AhnLab

安全月刊

2022.12 Vol.121

2022 年网络安全趋势

2022 年十大网络威胁趋势

2022年开始于2021年12月引发的 Log4j 漏洞的影响仍然存在。随着世界各地安排许多政治和文化活动，对网络领域的安全威胁的预测比以往任何时候都多。CES 是每年举办时间最早的全球盛会，各家公司展示技术实力和当年的战略方向。在这备受世界瞩目的大会上，网络安全成为了2022年的五大主题之一。我认为这促使我们更加专注于网络安全领域的活动。此外，突发的俄乌战争和激烈的网络攻击者活动，面临前所未有的新局面。

在本文中，让我们回顾一下2022年一年中的国内外出现的主要网络安全威胁，了解当前的安全现状，思考解决或缓解问题的方案。

#1. Log4j 漏洞的出现和影响，以及启示

Log4j 是一种流行的开放源代码，多年来出现了各种版本。自 Log4j 漏洞被发现后，以 Log4j 作为必备元素的应用程序非常多，制造商和使用企业都很难查清现状。此外，可被恶意利用的安全漏洞不断出现，导致相关响应组织一直在不间断工作。

虽然在存在 Log4j 漏洞的安全性薄弱的服务器上安装加密货币挖掘器和相关恶意代码的案例并不多，但也有一些检测到的案例。其中，最引人注目的就是针对型勒索软件组织“NightSky”对 Log4j 漏洞的利用。

NightSky 以双重威胁而闻名，在窃取企业内部信息后，将所有信息加密，然后要求金钱补偿作为解密条件进行威胁。然后再次威胁企业会将其遭到入侵的消息和内部信息公开到暗网（Dark Web）。这是一种规模不同于安装收集和泄露计算机用户信息的恶意代码（例如加密货币挖掘器或 Infostealer）的网络攻击。

NightSky不像其他针对型勒索软件组织那样活跃，但它恶意利用 Log4j 安全漏洞，以及与受害企业进行通信时使用 Rocket.Chat 而不是 Tor 的这一特点引起了人们的关注。该勒索软件虽然没有对其他针对型勒索软件产生太大影响力，但可以说是勒索软件恶意利用 Log4j 的典型案例。

Log4j 漏洞大部分都没有进行到最后恶意代码安装，只进行到在处理字符串后与恶意服务器进行通信，这反而加重了安全人员的负担。这是因为不仅无法确定攻击者的意图，而且也不知道何时会发生什么样的安全事件的焦虑一直要持续到应用安全补丁为止。

至此，当针对个别安全补丁的引导已完成，相关监控也正在以国家和企业单位全面展开，这时就有必要在各个应用程序层面重新审核是否存在问题。目前，企业正在很好地应用策略，即果断屏蔽与不断发送易受攻击字符串的服务器通信，因此将当前情况和变化趋势一起分析后得出结论，以便在未来发生类似的网络安全威胁时为决策提供依据。

另外，也为所有安全人员和相关部门的努力和心情工作点赞，他们在全力应对 Log4j 漏洞，依然恪尽职守地履行各自岗位职责。

#2.针对型勒索软件主密钥的公开及解密工具的制作

首先，已公开主密钥的主要针对型勒索软件组织和活动期间如【表1】所示。

勒索软件组织	活动期间
Maze	2019.05 ~ 2020.10
Egregor	2020.09 ~ 2021.02
Sekhmet	2020.03 ~

【表1】公开主密钥的勒索软件组织和活动期间

Maze 勒索软件组织可以说是第一代针对型勒索软件组织，它以多家世界级企业（包括韩国企业）执行针对性攻击并在其官方网页上披露内部信息来实现双重威胁，从而逐渐为人所知。他们频繁发动攻击获取经济利益并提高影响力，却突然在2020年10月宣布隐退并就此销声匿迹。然而，就在他们消失之前，出现了一个叫做 Egregor 的勒索软件组织，有分析人士推测，部分 Maze 勒索软件组织成员加入了 Egregor 的行列当中。

Egregor 勒索软件组织攻击了大型连锁书店“Barnes & Noble”、软件开发商“Crytek”和“Ubisoft”，逐渐发展成了有名的针对型勒索软件组织。此后，在2021年2月，欧洲调查机构联合将其与 Netwalker 勒索软件组织一并捕获，因此才被迫停止了服务。由于 Sekhmet 勒索软件的勒索笔记与 Egregor 相同，被判断为同一个勒索软件组织。

