网络攻击

什么是网络攻击

与可触发立即行动的实体威胁不同，网络威胁和攻击通常难以识别或了解。网络安全包括对网络事件的预防、侦测和响应。事实上所有现代组织 – 包括政府、医院、公司、银行和公共设施 – 都依靠计算机系统进行运营和数据管理，因此都容易受到网络攻击。

可能易受不良人员攻击的所谓“受攻击面”可包括计算机硬件、平板电脑、电话和很多其他基于网络的设备和所谓“物联网”中的家用电器。网络攻击的危险有入侵者擦除整个系统、把持数据或操作系统勒索赎金、盗窃机密或个人信息、闯入系统篡改文件，或利用计算机或设备访问联系人列表并攻击和感染他人。

关键术语

- **网络攻击**可能由个人、联网的团体、恐怖主义团体或国家发起，而且可能给政府、企业、公共设施和普通公众造成严重（和危险）问题。
- **黑客攻击**是一种“通过线路”对系统发起的直接攻击，其中攻击者（真人或自动化“机器人”）获得受保护/受限数据或运行的直接访问权。通常允许此种黑客攻击的路径是通过“网络钓鱼”或下载欺诈病毒打开的。
- **物联网（IoT）**包括网络启用的设备和家用电器，包括冰箱、音响系统、钟表、恒温器、安保系统、咖啡机等。
- **网络钓鱼**由广泛传播的电子邮件或文本通信组成，旨在希望某些收件人会点击信息的某个地方（比如，附件、链接、“启用宏”按钮），以激活病毒或其他恶意软件。定向网络钓鱼活动 – 例如，针对特定政府或公共设施的活动 – 被称为鱼叉式网络钓鱼。
- **社交工程**采用利用用户的漏洞，而不是其系统，从而绕开 IT 安保措施。实例包括网络钓鱼、电子邮件欺诈病毒以及其他面向连接的网络服务。用户通常是 IT 安保架构中最容易被打败的因素。

怎么办

灾前（准备/规避）

- ❑ 保持防火墙打开并更新。
- ❑ 安装或更新防病毒/防间谍软件。
- ❑ 使用强度高、独一的密码并定期更改。
- ❑ 搜索并立即安装您操作系统、固件、软件和防病毒软件的所有更新。
- ❑ 下载东西时要小心。切勿点击不请自来的电子邮件或文本中的附件、链接或宏。
- ❑ 不用时要关闭计算机。
- ❑ 务必核实电子邮件来源，如果有疑问，则删除之。
- ❑ 要警惕来自“不太正常”的已知联系人的电子邮件 – 拼写错误、奇怪的句法或用词、通用性语言、怪异的链接网址 – 很多黑客活动都冒充已知的电子邮件。
- ❑ 删除可疑内容之前要截屏，以便用于分析。
- ❑ 在外部硬盘或 Cloud 上定期备份所有数据；如果您使用 Mac系统，要启用“Time Machine”（时间机器）功能。

灾中（响应）

- ❑ 从网络中断开被感染设备的连接。
- ❑ 如果您在工作，要通知您的 IT 人员您设备遭受的任何可疑或确认的攻击，并提供截屏。
- ❑ 如果事件发生了财务、个人或医疗信息丢失，要报警。

灾后（重建）

- ❑ 要通知可能受到不利影响的任何人，包括您的信用账户、银行账户、客户、雇主、家人和朋友。更改您的账户以及全部密码。
- ❑ 运行适当的扫描和实用程序，消除感染。
- ❑ 监控您的信用报告、银行账单、投资和信用卡账单。
- ❑ 确保您的设备未受感染，如果有疑问，要擦除硬盘并重新安装所有软件。