瑞星预警：APT组织Lazarus Group对中国发起攻击 - 瑞星

it.rising.com.cn/dongtai/19777.html

瑞星预警：APT组织Lazarus Group对中国发起攻击

2021-06-01

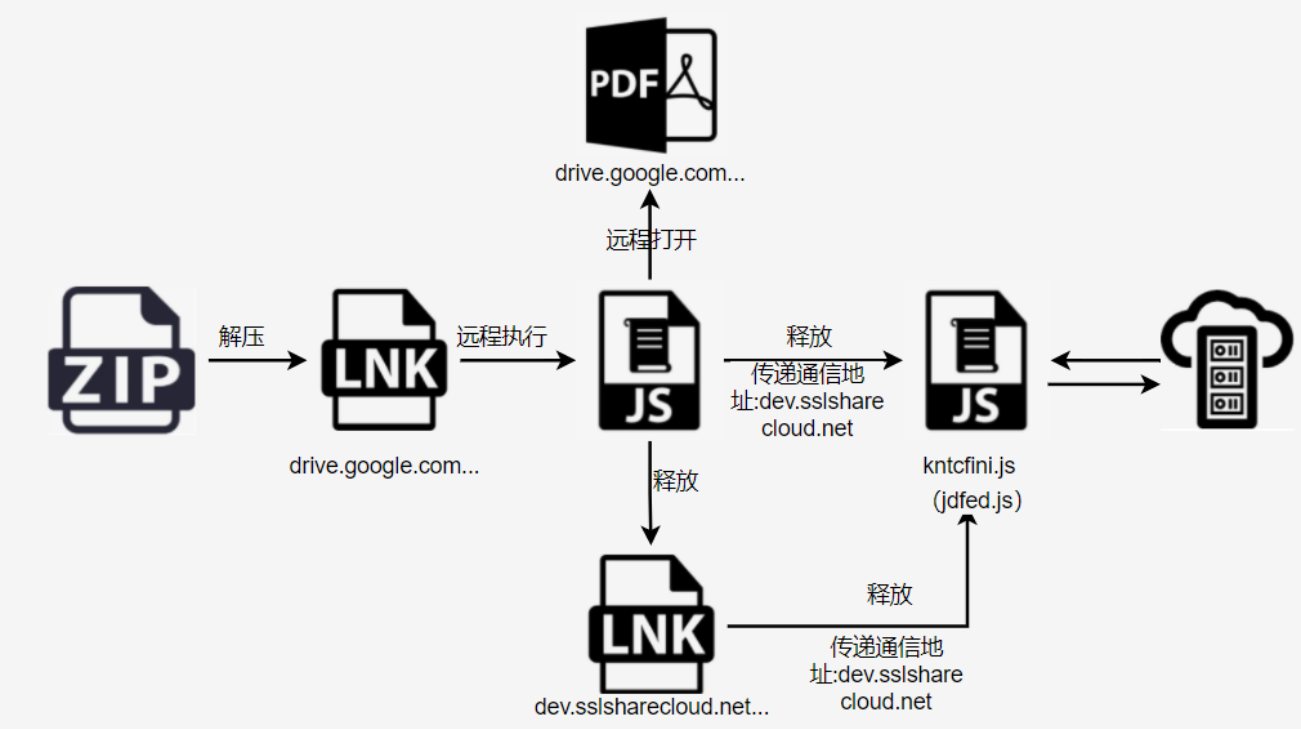
> 近日，瑞星威胁情报中心捕获到一起针对中国政府或企业发起的APT攻击事件，通过分析发现，攻击者利用钓鱼邮件等方式投递名为“安全状态检查.zip”的压缩包文件，其主题为《信息安全技术 信息系统安全等级保护实施指南》，以此来诱使中国大量政府部门或企业上钩，一旦中招，电脑将被攻击者远程控制，执行任意代码并盗取重要数据信息。

近日，瑞星威胁情报中心捕获到一起针对中国政府或企业发起的APT攻击事件，通过分析发现，攻击者利用钓鱼邮件等方式投递名为“安全状态检查.zip”的压缩包文件，其主题为《信息安全技术 信息系统安全等级保护实施指南》，以此来诱使中国大量政府部门或企业上钩，一旦中招，电脑将被攻击者远程控制，执行任意代码并盗取重要数据信息。

