SANGFOR
深信服科技

让每个用户的数字化更简单、更安全

深信服官方微信

深信服移动官网

深圳市南山区学苑大道1001号南山智园A1栋
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY | 深信服千里目 Sangfor DeepINSight

2022APT趋势洞察报告

2022 APT TRENDS INSIGHT REPORTS

深瞻情报实验室

目录 CONTENTS

写在开始

2022 年，受复杂的国际政治、经济摩擦及疫情等诸多因素影响，网络黑产和 APT 攻击大行其道，技术界限也正日渐模糊。

浏览器漏洞和操作系统漏洞仍是 APT 组织的最爱。网络安全企业监测到的在野 0Day 漏洞在 2022 年达到 20 余个，主要被 APT 攻击者应用在初始打点和提权阶段。从趋势看，出于经济利益的考虑，各大勒索组织也逐渐成为在黑客论坛购买 0Day 漏洞的一大主力。

APT 组织在攻击技巧方面的创新性受到红队安全研究社区的影响痕迹明显，同时非常擅长将最新技术、最新工具应用在其攻击行动上。无论是“白加黑”还是 BYOVD，攻击者的应用技巧愈发炉火纯青。而随着攻击者对现代终端安全的研究逐渐深入，近年来高对抗性的 C2 工具不断出现，且被越来越多的 APT 组织应用在实际攻击中，对 APT 攻击防御以及溯源的挑战也在不断增加。

从 2021~2022 年已经披露的 APT 攻击事件来看，掺杂政治目的的网络监控、情报目的的大规模渗透、金钱目的的定向勒索、啼笑皆非的“自杀式”网络攻击以及“罗宾汉”式的劫富济贫，各类定向攻击事件让安全研究者面前的网络安全攻防场景故事目不暇接，而大国博弈背景下，消除勒索软件和供应链攻击影响经济、科技、民生发展的隐患也迫在眉睫。

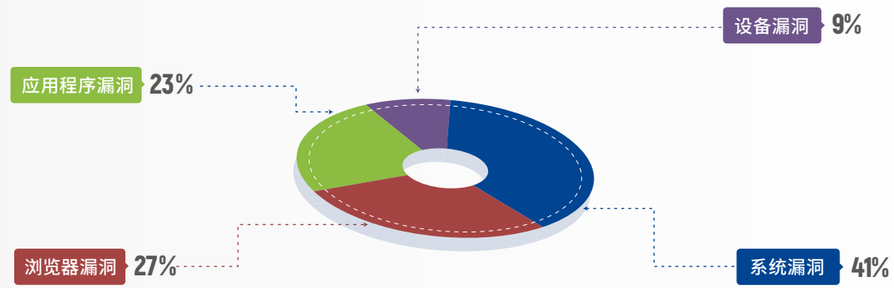
本报告将从漏洞利用视角、攻击技巧视角、攻击事件视角、全球 APT 组织活动视角等多个维度，为您呈现深信服千里目安全技术中心研究人员的技术洞察。本报告初看篇幅较多，读者完全可以选择自己感兴趣的章节阅读，下图是本报告的各章框架提要：

漏洞利用视角

0Day漏洞攻击趋势

2022 年我们监测到多个 APT 组织利用多个平台以及应用的 0Day 漏洞开展攻击。APT 组织使用的 0Day 漏洞约 21 个，漏洞类型涉及浏览器漏洞、Windows/Linux/iOS 等操作系统漏洞、网络设备漏洞、应用程序漏洞等 4 种，其中应用程序、浏览器以及操作系统漏洞占比较大。该趋势说明社会工程学攻击，包括各类定向钓鱼、水坑等攻击场景仍是 APT 攻击组织获得目标内网初始落脚点的重要途径，安全意识培训、社工攻击的及时发现及事件响应和遏制能力是易受 APT 攻击的组织降低定向攻击潜在后果及损失的有价值方法。

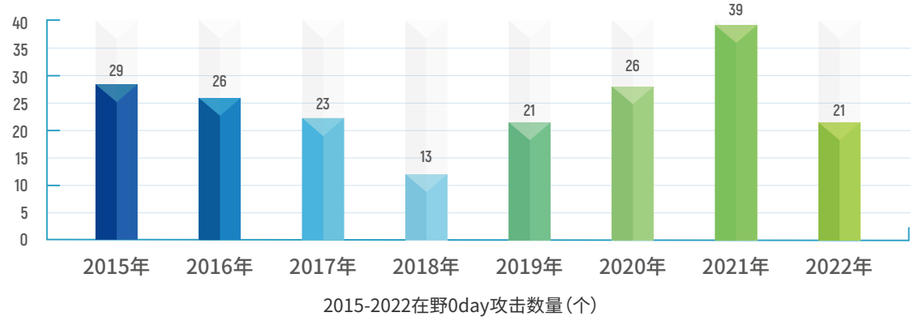
2022年0day漏洞类型饼状图



数据来源:《2022APT趋势洞察报告》

0Day 漏洞攻击频度发展趋势

2022 年，在野 0Day 漏洞已达 21 个，相较于 2021 年数量有所下降。但是，从整体趋势上看，0Day 漏洞的影响组件 / 系统日益通用，0Day 攻击对网络空间的威胁程度呈逐年上升趋势。特别说明，这些已被发现的 0Day 并非全部，黑客个人或攻击组织通过暗网等渠道对 0Day 进行交易的情况被安全行业监测的信息十分有限，还有很多 0Day 攻击未被发现或公开。

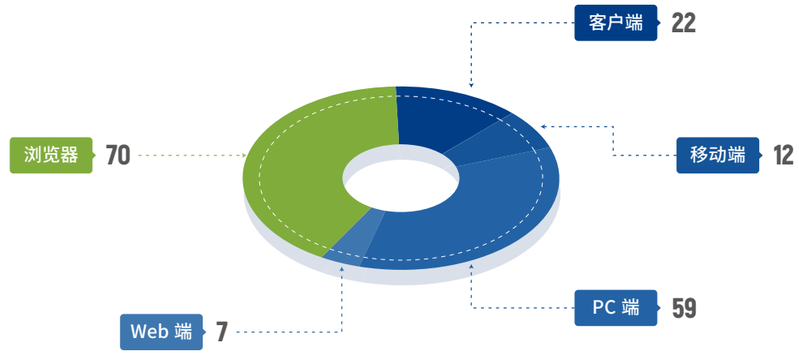


2015-2022在野0day攻击数量（个）

数据来源：《2022APT趋势洞察报告》

在野 0Day 漏洞的平台选择

我们通过对 2015 年以来的在野 0Day 攻击漏洞所属平台进行定量分析，可以看出 PC 端操作系统和浏览器 0Day 漏洞攻击数量较多，占据主要部分。其中浏览器 0Day 漏洞（配合 PC 端操作系统本地提权）是 APT 攻击的常见入口。从攻击难度和攻击效益来看，浏览器 0Day 漏洞攻击实施复杂度低、攻击效率高，攻击者只需要诱导用户访问一个 URL 即可获取受害者主机权限，这仍然是众多黑客或 APT 组织追逐的理想攻击方式。



