新闻稿

[即时发布]

“有本事就来抓我呀!”企业发现 APT 攻击平均需要 205 天

亚信安全提醒信息安全管理员，要格外小心“图片”和“文档”中的黑色代码

【亚信安全】-【2016 年 1 月 8 日】近日，一份关于 APT 攻击的报告显示，在所有数据泄漏事件当中，黑客平均潜伏的天数长达 205 天。受害企业通常都有一个同样的疑惑：

“黑客是如何在我的网络中长期躲藏而不被发现？”。亚信安全通过对 APT 攻击长期的追踪发现，黑客往往会精心选择隐匿行踪的技巧，而且擅长通过有组织的行动将攻击分散开来，以躲避查杀。针对 APT 攻击的特征，亚信安全建议企业用户持续监察网络内的异常流量，并格外小心“图片”和“文档”中的黑色代码。

APT 攻击黑客团体特别擅长隐匿行踪

在所有黑客攻击行为当中，最有能力在企业网络内部四处隐藏及游走的，就应该是 APT 攻击。黑客团体有着组织性犯罪的显著特征，而且特别擅长隐匿行踪，他们通常会运用“零时差”漏洞进入网络。其盗取的核心机密数据能够在地下黑市为其换得高额回报，巨大的诱惑让他们长期潜伏下来，并且持续渗透。

黑客团体的成员之间，有着统一的指挥通道并且分工明确，要缉拿这些行动背后的首脑相当困难，尤其是当他们躲藏在国外的时候。事实上，许多 APT 攻击团体通常都有政府在背后支持。还有，即使我们可以从攻击行动所使用的网址来追溯到某个地区，但该网址注册的 DNS 和 IP 服务厂商通常也不愿配合国外的执法机关。正因如此，那些由政府在背后撑腰的黑客，就能一再发动恶意攻击而不会遭到任何惩罚。严重的是，这些黑客团体还会被一些投机取巧、恶意竞争的企业，甚至是恐怖组织雇佣。在低风险、高报酬的条件下，他们会不断从过去的失败当中吸取教训，并且每一次都比上一次的行动更加小心谨慎。

“如果我们还不能建立起有效的 APT 攻击防御架构，任何一个组织都可能遇到数据泄漏的危险。管理员必须要熟悉黑客窃取数据的方法，掌握 APT 攻击各个阶段的特点，并且能够针对 APT 攻击链条建立有效的抑制点，在互联网入口、内部交换层，都要配备更智能的过滤和分析机制，因为黑客正在把 APT 攻击代码写进看似正常的图片和文档中。”亚信安全 APT 治理专家徐江明提醒：“企业用户一定要关注 APT 攻击的变化。我们的工程师已经发现了更糟糕的状况，地下市场上随处可见的恶意程序，以及卷土重来的宏病毒已经被 APT 攻击者广泛采用。”

APT 攻击“武器”正在升级

亚信安全的研究人员发现，当前地下市场上最精密的恶意软件之一就是 Stegoloader，它可以将 C&C 通信隐藏在图片当中。大多数的系统管理员都会被这样的技巧所骗，因为他们习惯上只会在安全网关上拦截可以执行文件并进行分析，不会拦截图片文件。但这些图片一旦进入目标网络之后，恶意软件就会帮助黑客发挥“横向移动”的能力。另外，Stegoloader 采用了模块化的设计可让它在不同类型的终端之间移动，并且迅速发掘可窃取的数据类型及数量，进而判断是否值得花时间来发动进一步攻击。大多数的安全专家都认为 Stegoloader 是一种高级黑客用来从事长期攻击行动的工具。

能够骗过管理员和用户的另外一个伎俩就是 Office 文档，而这也是宏病毒藏身的地方。上世纪末最恶名昭彰的梅丽莎病毒(Melissa)出现之后，宏病毒貌似离开了人们的视线。但是，现在宏病毒强势回归，并成为了 APT 攻击的惯用工具。例如：2014 年出现的数据窃取软件 ZeuS，它通过启用宏的 Microsoft Word 文件来进行散播。在同年 11 月还发现了 DRIDEX(一个针对网络银行用户的数据窃取软件)采用相同的感染策略。紧随其后的是 ROVNIX、VAWTRAK、BARTALEX 这些后门恶意软件，黑客还加上自己的防御手段，他们或是对启用宏的文件加上密码保护来防止防毒软件的查杀，或是开辟新方法来通过宏恶意软件感染用户。

找出 APT 攻击的藏身之处

APT 攻击共有六个阶段，这包括：情报收集、单点突破、命令与控制 （C&C 通信）、横向移动、资产/资料发掘、资料窃取。在黑客团体常常分工明确，每一阶段由一组专门的黑客负责。另外，需要注意的不仅是在“单点突破”这个阶段的恶意代码，黑客在第四阶段的“横向移动”对于最后资料窃取阶段的布局也至关重要。不断地在不同终端之间移动，可以让黑客完整扫描整个网络，并且找到最珍贵的数据。

发现 APT 攻击者在企业内部的藏身之处有一定的难度，但不是说企业就束手无策。相反，企业必须不断提升自己的安全防护，并随时掌握整个企业网络的情况。亚信安全服务器深度安全防护系统（Deep Security）产品可提供 360 度全方位掌握来侦测 APT ,防范黑客窃取企业敏感信息。在今日的大环境下 ,黑客入侵已经是无可避免的事，因此尽可能降低黑客潜伏的时间，并且妥善保护核心的数字资产，这才是最重要的。

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式 ,助力客户构建“立体化主动防御体系” ，为国家提供网络安全与云产业安全保障 ,推动实施自主可控战略。更多关于亚信安全公司及最新产品信息 ,请访问: http://www.asiainfo-sec.com