上述勒索软件的主密钥以及基于此的解密工具现已成功制作并公开于网络。目前，推测公开者为曾隶属于此类勒索软件制作组织的成员，而且与活动在欧洲和东欧的勒索软件制作组织的被捕事件无关。

要用数字方式寻找并解决勒索软件，以现阶段技术仍存在局限性。若达到一定条件能够不受限制使用近期热门的量子计算，情况则会有所不同，但遗憾的是，按当前情况很难实现这一点。然而，像本次案例一样，被动的等待制作组织或调查机构发布主密钥，也并不是万全之策。主密钥的公开是在此类针对型勒索软件组织在隐退或退出业界一段时间后，有人出自善意而进行的行为，而且到目前为止，主密钥的公开案例也非常少见。

总而言之，对于在全球范围内造成巨大损失的第一代针对型勒索软件组织 Maze 的主密钥公开和解密工具的制作，其行为本身具有充分的意义。如果有企业或机构因此类勒索软件蒙受损失并需要解密，建议尝试使用解密工具进行恢复。作为参考，解密需要勒索笔记文件。

#3.勒索软件的两极分化

对一些攻击活跃势头正盛的勒索软件，我们已经非常熟悉了。其中之一是 LockBit 勒索软件。不断进化的 Lockbit 3.0 已经发展成为一款针对型勒索软件，它通过加密文件、公开窃取信息和 DDoS 攻击来施加三重威胁。

从“针对型”勒索软件一词可以获知，目前的勒索软件通过偶发性攻击某人的情况很少见。我们一定要明白，此类组织总是以精心计算的意图发动经万全准备的攻击。

通过 AhnLab 公开在 ASEC 博客的 Lockbit 3.0 攻击案例可以看出，攻击者会传播一个伪装成入职申请表的恶意 Word 文档，它巧妙地使用诸如“任圭敏.docx”或“全彩琳.docx”之类的人名来进行伪装。

仅是从公开的攻击模式，就可以看出他们的攻击并非偶然。此类攻击大部分是以“渗透组织内部网络或受害者

计算机 > 安装恶意代码 > 根据意图传播额外的恶意代码或攻击工具 > 窃取管理员帐户 > 为达到妨碍系统恢复目的而删除恢复镜像并结束服务 > 达到目的”这一顺序开展攻击的。从他们成功入侵企业或组织内部后的行为来看，可以推断极有可能是有意接近的。

但值得注意的一点是，新增勒索软件的制作比例明显在逐年下降。现在，一般的勒索软件制作和传播并不会带来多少利润，勒索软件市场也呈现出一种两极分化的趋势。部分有名且大规模的针对型勒索软件会频繁攻击政府机构和主要企业并从中谋取利益，而相反许多其他勒索软件也只活动一两次后便销声匿迹。尽管总体勒索软件数量呈逐渐下降的趋势，但我们要时刻牢记，真正造成威胁的高级针对型勒索软件并没有降低攻击级别。

#4.想方设法使安全系统瘫痪的攻击者

将计算机和服务器上运行的安全系统造成瘫痪，其原理好比电影中入侵者击杀哨兵。由于哨兵的作用也同样是拦截身份不明或可疑的对象，因此内在的关系也有相似之处。

在网络安全领域，攻击者与防御者的较量仍在继续，技术也不断发展到现在。防病毒（AV）产品会删除在正常操作系统环境中被识别为恶意代码的文件，而攻击者会为了阻止干扰他们的 AV 产品正常运行，不断进行各种尝试。

以往，当攻击者尝试卸载（uninstall）AV 产品时，一直采用了输入验证码这一过程来防御攻击。然而，最近发现攻击者会通过直接干预等多种方式从而使防御系统瘫痪。下面让我们来看两则示例。

首先，通过 AhnLab 在9月份发布的“Lazarus攻击组织利用BYOVD的Rootkit恶意代码分析报告”可以看出，攻击者会恶意利用旧版本的 INITECH 进程执行初始入侵企业，其后从攻击者的服务器下载并执行 Rootkit 恶意代码。Rootkit 恶意代码恶意利用易受攻击的驱动内核模块直接对内核内存区域执行读写操作，使系统中包括 AV 在内的所有监控系统无法运行。

此外，最近以“韩国型”勒索软件闻名的“鬼神（Gwisin）勒索软件”会以安全模式重启，而后加密文件，由此绕过 AV 产品。安全模式中仅运行必要的服务，不加载除 Windows 基本驱动外的其他软件，从而可以绕过 AV 产品的监控。