2015-2022各平台在野0day攻击数量(个)

数据来源：《2022APT趋势洞察报告》

0Day 漏洞攻击变化趋势：多为已知漏洞的补丁绕过

分析 2022 年已披露的在野利用 0day 漏洞，我们发现很多 0day 漏洞都是因为先前漏洞没有完全修补而产生的。相关趋势说明，对于被 APT 攻击者利用的软件厂商，如何充分理解漏洞利用原理，并及时且彻底缓解或修复漏洞利用点将是长期存在的技术挑战，对于最终的软件产品用户而言，持续跟踪攻击趋势并及时更新补丁，提升安全意识，减少攻击平面，可能是缓解相关风险有意义的举措。

具体来看，研究发现至少有 8 个在野利用的 0day 漏洞为已知漏洞的补丁绕过，其中部分新发现的 0day 漏洞，是基于 2021 年发现在野利用的漏洞的变体 [1]。当原始的漏洞被修补后，攻击者又开始使用新变体 0 day 漏洞进行攻击活动。

例如，Windows 权限提升漏洞（CVE-2022-21882），概念验证漏洞利用的执行流程得到了修补，但没有得到根本解决，攻击者依然能够通过其他路径触发原始漏洞。

Windows LSA 远程代码执行漏洞（CVE-2022-26925），最初的漏洞已被修补，但在某个时候补丁回退，因此攻击者可以再次利用相同的漏洞。

Windows 脚本语言远程代码执行漏洞（CVE-2022-41128）[2] 与 Ivan Fratric 通过模糊测试发现的 CVE-2021-34480 非常相似，通过变体分析发现的新的漏洞，目前已发现在野利用情况。

Apple 内存损坏漏洞（CVE-2022-22587），缓冲区溢出通过检查缓冲区是否小于某值来解决，但修补后没有检查下界，从而产生新的漏洞。

下图为 2022 年在野利用的 0day 漏洞补丁绕过与原始漏洞关联说明表。

[1] https://googleprojectzero.blogspot.com/2022/06/2022-0-day-in-wild-exploitationso-far.html
[2] https://googleprojectzero.github.io/0days-in-the-wild/0day-RCAs/2022/CVE-2022-41128.html

序号	漏洞名称	2022 年 0day	已修补的 0day
1	Windows 权限提升漏洞	CVE-2022-21882	CVE-2021-1732 (2021年发现在野利用)
2	Apple 内存损坏漏洞	CVE-2022-22587	CVE-2021-30983 (2021年发现在野利用)
3	Windows MSDT 远程代码执行漏洞	CVE-2022-30190	CVE-2021-40444 (2021年发现在野利用)
4	Windows 脚本语言远程代码执行漏洞	CVE-2022-41128	CVE-2021-34480
5	Chrome v8 类型混淆漏洞	CVE-2022-1096	CVE-2016-5128 CVE-2021-30551 (2021年发现在野利用) CVE-2022-1232
6	Chrome v8 类型混淆漏洞	CVE-2022-1364	CVE-2021-21195
7	Atlassian Confluence Server 远程代码执行漏洞	CVE-2022-26134	CVE-2021-26084
8	Windows LSA 远程代码执行漏洞	CVE-2022-26925	CVE-2021-36942

表 1 2022 年变体 0day 漏洞说明

人们谈及 0day 漏洞利用时，通常认为在漏洞细节未知的情况下，很难去捕获 0day 漏洞利用。从今年 0day 漏洞利用的趋势来看，猎捕 0day 漏洞有了一种新的可能性，即安全专家可以通过分析曾经是在野利用的 0day 漏洞的根本成因以及补丁，编写适当的猎捕规则，主动猎捕变体的 0day 漏洞。此外，由于国际上一些大型勒索集团每年赚取数百万美元的利润，他们逐渐成为在暗网或黑客论坛购买 0day 漏洞的一大主力。

已被披露的各APT组织0Day利用情况

从攻击阶段来看，攻击者在“初始打点”(InitialAccess) 阶段主要使用不同系统的浏览器、防火墙等网络设备、应用程序漏洞，“提权”(PriviledgeEscalation) 阶段一般利用 Windows 漏洞进行提权。2022 年已监测到的 APT 组织利用漏洞的情况总结如下：

Lazarus

2022 年 3 月 24 日，谷歌威胁分析小组（TAG）[3] 披露了两个归因于东北亚某国黑客组织的针对美国新闻媒体、IT、加密货币和金融科技行业的攻击活动。

攻击者对特定目标进行社会工程学攻击，单击链接的受害者将收到一个隐藏的 iframe，攻击者在隐藏的 iframe 中放置指向漏洞利用工具包的链接。

该漏洞利用套件首先执行一段高度混淆的 javascript 脚本对目标系统进行指纹识别。该脚本收集了所有可用的客户端信息，例如用户代理、分辨率等，然后将其发送回利用服务器。如果满足条件，C2 服务器将下发有关 Chrome 远程代码执行漏洞（CVE-2022-0609）利用的 EXP。