图：主题为“信息安全技术 信息系统安全等级保护实施指南”的诱饵文档

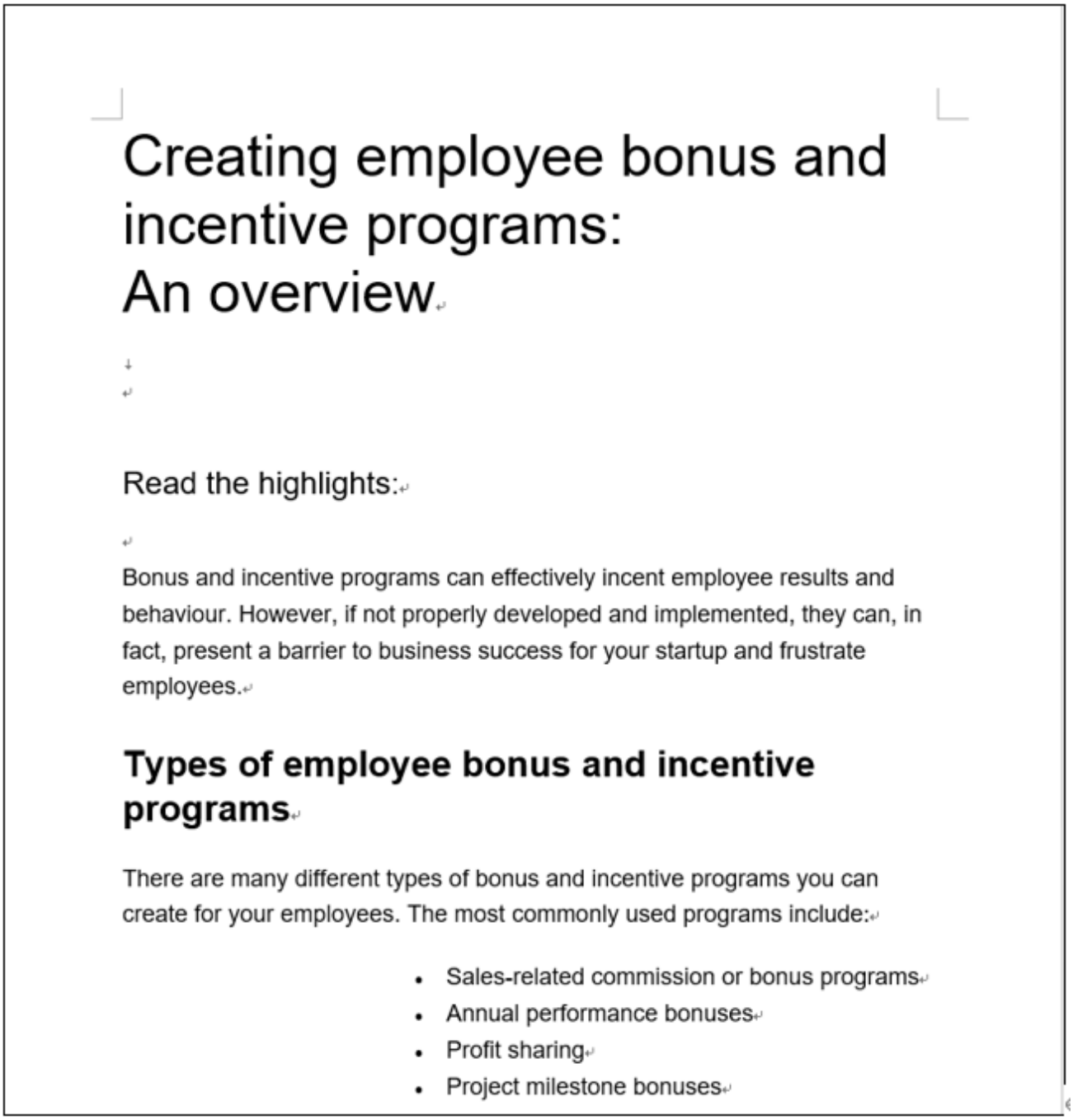
瑞星安全专家通过威胁情报数据对攻击手法、攻击方式分析后发现，此次攻击和Lazarus Group组织相关，该组织又被称为Group 77、Hastati Group、Hidden Cobra、APT-C-26、T-APT-15、Zinc和Nickel Academy等，是一个从2007年开始到现在最活跃的威胁组织之一。

Lazarus Group来自朝鲜，具有国家背景，其除了擅长信息盗取，间谍活动，还会蓄意破坏计算机系统，加密数据以获取经济利益，攻击的国家包括中国、德国、澳大利亚、日本等，涉及的领域有航空航天、政府、医疗、金融和媒体等。



图：攻击流程

通过关联分析，在5月份瑞星还捕获到Lazarus Group组织以相同攻击手法模仿加拿大玛斯（MaRS）网站中文章的诱饵文档，内容主要是关于创建员工奖金和激励计划。由于MaRS与中国一直有着紧密的合作，因此该攻击或与中国企业相关。



Creating employee bonus and incentive programs: An overview

Read the highlights:

Bonus and incentive programs can effectively incent employee results and behaviour. However, if not properly developed and implemented, they can, in fact, present a barrier to business success for your startup and frustrate employees.

Types of employee bonus and incentive programs

There are many different types of bonus and incentive programs you can create for your employees. The most commonly used programs include:

- Sales-related commission or bonus programs
- Annual performance bonuses
- Profit sharing
- Project milestone bonuses

图：模仿加拿大玛斯（MaRS）网站中文章的诱饵文档

瑞星公司表示，由于APT攻击有着针对性强、组织严密、持续时间长、高隐蔽性和间接攻击等显著特征，针对的目标都是具有重大信息资产如国家军事、情报、战略部门，和影响国计民生的行业如金融、能源等，因此国内相关政府机构和企业单位务必要引起重视，加强防御措施，具体方法如下：

1. 不打开可疑文件。

不打开未知来源的可疑文件和邮件，防止社会工程学和钓鱼攻击。

2. 部署网络安全态势感知、预警系统等网关安全产品。

网关安全产品可利用威胁情报追溯威胁行为轨迹，帮助用户进行威胁行为分析、定位威胁源和目的，追溯攻击的手段和路径，从源头解决网络威胁，最大范围内发现被攻击的节点，帮助企业更快响应和处理。

3. 安装有效的杀毒软件，拦截查杀恶意文档和木马病毒。

杀毒软件可拦截恶意文档和木马病毒，如果用户不小心下载了恶意文件，杀毒软件可拦截查杀，阻止病毒运行，保护用户的终端安全。

4. 及时修补系统补丁和重要软件的补丁。

编辑：瑞瑞 阅读：