AhnLab

安全月刊

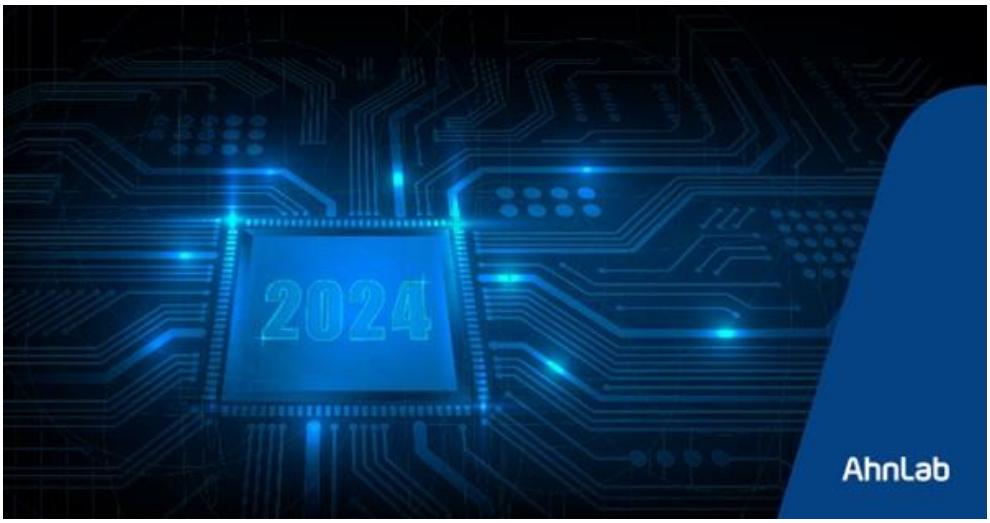
2024.01 Vol.134

2023 网络威胁总结和 2024 年预测

2023 网络威胁总结以及 2024 年预测

AhnLab发布了2023年5大网络安全威胁总结和2024年5大网络安全威胁预测。根据发布内容，攻击者预计将在2024年继续并扩大进行基于地区冲突的攻击、供应链攻击、网络钓鱼攻击等与2023年它们发起的攻击。

下面，让我们详细了解2023年威胁总结以及2024年的威胁展望。



2023 年的威胁总结 - 线上线下无处不在的网络威胁

2023年最值得关注的网络威胁特征是，俄罗斯与乌克兰、哈马斯与以色列等现实中的冲突演变成了网络战。此外，致力于扫荡网络攻击组织的国际合作不断扩大，而攻击者为了提高攻击成功率，使用更加巧妙的方法攻占目标组织或个人。

2023年主要网络威胁总结如下：

#1.现实中的冲突演变成网络攻击

去年，在冲突地区发现了多起冲突或战争的各支持势力发起的网络攻击。冲突地区之间的攻击主要发生在俄罗斯与乌克兰、哈马斯与以色列、印度与巴基斯坦等国。支持特定阵营的黑客组织对对方势力进行了DDoS攻击、篡改网站的Deface攻击、信息泄露和破坏等。

作为攻击目标组织的前期工作，黑客组织会查看周围相关人员的社交媒体，通过网络钓鱼攻击、间谍软件恶意代码攻击等获取相关人员的凭证（Credential）信息，并将其用于攻击。在攻击中，使用电子邮件的情况最多，从网上下载的文档文件的宏功能被阻止，因此使用宏的攻击急剧减少，恶意代码附件被更改为CHM文件或LNK文件。还发现了许多利用收集到的凭证信息，通过RDP（Remote Desktop Protocol，远程桌面协议）远程连接的入侵案例。

#2.加强对RaaS组织的应对

2023年，各国执法机构加强了对网络犯罪论坛和黑市的应对。通过这些努力逮捕了部分运营人员，还关闭了一些暗网网站。也有一些黑市是因运营人员自行退出而关闭的。

此外，执法机构还加强了对“勒索软件即服务（Ransom-as-a-Service，RaaS）”组织的应对。RaaS是一种勒索软件商业模式，提供网络犯罪分子部署和管理勒索软件所需的工具和服务，近期勒索软件攻击被广泛应用。
加强应对的结果是，关闭了Hive、Ragnar Locker、BlackCat（推测）等勒索软件团伙的“数据泄露网站（Data Leak Sites，DLS）”和组织，并在乌克兰逮捕和起诉了多名RaaS组织成员。逮捕行动不仅向其他网络犯罪分子发出了警告，还让其了解到他们的行动已受到国际关注并必将承担法律责任。