攻击者对 0day EXP 投递在多个阶段进行保护，包括但不限于：

仅在特定时间提供 iframe 漏洞利用的跳转

鱼叉邮件中的链接包含唯一 ID，保证只触发一次

漏洞利用套件对每个阶段进行 AES 加密

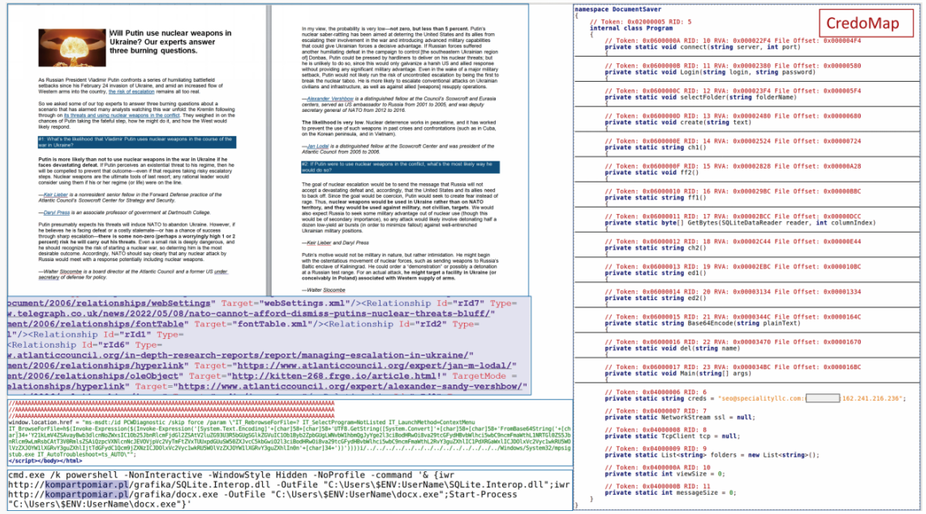
如果前一阶段失败，则终止攻击

[3] https://securelist.com/apt-trends-report-q2-2021/103517/

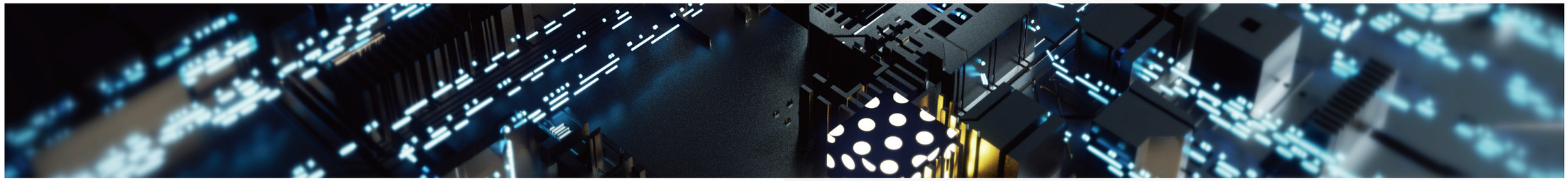
APT28

2022 年 6 月 20 日，乌克兰计算机应急响应小组 (CERT-UA) 披露利用 Windows MSDT 远程代码执行漏洞 (CVE-2022-30190) 部署密码窃取恶意软件的鱼叉式网络钓鱼攻击活动。

攻击者利用名为“Nuclear Terrorism A Very Real Threat.rtf”的诱饵文件进行鱼叉式网络钓鱼活动，点击此文件将下载 恶意的HTML 文件并执行 CVE-2022-30190 漏洞利用的 JavaScript 代码 ，最终下载并执行 CredoMap 恶意软件。



乌克兰计算机应急响应小组 (CERT-UA) 声称，基于 IOC 特征与攻击目标，将此次攻击活动归因于 APT28 (又名 Fancy Bear 或 Sofacy)。



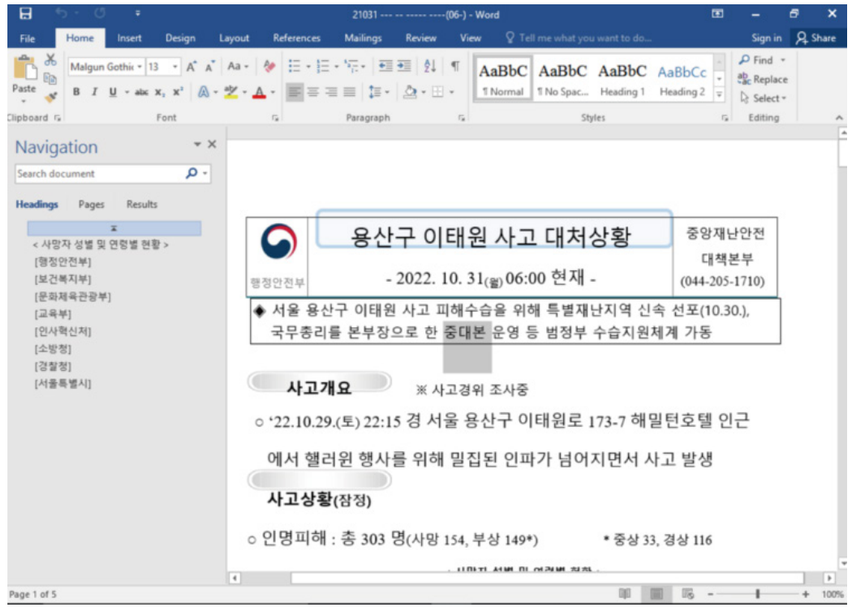
APT37

2022 年 12 月 7 日，谷歌威胁分析小组 (TAG) 于 2022 年 10 月下旬捕获的一个 0day 漏洞攻击事件。攻击者针对韩国用户，投放包含 Windows 脚本语言远程代码执行漏洞（CVE-2022-41128）利用的钓鱼文档，谷歌威胁分析小组将此活动归因于 APT37 。

2022 年 10 月 31 日，来自韩国的多名提交者将一份可疑的 Office 文档上传到 VirusTotal 。

这份名为《221031 首尔龙山梨泰院事故应对情况 (06:00) .docx》的文件提到了 2022 年 10 月 29 日万圣节庆祝活动期间发生在韩国首尔梨泰院附近的悲惨事件。这一事件被广泛报道上，诱饵利用了公众对此次事故的广泛关注。

这不是 APT37 第一次使用 Internet Explorer 0day 漏洞攻击目标用户。



该文档下载了一个富文本文件 (RTF) 远程模板，该模板又获取了远程 HTML 内容。由于 Office 使用 Internet Explorer (IE) 解析此 HTML 内容，自 2017 年以来，该技术已被广泛用于通过 Office 文件分发 IE 漏洞（例如 CVE-2017-0199）。通过此攻击向量传送 IE 漏洞的优点是不需要目标使用 Internet Explorer 作为其默认浏览器，也不需要将漏洞与 EPM 沙箱逃逸链接起来。

经过调查，谷歌威胁分析小组 (TAG) 发现到攻击者滥用了 Internet Explorer 的 JScript 引擎中的一个 0day 漏洞。

该漏洞存在于 Internet Explorer 的 JavaScript 引擎 jscript9.dll 中，由于错误的 JIT 优化导致类型混淆问题，TAG 于 2022 年 10 月 31 日向微软报告了该漏洞，并于 2022 年 11 月 3 日分配 CVE-2022-41128 编号。该漏洞已于 2022 年 11 月 8 日修补。

攻击者下发远程 RTF 时，Web 服务器会在响应中设置一个唯一的 cookie，当请求远程 HTML 内容时再次发送该 cookie。漏洞利用的 JavaScript 会在执行 payload 之前验证 cookie 是否已设置。此外，在执行漏洞利用之前和漏洞利用成功之后，向 C2 服务器发包两次，验证攻击利用情况。shellcode 部分使用自定义哈希算法来解析 Windows API。在下载下一阶段之前，shellcode 通过删除 Internet Explorer 缓存和历史记录来清除所有利用痕迹。最后设置下发远程 RTF 时相同的 cookie 下载最终有效载荷。

其它

另外，还有一些未知 APT 组织攻击事件的漏洞利用情况。攻击策略主要以社工攻击为主，攻击面主要以不同系统的浏览器和应用程序漏洞为主，用户需持续提升安全意识，及时更新软件补丁，减少攻击平面暴露。所利用的漏洞名称如表 1 所示。

