的链接。

| 产品 | 保护 |
| --- | --- |
| AMP | ✔ |
| CWS | ✔ |
| 邮件安全 | ✔ |
| 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。

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。

IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者实施的恶意网络活动。

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。

发布者：ALEXANDER CHIU；发布时间：晚上 8:22
标签：AMP、CLAMAV、防护、MAGIC HOUND、规则、SNORT