因此，在攻击者不断尝试瘫痪安全系统的情况下，防御者所能选择的最佳方案就是监控自身的安全系统并积极地进行管理，防止攻击者趁虚而入。此外，不仅要密切关注攻击者的攻击动向，还要时刻了解自身所处现状并进行应对。面对那些想方设法破坏我们安全系统的攻击者，我们要时刻做好万全准备。

#5.通过国际合作逮捕网络威胁者

毫不夸张地说，逮捕网络威胁者的消息始于一年前拘捕韩国CLOP勒索软件合作者的事件。这一事件成为了逮捕主要势力的起点，后来在乌克兰的帮助下最终逮捕成功。此外，在2021年10月，还获知了与 LockerGoga 勒索软件相关人员以及其他执行多次网络攻击的相关人员均被捕的消息。

近日，虽然未能获知勒索软件组织的名称，但有消息称，在50多个国家造成约100万美元损失的网络威胁者已被抓获，通过韩国以及与西方主要国家的紧密合作，陆续找到并逮捕了网络犯罪相关人员。

另一方面，有消息称，在今年1月份，在俄罗斯逮捕了一名参与 Revil 勒索软件组织的相关人员，该组织在韩国亦被称为 BlueCrab 勒索软件，在国外被称为 Sodinokibi 勒索软件。从俄罗斯传来逮捕网络罪犯的消息极为少见。由此可以看出，选择与国际社会合作而非保护本国国民可能是一种出于战略性的决策，也有可能是俄罗斯证明其与 DarkSide 勒索软件组织和 Revil 勒索软件组织的背后势力无关的一种“举措”。

考虑到美俄之间，对网络威胁既不承认也不合作的先例，俄罗斯的选择无疑对未来该做出何种战略选择提供了值得深思考虑的线索。

#6.国家背后的网络攻击组织动态

今年3月，韩国举行了第20届总统选举。当时，在韩国处于“重大事件”的期间，各方应该都在密切关注着各国会如何开展网络攻击。

目前，在政治或军事上与韩国对立的国家，在这样的特定时期直接开展网络攻击时，几乎无法从中获取实际利益。但是，他们似乎曾间接地尝试寻找各领域内他们所需信息的方法，以准备应对各种情况。

作为其中的一部分，他们持续开展了攻击，将插入恶意脚本的文档文件发送给特定收件人。该攻击中使用的恶意脚本基本上已经过代码混淆（Obfuscation）处理，使普通用户无法正常阅读。阅览文档文件从而使恶意脚本运行时，它会收集并泄露保存在用户计算机上的敏感信息，同时也会收集有关计算机本身的信息。由此可以看出，这些攻击者的攻击方式是为了明确区分对象的权宜之计。

例如，AhnLab 最近在 ASEC 博客上发布了一篇“伪装成新闻问卷的恶意Word文档”的帖子。该恶意 Word 文档的文件名为“CNA[Q].doc”，伪装成了针对与朝鲜有关的人员进行的 CNA 新加坡广播公司的采访。当用户开始键入时，会弹出一个消息框，指示需要运行宏。为了撰写文档，用户会点击允许授权内容的按钮，届时将运行包含在文档中的恶意 VBA 宏。

这种类型的攻击与收集并泄露用户信息的 Infostealer 相似。然而，与上述案例一样，关键的区别在于国家背后的网络攻击组织会带着明确的目的行动。目前成为攻击目标的行业包括政治、统一、外交、航空航天、国防工业以及能源&可再生能源等。因此，涉及国家相关主要技术或企业的核心技术以及资料的组织必须更要提高警惕。

#7.受到瞩目的多因素认证，留给我们哪些作业?

2021年5月，发生了一起俄罗斯网络犯罪分子在非政府机构（NGO）设置为默认多因素验证（MFA）协议的情况下，通过利用错误配置的帐户注册了 MFA 专用新设备，而后访问受害者网络的案例。在此过程中，攻击者恶意利用了Windows打印后台处理程序（spooler）漏洞“Print Nightmare （CVE-2021-34527）”并以系统权限运行了任意代码。

由于 MFA 会通过两个以上的授权设备验证用户，因此它显然是攻击者难以攻击的防御措施之一。然而，对此进行迂回的事故却时有发生，引发了诸多担忧。当然，不能说 MFA 是一个可以阻挡所有攻击的100%完美的安全系统，但如果使用得当，它可以给攻击者带来不便，使他们无法轻易达到预期目的。

因此，不必因上述安全事故就怀疑并弃用 MFA 本身，反而要积极应用，而且需要仔细考虑配置策略，以消除任何误用或滥用的可能性。此外，通过定期检查和删除组织内部的用户帐户中不再存在的帐户信息，并快速应用已知安全漏洞的补丁，从而最大限度地降低风险因素。若能持续执行此类措施，便能最大限度地发挥 MFA 的效果，进而在更安全的环境下专注于业务。