序号	漏洞名称	CVE 编号	漏洞类型
1	Chrome 远程代码执行漏洞	CVE-2022-0609	浏览器漏洞
2	Chrome v8 类型混淆漏洞	CVE-2022-1096	浏览器漏洞
3	Chrome v8 类型混淆漏洞	CVE-2022-1364	浏览器漏洞
4	WebKit 远程代码执行漏洞	CVE-2022-22620	浏览器漏洞
5	Firefox 释放重引用漏洞	CVE-2022-26485	浏览器漏洞
6	Firefox 释放重引用漏洞	CVE-2022-26486	浏览器漏洞
7	Sophos Firewall 认证绕过漏洞	CVE-2022-1040	设备漏洞
8	Zyxel USG FLEX 远程命令执行漏洞	CVE-2022-30525	设备漏洞
9	Windows 权限提升漏洞	CVE-2022-21882	系统漏洞
10	Apple 内存损坏漏洞	CVE-2022-22587	系统漏洞
11	Apple 内存损坏漏洞	CVE-2022-22674	系统漏洞
12	Apple 内存损坏漏洞	CVE-2022-22675	系统漏洞
13	Windows 权限提升漏洞	CVE-2022-24481	系统漏洞
14	Windows CLFS 权限提升漏洞	CVE-2022-24521	系统漏洞
15	Windows LSA 远程代码执行漏洞	CVE-2022-26925	系统漏洞
16	Windows MSDT 远程代码执行漏洞	CVE-2022-30190	系统漏洞
17	Windows 脚本语言远程代码执行漏洞	CVE-2022-41128	系统漏洞
18	Apache log4j2 远程代码执行漏洞	CVE-2021-44228	应用程序漏洞
19	Atlassian Confluence Server 远程代码执行漏洞	CVE-2022-26134	应用程序漏洞
20	Trend Micro Apex Central 远程代码执行漏洞	CVE-2022-26871	应用程序漏洞
21	Zimbra Collaboration 文件上传漏洞	CVE-2022-41352	应用程序漏洞
22	向日葵远程代码执行漏洞	NA	应用程序漏洞

表 1 未知 APT 组织的漏洞利用情况

APT组织的0Day漏洞利用阶段特征

我们监测到的热门 APT 组织主要在 APT 攻击的“初始打点”(Initial Access) 阶段和“权限提升”(Privilege Escalation) 阶段利用 0Day 漏洞开展攻击，原因在于打点阶段是攻击者获得目标初始立脚点的关键环节，如何在此阶段有效利用目标脆弱点、绕过安全防御并降低目标意识到攻陷发生的可能性，便是攻击者考虑的重要因素；而提权阶段则与攻击者扩大信息收集成果并有效提升目标内网的攻击范围密切相关。攻击者在这两个攻击环节的 0day 漏洞，具体利用情况总结如下：

Initial Access阶段

特征：在“初始打点”阶段，APT 攻击者主要利用面向互联网的应用程序的漏洞进行攻击，以此获取对系统的初始访问权限，其中浏览器 0Day 漏洞的使用量大幅提高。基于 [MITRE ATT&CK] 的 TTPs 命名，攻击者主要采用的攻击技术包括 Exploit Public-Facing Application 和 External Remote Services。

在“初始打点”阶段利用的漏洞包括：CVE-2022-0609、CVE-2022-1096、CVE-2022-1364、CVE-2022-22620、CVE-2022-26485、CVE-2022-26486、CVE-2022-1040、CVE-2022-30525、CVE-2022-26925、CVE-2022-30190、CVE-2021-44228、CVE-2022-26134、CVE-2022-26871、CVE-2022-41352 等 15 个漏洞。本阶段内利用漏洞开展攻击的技术对应于 MITRE ATT&CK 技巧编号：T1190、T1566.003。

综合各方面的信息，2022 年 0Day 漏洞在 Initial Access 阶段利用情况汇总如表 2。

序号	战术	漏洞名称	CVE	漏洞类型	攻击策略	APT 组织
1	T1566.003	Chrome 远程代码执行漏洞	CVE-2022-0609	浏览器漏洞	结合社会工程学进行水坑攻击	Lazarus
2	T1566.003	Chrome v8 类型混淆漏洞	CVE-2022-1096	浏览器漏洞	结合社会工程学进行水坑攻击	NA
3	T1566.003	Chrome v8 类型混淆漏洞	CVE-2022-1364	浏览器漏洞	结合社会工程学进行水坑攻击	NA
4	T1566.003	WebKit 远程代码执行漏洞	CVE-2022-22620	浏览器漏洞	结合社会工程学进行水坑攻击	NA
5	T1566.003	Firefox 释放重引用漏洞	CVE-2022-26485	浏览器漏洞	结合社会工程学进行水坑攻击	NA
6	T1566.003	Firefox 释放重引用漏洞	CVE-2022-26486	浏览器漏洞	结合社会工程学进行水坑攻击	NA
7	T1190	Sophos Firewall 认证绕过漏洞	CVE-2022-1040	设备漏洞	攻击公开暴露应用并植入后门	NA
8	T1190	Zyxel USG FLEX 远程命令执行漏洞	CVE-2022-30525	设备漏洞	攻击公开暴露应用并植入后门	NA
9	T1190	Windows LSA 远程代码执行漏洞	CVE-2022-26925	系统漏洞	攻击公开暴露应用并植入后门	NA
10	T1190	Windows MSDT 远程代码执行漏洞	CVE-2022-30190	系统漏洞	攻击公开暴露应用并植入后门	NA
11	T1190	Windows 脚本语言远程代码执行漏洞	CVE-2022-41128	系统漏洞	攻击公开暴露应用并植入后门	APT37
12	T1190	Apache log4j2 远程代码执行漏洞	CVE-2021-44228	应用程序漏洞	攻击公开暴露应用并植入后门	Lazarus/APT42
13	T1190	Atlassian Confluence Server 远程代码执行漏洞	CVE-2022-26134	应用程序漏洞	攻击公开暴露应用并植入后门	Driftingcloud
14	T1190	Trend Micro Apex Central 远程代码执行漏洞	CVE-2022-26871	应用程序漏洞	攻击公开暴露应用并植入后门	NA
15	T1190	Zimbra Collaboration 文件上传漏洞	CVE-2022-41352	应用程序漏洞	攻击公开暴露应用并植入后门	NA
15	T1190	向日葵远程代码执行漏洞	NA	应用程序漏洞	攻击公开暴露应用并植入后门	OceanLotus

表 2 漏洞在“初始打点”阶段的应用情况

分析发现，Apache log4j2 远程代码执行漏洞以及 Chrome 远程代码执行漏洞被 APT 组织广泛使用。攻击者主要利用浏览器漏洞结合社会工程学进行水坑攻击获得攻击目标的初始访问权限。

具体包括：

- Apache log4j2 远程代码执行漏洞（CVE-2021-44228）
- Chrome 远程代码执行漏洞（CVE-2022-0609）
- Windows LSA 远程代码执行漏洞（CVE-2022-26925）
- Windows MSDT 远程代码执行漏洞（CVE-2022-30190）
- Windows 脚本语言远程代码执行漏洞（CVE-2022-41128）
- Zyxel USG FLEX 远程命令执行漏洞（CVE-2022-41352）
- Atlassian Confluence Server 远程代码执行漏洞（CVE-2022-26134）
- Zimbra Collaboration 文件上传漏洞（CVE-2022-41352）