#3.利用软件漏洞进行APT攻击

2023年发生了多起利用韩国软件漏洞进行的攻击。恶意利用软件漏洞的针对性攻击主要针对韩国公共机构和企业进行。已确认的攻击包括零日漏洞（Zero-day）攻击和虽已发布补丁但未得到应用的“N-day”攻击。
攻击者恶意利用漏洞生成恶意文件或试图横向移动（Lateral Movement）以进行内部传播。他们通过这种方式，掌握攻击对象的基础设施，持续进行监控或泄露所收集的机密信息。

除了对攻击对象进行直接攻击外，还以开发人员为对象，在开发相关源代码或库中隐藏恶意功能，或者入侵知名软件制造商（例如：3CX），由此进行传播恶意代码的供应链攻击。这种供应链攻击的特点是，用户很难预防，且攻击一旦成功，仅1次的损失规模就会扩大到无法控制的程度。

#4.恶意利用双因素验证窃取资金的恶意应用程序增加

过去攻击者通过电话诈骗APP威胁受害者，窃取受害者发送的资金。然而，近期出现了通过绕过金融应用的双因素（2 Factor Authentication）验证进行登录的恶意应用，直接窃取受害者资金的情况。

目前在使用金融服务时，通常会在登录时收到金融公司发送的验证码，输入相应验证码进行验证后使用服务。而恶意应用程序会通过监视消息状态，窃取受害者接收的验证码，并利用该验证码连接到受害者的金融服务。具代表性的监视和窃取消息的恶意应用程序SMSstealer（Trojan/SMSstealer）就是以韩国快递公司、冒充熟人的请帖或讣告等与实际生活相关的主题，通过短信诈骗（Smishing）消息进行传播，从而欺骗用户将恶意应用程序安装到移动设备上。

#5.Magniber勒索软件停止传播

在过去的数年间，Magniber勒索软件一直是臭名昭著的勒索软件之一，从2017年开始将韩国网络用户作为攻击对象，并于2021年在全球范围内发起了攻击。Magniber勒索软件一直在使用“恶意广告（Malvertising）”技术，通过在网站广告中植入恶意脚本，使存在安全漏洞的系统感染恶意代码。最近还诱导用户运行其下载的恶意代码，使其感染勒索软件。

在过去6年间一直十分活跃的Magniber勒索软件从2023年下半年开始停止了传播。然而对于被感染的文件，目前还不清楚具体的解密方法。

2024 年的预测 - 2023 年的威胁仍在持续

AhnLab预测的2024年5大安全威胁包括：敌对势力之间网络攻击和黑客活动家的活动将增加、RaaS（勒索软件即服务）提供组织的变化加速、针对虚拟化平台的勒索软件攻击的活跃、针对金钱和个人信息的恶意安卓应用的扩散、以窃取加密货币为目的的个人钱包攻击加剧。

2024年5大网络安全威胁预测

1.敌对势力之间网络攻击和黑客活动家的活动将增加

在全球范围内，由于理念、宗教、利益等各种因素引起的冲突加剧，预计明年敌对势力之间的网络攻击将继续增加。为了实现目标，他们可能会采用各种方法。他们可能利用深度伪造技术制造假新闻以达到宣传和煽动（Propaganda，宣传活动）的目的，或者可能谎称过去泄露的内容是新的黑客攻击结果。特别是国家背后的攻击组织，他们可能不仅仅是为了窃取敌对势力的信息，还可能尝试针对基础设施障碍发起攻击。为了实现这一目的，攻击者预计将尝试直接攻击目标外，还有可能尝试“供应链攻击”，攻击安全管理相对薄弱的（敌对势力的）协作公司等。

在相同的背景下，“黑客活动家”的活动也预计会增加。黑客活动家是黑客（hacker）和活动家（activist）这两个词的合成词，是指在互联网上利用计算机技术进行整治抗议或推动社会变革的人。为达到政治或理念方面的某种目的，他们有可能会利用人工智能（AI）轻而易举地制作出深度伪造的语音和视频并大量流通。其中一些人有可能接受特定国家的资金支援或形成组织。