#8.窃取（Steal）信息（Info）

Infostealer 是一种信息窃取型恶意代码，其目的是窃取保存在网络浏览器或电子邮件客户端等程序中的用户帐户信息或加密货币钱包地址、文件等用户信息。根据ASEC 2022年第三季度报告，Infostealer 被攻击者积极用于攻击，在该期间传播的恶意代码中占比高达55.1%。

近期，从 Infostealer 恶意代码的发展趋势来看，它们之间正持续发生着链接和变化。一个代表性的案例就是线上银行恶意代码系列之一的 Emotet。在一段时间内反复出现又消失的 Emotet，通过与 Trickbot 的链接实现了迅速的传播，但在2021年初，其基础设施被调查机构查封后便逐渐平息了下来。

9个月后，即2021年底，再次复活的 Emotet 不再与之前的机器人（bot）系列的恶意代码联动，转而搭载了独有的垃圾邮件发送功能，具有了自我传播的能力。此外，Emotet 原有的信息收集和泄漏功能得到了进一步改进。目前，Emotet 完全可以被包含在自去年以来迅速成为主要恶意代码的 Infostealer 中，AhnLab 也在密切关注其未来的发展态势。

#9.针对 IoT 设备漏洞的攻击

在针对连接到网络的各种 IoT 设备漏洞的攻击不断发生的情况下，利用世界范围内众多客户使用的无线路由器（或路由器）漏洞的网络攻击也在肆意猖獗。考虑到通过单个路由器可以控制所有连接到有线/无线互联网的设备，其连锁反应可谓不容小觑。

攻击者通过掌握无线路由器或路由器可以获取什么利益？它可以拦截用户输入的各种个人信息，并诱导用户访问他们所创建的伪装成正常网站的钓鱼页面。此外，被掌握的路由器可用来面向连接到网络的不特定人群展开的 DDoS 攻击。攻击IoT设备的代表性恶意代码为 Mirai 和 Tsunami 等。

为针对此类攻击采取安全措施，需要对最先被攻击的路由器（或有线/无线路由器）执行安全漏洞的补丁应用，并检查受控路由器是否存在 DDoS 攻击和针对登录帐户的暴力破解（Brute Force）攻击。此外，需要持续管理登录帐户，及时移除不使用的可登录帐户，并应用仅允许受限用户访问设备的安全策略，以最大限度地减少威胁造成的损害。

#10.挖矿恶意软件（Miner），其独有的经济体系

挖矿恶意软件（Miner）是为挖掘加密货币而制作的应用程序的总称，其正式名称为 Coin Miner，简称挖矿恶意软件（Miner）。

在2018年初，当加密货币备受关注时，通过网络浏览器进行加密劫持（Crypto Jacking）的恶意代码造成了巨大的破坏。在今年，随着经济下滑速度的加快，关注度开始有所下降，但与加密货币挖矿相关的恶意代码，虽不似从前，但也在不断地制作和传播，

而且最近的挖矿恶意软件正呈现出扩展领域的态势，甚至还发现了与收集和泄露用户信息的 Infostealer 联动的现象。如上所述，Infostealer 窃取的信息包括保存在网络浏览器或应用程序中的用户帐户信息，以及加密货币钱包地址。此外，如今还出现了搭载有能够将很长的加密货币钱包地址转换为攻击者钱包地址的 Clipper 功能的恶意代码。

作为参考，2017年有一个名为 Crypto Shuffler 的恶意代码，它具有替换加密货币钱包地址的功能，由此重新诞生的 Clipper 加强了该功能。Crypto Shuffler 在恶意代码中包含了钱包地址，其文件大小达到数十兆字节。但 Clipper 与之不同，Clipper 会通过内部运算结构判断相关加密货币，并将其替换为攻击者的地址，大幅缩小了文件体积。从攻击者的角度来看，它不仅减轻了文件体积负担，还可以针对各种加密货币钱包，而且包括具有泄露信息的 Infostealer 功能以及 Coin Miner 的挖矿功能，是一种集合了各种恶意代码长处的恶意代码。

一直以来，挖矿恶意软件被认为只能导致组织和企业资源枯竭这种程度的损害。但是，它们在自身的经济结构中不断生产并活跃着，摆脱了以往的简单功能，如今已经能够收集和泄露主要信息，窃取加密货币钱包地址等从而直接造成打击。组织需要了解此类变化，并持续检查内部基础设施中的挖矿恶意软件活动。

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