下面，我们对这几个关键的漏洞进行简要介绍。

Apache log4j2 远程代码执行漏洞（CVE-2021-44228）

2021年12月9日，深信服安全团队监测到一则Apache Log4j2组件存在远程代码执行漏洞的信息，并成功复现该漏洞。

该漏洞是由于Apache Log4j2某些功能存在递归解析功能，攻击者可利用该漏洞在未授权的情况下，构造恶意数据进行远程代码执行攻击，最终获取服务器最高权限。

2021年12月10日，Apache Log4j2官方针对此漏洞发布的2.15.0-rc1版本存在绕过，官方再次发布 2.15.0-rc2版本以解决绕过问题。

Chrome 远程代码执行漏洞（CVE-2022-0609）

2022年2月16日，深信服安全团队监测到Chrome 组件存在远程代码执行漏洞的信息。

该漏洞是 Chrome 动画组件存在 use-after-free 漏洞，攻击者可利用该漏洞结合社会工程学进行水坑攻击获得攻击目标的初始访问权限。

Windows LSA 远程代码执行漏洞（CVE-2022-26925）

2022年5月11日，深信服安全团队监测到一则efslsaext.dll组件存在远程代码执行漏洞的信息，漏洞编号：CVE-2022-26925，漏洞威胁等级：高危。

该漏洞是由于逻辑错误，攻击者可利用该漏洞在未授权的情况下，构造恶意数据进行远程代码执行攻击，最终获取服务器最高权限。

Zyxel USG FLEX 远程命令执行漏洞（CVE-2022-41352）

2022年5月14日，深信服安全团队监测到Zyxel USG FLEX 存在远程命令执行漏洞。

该漏洞是由于特定路径处理json格式的传入数据时存在错误，攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行系统命令注入攻击，最终执行任意代码。

Windows MSDT 远程代码执行漏洞（CVE-2022-30190）

2022 年 5 月 30 日，深信服安全团队监测到一则 Windows MSDT 组件存在远程执行代码漏洞的信息，漏洞编号：CVE-2022-30190，漏洞威胁等级：高危。

该漏洞是由于 MSDT 被用户应用使用 URL 协议调用，攻击者通过社会工程诱使受害者从网站下载并打开特制文件，最终获取用户权限。

Windows 脚本语言远程代码执行漏洞（CVE-2022-41128）

2022 年 11 月 30 日，深信服安全团队监测到一则 Windows 中 Internet Explorer 的 JScript9 引擎存在类型混淆漏洞的信息。

该漏洞是由于错误的 JIT 优化导致类型混淆问题，攻击者通过加载包含 JavaScript 的远程 HTML 的 Office 文档来执行任意代码。

Atlassian Confluence Server 远程代码执行漏洞（CVE-2022-26134）

2022 年 6 月 4 日，深信服安全团队监测到一则 Atlassian Confluence Server and Data Center 组件存在远程代码执行漏洞的信息，漏洞编号：CVE-2022-26134，漏洞威胁等级：严重。

该漏洞是由于数据处理不当，攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行 OGNL 表达式注入攻击，最终导致远程代码执行。

Zimbra Collaboration 文件上传漏洞（CVE-2022-41352）

2022 年 10 月 24 日，深信服安全团队监测到一则 Zimbra Collaboration 组件存在任意文件上传漏洞的信息，漏洞编号：CVE-2022-41352，漏洞威胁等级：高危。

攻击者可以利用漏洞上传恶意文件到 web 目录 /opt/zimbra/jetty/webapps/zimbra/public，最终可在目标系统上执行恶意代码。

Privilege Escalation阶段

特征：在获取初始访问权限之后，APT 攻击者开始采用相关技术手段来扩展对环境的访问权限，实现“权限提升”(Privilege Escalation)。

在 Privilege Escalation 阶段利用的漏洞包括：CVE-2022-21882、CVE-2022-22587、CVE-2022-22674、CVE-2022-22675、CVE-2022-24481、CVE-2022-24521 等 6 个漏洞。本阶段内利用漏洞开展攻击的技术对应于 MITRE ATT&CK 技巧编号为 T1190。

通过综合分析，我们将 2022 年 0Day 漏洞在 Privilege Escalation 阶段利用情况简要汇总如表 3。

序号	战术	漏洞名称	CVE	漏洞类型	攻击策略	APT 组织
1	T1190	Windows 权限提升漏洞	CVE-2022-21882	系统漏洞	获取初始访问权限后进行权限提升	NA
2	T1190	Apple 内存损坏漏洞	CVE-2022-22587	系统漏洞	获取初始访问权限后进行权限提升	NA
3	T1190	Apple 内存损坏漏洞	CVE-2022-22674	系统漏洞	获取初始访问权限后进行权限提升	NA
4	T1190	Apple 内存损坏漏洞	CVE-2022-22675	系统漏洞	获取初始访问权限后进行权限提升	NA
5	T1190	Windows 权限提升漏洞	CVE-2022-24481	系统漏洞	获取初始访问权限后进行权限提升	NA
6	T1190	Windows CLFS 权限提升漏洞	CVE-2022-24521	系统漏洞	获取初始访问权限后进行权限提升	NA

表 3 漏洞在“权限提升”阶段的应用情况

下面，深信服千里目深瞻情报实验室对以下关键漏洞进行简要介绍：

- Windows 权限提升漏洞（CVE-2022-21882）
- Windows CLFS 权限提升漏洞（CVE-2022-24521）

Windows 权限提升漏洞（CVE-2022-21882）

2022年1月12日，深信服安全团队监测到一则Windows CLFS组件存在权限提升漏洞的信息，win32k 在处理用户请求时存在内存越界读写漏洞，攻击者可以利用此漏洞进行本地提权，获得系统管理员权限。

Windows CLFS 权限提升漏洞（CVE-2022-24521）

2022年4月13日，深信服安全团队监测到一则Windows通用日志文件系统存在本地提权漏洞的信息。该漏洞是由于类型混淆，攻击者可利用该漏洞在获得低权限的情况下，构造恶意数据执行本地提权攻击，最终获取服务器最高权限。

攻击技巧视角

本章内容将为读者介绍今年以来在 APT 攻击活动中高频出现的多项热点技术，并结合攻击实例分析其技术利用动机、后期演变趋势，以及作为防御者如何具备和提升检测猎捕能力。

本章介绍的主题包括：

热点技术 1：DLL Hijacking

即 DLL 劫持，其原理是劫持进程的 DLL 加载过程。攻击成功会使得目标进程载入和执行恶意 DLL，从而导致攻击者达成代码执行、权限提升、权限维持等攻击目标。同时，由于攻击者在利用这项技术时所选择的劫持目标往往只会是系统进程或其它具有签名认证的第三方进程，所以在国内我们也常常把这种利用技术手段称为“白加黑”利用。

热点技术 2：BYOVD/ 泄露证书

随着 Windows 内核保护机制的逐步完善，攻击者入侵内核的成本也在急剧增加，也因此，近些年来针对 Windows 内核入侵的场景并非攻击活动的主战场。但从今年的情况来看，攻击者在技术利用上又有着向内核入侵场景的偏移倾向，且内核入侵的最终目标相较于以往也有所转变。

热点技术 3：多款 C2 或成“新宠”

近年来，多款 C2 相继发布，它们大多具备前沿的防御规避能力，并呈现出分庭抗礼之势，这意味着未来的攻击活动在 C2 选择上将不再局限于 Cobalt Strike，这类新型 C2 或许也将凭借着其优秀的能力而受到攻击者的青睐，同时对于那些喜欢采用自研工具的 APT 组织来说，这些 C2 所集成的技术能力也将具有很强的参考意义。