2.RaaS（Ransomware as a Service,勒索软件即服务）提供组织的变化加速

在执法机构对网络犯罪论坛和黑市的打击不断加强的同时，对于持续对个人和组织造成巨大损害的“勒索软件即服务（RaaS，Ransomware as a Service*）”提供组织的国际合作和应对预计将在2024年继续扩大。

** 勒索软件即服务（RaaS, Ransomware as a Service）：为网络罪犯提供勒索软件的分发及管理中所需的工具和服务的新型勒索软件商业模式*

因此，预测RaaS提供组织将尝试多种变革，以维持其生态系统。他们可能会加速在暗网内的论坛和市场之间的移动，通过更改名称来推动“品牌重塑”。此外，为了使调查机关难以追踪，并在攻击失败时作为替代手段，他们可能会采用其他RaaS提供组织使用的勒索软件的变体，实施所谓的“多重勒索软件”策略。

3.针对虚拟化平台的勒索软件攻击的活跃

为了有效管理云等硬件资源，采用“虚拟化平台”的企业数量正在不断增加。在这种情况下，为窃取企业的重要文件、基础设施或机密资料，针对“虚拟化平台”服务器的勒索软件攻击预计会增加。

特别是在市场占有高份额的解决方案很有可能成为攻击目标。例如，针对VMware的超级虚拟化平台——ESXi服务器的勒索软件攻击自2020年首次出现以来，其数量和变种一直在持续增加。此外，Hyper-V、KVM、Xen等各种虚拟化平台广泛应用于实际工作中，因此需要对各领域的勒索软件进行防范和监控。

4.针对金钱和个人信息的恶意安卓应用的扩散

随着金融服务的使用和用户敏感信息集中在智能手机上，2023年发现了各种恶意应用。2024年，针对用户金钱和敏感信息的恶意应用将不会升级，而且可能会传播到包括智能手机、智能电视、智能手表，智能家居等各种平台。

最近发现的贷款诈骗应用以提供合法个人贷款服务为名，收集联系方式、收入证明等个人信息以及银行账户等金融信息并泄露。这类应用通过精心制作移动网站以及发布到官方Google Play商店中，逐渐变得更加巧妙。这类恶意应用通过扩展到基于安卓操作系统的平台，如智能电视机顶盒、智能手表和智能家居等来传播，目的是个人信息泄露和广告收益。

5.以窃取加密货币为目的的对个人钱包的攻击加剧

各种攻击组织为窃取难以追踪交易记录的加密货币，一直在持续攻击用户的个人钱包和区块链漏洞。针对加密货币的攻击特点是随着加密货币价格的快速上涨和下跌而重复增加或减少。

在此情况下，预计到2024年4月，随着加密货币供给量减少的半衰期的临近，加密货币资产的整体的价格将上涨。攻击者可能会重新开展之前因加密货币价值上升而放缓的加密货币窃取攻击。特别是，攻击者为了提升攻击成功率，可能会专注于安全性相对薄弱的个人用户，而不是备有完善安全系统的加密货币交易所。

为预防这些安全威胁，组织应采取以下措施

- 对组织内的计算机、操作系统、软件、网站等进行定期的安全检查和补丁应用
- 利用安全解决方案和服务，并对内部员工实施安全教育
- 监控管理员账户的身份验证历史记录
- 建立符合组织环境的响应措施，如引进多因素身份验证（Multi-Factor Authentication）等

此外，个人应遵守以下安全措施

- 避免运行来历不明的邮件附件或URL
- 通过官方途径下载内容和软件
- 应用软件、操作系统、网络浏览器等的最新的安全补丁
- 在登录时，除登录密码外，还应使用双因素身份验证
- 保持防病毒软件为最新版本并启用实时监控功能

AhnLab安全情报中心（ASEC）的Hayeong,Yang主管表示：“如今，数字技术已经融入到我们生活的方方面面，以至于我们无法想象没有IT技术的生活。”，并补充说：“与此同时，由于这种环境也是网络犯罪分子活动的舞台，为了享受数字技术的便利，无论是组织或个人，都需要在生活中实践安全规则”。

AhnLab

安全月刊

https:// cn. ahnLab .com

https://global. ahnLab .com

https://www. ahnLab .com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ AhnLab .com