热点技术 4：被忽略的破坏性攻击

APT 攻击通常是指长期隐蔽的攻击行动，而破坏性攻击却意味着主动暴露，所以我们很少将 APT 与破坏性攻击联系在一起。再者，以摧毁目标系统为目的的攻击行动也不符合大部分攻击者的利益需求，使得破坏性攻击逐渐淡出人们视野。但通过俄乌网络战的表现不难看出，破坏性攻击的威胁并没有消失，仍然值得被我们重视。

热点技术 5：永不落幕的钓鱼攻击

长期以来，钓鱼攻击都是最为主要的打点手段之一，也颇受 APT 组织喜爱，钓鱼攻击一旦成功，便能极大地节省攻击成本。源于此，攻击者们也在不断地挖掘与钓鱼相关的漏洞和攻击技巧，并将其投入到实际攻击活动中。

DLL Hijacking

实战案例分析

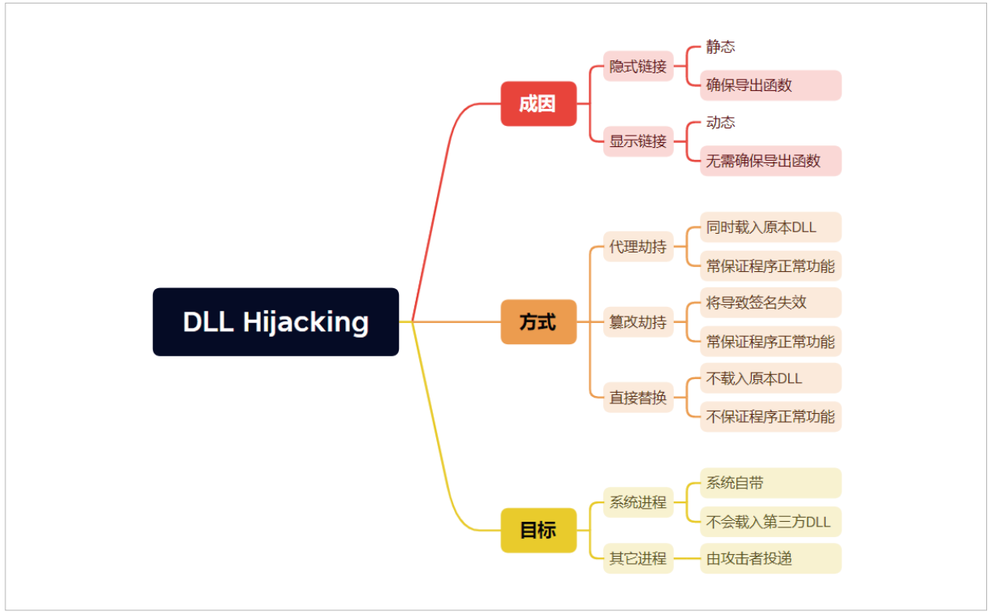
DLL 劫持技术由来已久，其核心是通过系统进程或具有数字签名的合法文件来执行攻击代码，从而使得每项恶意行为都由受信任的合法进程发起，或藏匿在正常的行为之中，这能有效地帮助攻击者绕过终端安全软件的检测，以及混淆安全分析人员的视听。这同时也是此项技术经久不衰的主要原因。

下图罗列了自 2022 年以来不同 APT 组织关于此项技术的利用情况。从图中可以看出该项技术正在被源自不同地区、不同背景，有着不同攻击目标的 APT 组织所使用，相同组织在不同时间节点也表现出了对该项技术的同一偏好，技术在具体利用过程中会倾向于选择系统进程，以及较为常见的第三方进程。

DLL Hijacking			
MuddyWater	1月	GoogleUpdate.exe	https://www.picussecurity.com/resource/blog/ttp-ioc-used-by-muddywater-apt-group-attacks
	...		
APT29	4月	jucheck.exe	https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns
	7月	OneDriveUpdater.exe	https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/
	...		
Lazarus	9月	colorcpl.exe	https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/
	10月	wsmprovhost.exe	https://asec.ahnlab.com/en/39828/
	...		
...			

技术原理分析

实际上，将此技术放到历史的多个时间节点里，都可以称得上热点技术，安全研究员们长期以来也对此场景有着高度关注。但归根结底，该项技术主要是其套上的合法外壳给防御检测带来了较大困扰。单从技术本身来讲，其仍旧暴露出许多可疑特征，这些特征将为防御检测提供机会。从下图所示三个维度出发，可以更好地认识 DLL 劫持技术。



从劫持成因来看，DLL 动态链接库的加载可分为隐式链接和显示链接，当它们出现劫持漏洞时，会表现出不同的状态。隐式链接的 DLL 必须拥有其所需函数，否则就会产生“无法定位程序输入点 ... 于动态链接库 ... 上”的告警，而显示链接的 DLL 却不会。这也意味着当目标进程存在劫持漏洞时，若想要劫持的 DLL 是显示链接的载入方式，则攻击者可以直接替换 DLL，若想要劫持的 DLL 是隐式链接的载入方式，则必须做代理转发或伪造导出函数。

从劫持方式来看，可将其从整体上分为直接替换、代理劫持和篡改劫持三种方式。其中直接替换是指使用恶意 DLL 直接替换掉原本的 DLL 文件。代理劫持在它的基础上会通过代理转发的方式载入原本 DLL 以保证程序正常运行，这会使得载入的某一 DLL 的名称与另一 DLL 的原始文件名相同。而篡改劫持是指对原本 DLL 进行修改以植入恶意代码，此操作会导致原本 DLL 的属性更改，如签名失效。

从劫持目标上来看，针对系统进程的劫持可能会伴随着系统进程加载目录异常等特征，且不会载入第三方 DLL，而针对第三方进程的劫持也常伴随着文件投递等行为。

综合上述三个维度的各项可疑点，即可获得行之有效的猎捕检测策略，这些策略有助于我们发现绝大部分使用 DLL 劫持技术的攻击活动。

BYOVD/泄露证书

演变过程

纵观历史攻击活动，攻击者通常有两种方式入侵 Windows 内核，分别是使用带漏洞的驱动程序和使用泄露的数字证书签发恶意驱动，如下图所示。但是，无论采用哪种入侵方式，想要在内核中植入恶意代码并不是一件易事。

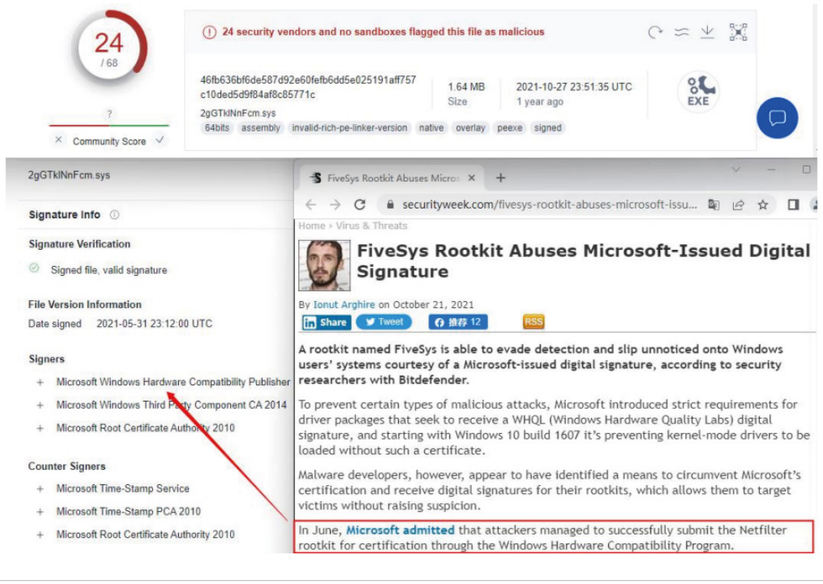
长期以来，这类技术也大多仅被类似于方程式组织这样的顶级 APT 组织所使用。但近来源于各类情报的不断公开和工程化的开源项目，这类技术也正逐步演变为一种常见且通用的攻击技术手段。

下图展示了 2022 年以来使用 BYOVD 技术的部分 APT 攻击和勒索攻击的实战案例。历史上该技术通常被 APT 组织用以绕过Windows驱动程序签名强制执行(DSE),从而在内核中部署恶意代码。但现在,攻击者在技术所用目标的倾向上有所偏移,通常为借助带有漏洞的合法驱动程序来致盲 / 杀死终端安全软件。

2022年部分驱动漏洞利用案例

5月	avoslocker(勒索攻击)	致盲/杀死 AV/EDR	https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-disable-anti-Virus-scans-log4shell.html
8月	Rever(勒索攻击)	致盲/杀死 AV/EDR	https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html
9月	Lazarus(APT攻击)	致盲/杀死 AV/EDR	https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium
10月	BlackByte(勒索攻击)	致盲/杀死 AV/EDR	https://news.sophos.com/en-us/2022/10/04/blackbyte-ransomware-returns

当然，BYOVD 技术并不是攻击者入侵内核的唯一选择。虽然从 Windows10 1607 版本开始，微软更新了对于驱动程序的签名验证机制，但 2015/7/29 时间节点之前所颁发的微软内核代码签名交叉证书签发的驱动仍被内核所接受，这意味着部分泄露证书将持续有效，且即便驱动被交由 Dev Port 进行认证，也难免错误签发。



应对策略

微软表示此技术作为 APT 和勒索组织的惯用伎俩，他们将会进一步强化对此场景的防护能力，解决 "vulnerable driver" 列表的更新问题，并从 Win11 2022 开始默认启动黑名单。

下图展示了微软对于 Vlun_Driver 的防护规则，主要通过文件 Hash 来封堵。这将产生一定效果，但并不是完全保险的，因为文件 HASH 可在不破坏签名的情况下改变，原理可参考 BlackHat 议题：《Certificate Bypass: Hiding and Executing Malware from a Digitally Signed Executable》。

```
<FileRules>
   <FileRules>
    <Allow ID="ID_ALLOW_ALL_1" FriendlyName="" FileName="*" />
    <Allow ID="ID_ALLOW_ALL_2" FriendlyName="" FileName="*" />
    <Deny ID="ID_DENY_AGENT64_SHA1" FriendlyName="Agent64\05f052_4045ae_694848_8cb62c_b1d962 Hash Sha1"
Hash="94F7575A6BB378D0CF85B3DC65941C95415E7A80" />
    <Deny ID="ID_DENY_AGENT64_SHA256" FriendlyName="Agent64\05f052_4045ae_694848_8cb62c_b1d962 Hash Sha256"
Hash="3BC0CEC99DCE687304DAD8F7A6DAF772E695CBD0169D346D03AE12500361A1E8" />
    <Deny ID="ID_DENY_AGENT64_SHA1_PAGE" FriendlyName="Agent64\05f052_4045ae_694848_8cb62c_b1d962 Hash Page Sha1"
Hash="E083142033C9653977D319B3DF4D2DE369756138" />
    <Deny ID="ID_DENY_AGENT64_SHA256_PAGE" FriendlyName="Agent64\05f052_4045ae_694848_8cb62c_b1d962 Hash Page
Sha256" Hash="68EFBAB6FEADAB076DC97DB359A287193C51199742F92E07B60417F093040FED" />
    ...
  </FileRules>
```

与之相对应的，微软对于泄露证书的封堵策略如下，其中 CertRoot 的 Vlaue 值由 CERT_SIGNATURE_HASH_PROP_ID 所指定。

XML 复制

```
<Signer ID="ID_SIGNER_S_XXXXX" Name="Microsoft Code Signing PCA 2011">
  <CertRoot Type="TBS" Value="F6F717A43AD9ABDDC8CEFDDE1C505462535E7D1307E630F9544A2D14FE8BF26E" />
  <CertPublisher Value="Microsoft Corporation" />
</Signer>
```

总的来说，考虑到 APT 组织可能会进行 0day 漏洞挖掘，以及存在潜在的未知证书泄露情况，我们可以把此攻击场景划分为基于已知黑驱动的猎捕和基于未知黑驱动的猎捕。针对已知黑驱动的场景，从情报下手能最为高效地对其进行封堵；而针对未知黑驱动的场景，亦可基于异常的驱动安装链路和 rtk 行为形成一定的猎捕检测策略。

多款C2或成“新宠”

后起之秀

APT 组织正在尝试一些新型 C2，如 APT29 于去年 5 月在真实攻击活动中使用 Sliver 替换掉了 Cobalt Strike，而今年 7 月，其又尝试了一款名为 Brute Ratel C4 的 C2 工具。

下图来源于 BRC4 的官网，从图中可以看出 BRC4 涵盖了包括直接系统调用、EDR 脱钩、睡眠混淆，以及 ETW 绕过等多种防御规避技巧。

Various Out-Of-Box Evasion Capabilities

Evasion Capabilities	x64 Support	x86 Support	x86 on Wow64 Support
Indirect System Calls	Yes	Yes	Yes
Hide Shellcode Sections in Memory	Yes	Yes	Yes
Multiple Sleeping Masking Techniques	Yes	No	No
Unhook EDR Userland Hooks and Dlls	Yes	No	No
LoadLibrary Proxy for ETW Evasion	Yes	No	No
Thread Stack Encryption	Yes	Yes	Yes
Badger Heap Encryption	Yes	Yes	Yes
Masquerade Thread Stack Frame	Yes	Yes	Yes
Hardware Breakpoint for AMSI/ETW Evasion	Yes	Yes	Yes
Reuse Virtual Memory For ETW Evasion	Yes	Yes	Yes
Reuse Existing Libraries from PEB	Yes	Yes	Yes
Secure Free Badger Heap for Volatility Evasion	Yes	Yes	Yes

当然，除 Sliver 和 BRC4 外还存在其它多种新型 C2，下图是 Nighthawk 的官方介绍，总的来说，这些 C2 都是在对现代终端安全进行深入研究之后诞生的，这使得其表现出了极强的对抗性。

Features Overview:

- Multi-operator, API driven, highly malleable native implant,
- Extensible, profile-driven, custom command-and-control in .NET,
- Advanced in-memory obfuscation and evasion strategies,
- Operationally secure post-exploitation features, optionally implemented using syscalls,
- In-process and remote process .NET assembly execution,
- Support for both x86 and x64 Beacon Object Files (BOFs),
- Token stores, keystroke loggers, screen grabbers and credential recovery,
- Much, much more.

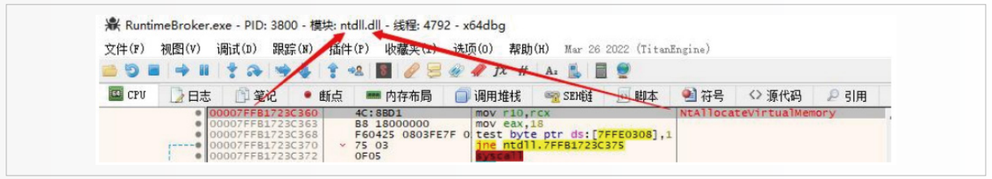
新型C2带来的挑战

考虑到新型 C2 在能力上的优秀表现，且业内还缺乏对于这些 C2 的分析研究，预测未来可能会有更多的 APT 组织在实战攻击中使用此类 C2，这也将对我们的终端安全软件提出更大的挑战。

从整体上看，依托于各类字符串、函数混淆技术、API HASH 等动态寻址技术，以及部分 C2 工具开始使用 rust、Golang 来编写，针对 APT 攻击样本静态查杀的可能性将非常小，所以内存对抗和行为对抗或将是未来的主战场。而从各类 C2 的表现来看，他们也在进一步加强这方面的对抗能力。

当然，防御者们也在密切地关注这些规避技巧，并探索相应的检测方式。值得庆幸的是，这些技巧大多并非完全无法检测的，且有可能引入新的检测点，以APT29使用的BRC4样本为例，该样本会通过Direct Syscall调用NtAllocateVirtualMemory，这致使其出现在了动态分配的内存区域。

而正常情况下，它仅应该位于 Ntdll 的内存区域。基于这个异常点，我们可以形成有效的猎捕检测策略。



上述特征在 SysWhispers3 项目中得以优化，它将通过复用其它 NT 函数的 Syscall 指令从而实现调用，这将对我们的检测策略产生误导，这个误导包括错误地判断其为正常系统调用，以及捕获到错误的函数调用序列（如攻击者正在调用 NtAllocateVirtualMemory 函数，却被误认为在进行 NtCreateFile 函数调用）。这个更新，也再次表现出了安全处于持续对抗状态的特点。

Differences with SysWhispers2

The usage is pretty similar to SysWhispers2, with the following exceptions:

- It also supports x86/WoW64
- It supports syscalls instruction replacement with an EGG (to be dynamically replaced)
- It supports direct jumps to syscalls in x86/x64 mode (in WOW64 it's almost standard)
- It supports direct jumps to random syscalls (borrowing @ElephantSeal's idea)

A better explanation of these features are better outlined i the blog post SysWhispers is dead, long live SysWhispers!

与 Direct Syscall 类似，我们也在密切关注着新型 C2 所包含的其它技术能力，并持续地在检测猎捕上进行研究投入。

被忽略的破坏性攻击

俄乌战争回顾

APT 攻击是一种有着高度针对、高度隐蔽和高度持久属性的威胁，在一般情况下，这类攻击以其先进的技术手段和极强的隐蔽能力而著称，但破坏性攻击意味着行动即暴露，所以我们往往不会将 APT 与破坏性攻击联系到一起。另一方面，破坏性攻击在很多时候也不符合其它攻击组织的利益，比如僵尸网络、挖矿木马或其它黑产攻击等，对于这些攻击的发起者来说，破坏受害者主机并不会带来任何好处，反而会迫使受害者尽可能快地响应，这也使得现今的大部分攻击都倾向于与受害者主机“和谐共生”，破坏性攻击也慢慢淡出人们的视野。

但从俄乌网络战的表现来看，破坏性攻击带来的威胁并没有消散，反而可能会在某个特定时期演变为最为频繁的攻击活动，那些平时看似与破坏性攻击相距甚远的组织，也可以随时将其行动转换为破坏性打击，特别是对基础设施的网络打击活动。

下图展示了俄乌冲突期间的网络战概况，可以看出，除开有着对军人信息这类机密数据进行窃取的 APT 间谍行为外，还表现出了大量的、类似于 DDoS 和数据擦除在内的破坏性攻击。

俄乌网络战	
1-3 月	俄乌涉及政府在内的多个官方网站遭受 DDos 攻击，造成攻击目标资源枯竭，系统崩溃等
	俄乌期间，多款破坏性恶意软件如，WhisperGate 数据擦除器， 和 SonicVote 文件加密器等被投入真实活动
	俄乌期间，发生多起数据泄露事件，包括在役军人的个人信息被窃取和披露
	……

俄乌战启发

结合常见的 APT 攻击和俄乌冲突期间的特殊表现来看，在大部分场景下，APT 攻击仍会保持其隐蔽性以满足持久化的需求，但在特定时期或动机转变的情况下，不排除会急剧演变为破坏性攻击的可能性。

对于破坏性攻击，我们需要着重防御，虽然在大部分情况下这类攻击都会是一个低概率事件，但当它发生时，很有可能铺天盖地地席卷而来，如若没有未雨绸缪，难免会陷入措手不及的被动状态。

永不落幕的钓鱼攻击

钓鱼攻击仍会有着一席之位

人作为网络安全防护中最为薄弱的环节，一直深受各大攻击组织的青睐。一方面，受限于当前非专业人员网络安全意识的普遍缺失，另一方面，考虑到针对安全人员的，有预谋、高针对性的钓鱼行动 (如 Lazarus 针对安全研究员的钓鱼攻击)，未来，钓鱼攻击仍会不断上演。

下图展示了近来较为新颖的钓鱼技巧或漏洞利用，从中不难看出，传统的钓鱼方式如文档钓鱼仍在发生，新的钓鱼技巧也层出不穷，极具迷惑性。另外，部分攻击开始以邮件服务器为目标，一方面邮件服务器可能有着攻击者感兴趣的情报，另一方面攻击者也可以借助邮件服务器进一步扩大攻击面，这或许值得我们重视。

钓鱼攻击	
技巧	利用 ms-appinstaller 进行钓鱼，以安装恶意程序
	利用 Google Docs 评论功能进行钓鱼，发件人地址为谷歌官方邮箱
	Browser In The Bopwser (BITB) 钓鱼攻击，, 钓鱼网站和真实网站完全一致
	……
漏洞	CVE-2022-30190, 文档漏洞
	CVE-2022-41040，CVE-2022-41082，Microsoft Exchange Server 漏洞
	……

钓鱼攻击防范

一方面，对于钓鱼攻击我们仍需加强安全意识培训和常见钓鱼方式的普及，尽可能地让非专业人员在遭受钓鱼攻击时也能具备一定的辨别能力并联系相应团队及时处置。

另一方面，部分钓鱼技巧的产生是产品为了提高用户体验，在进行功能设计时产生的新的利用点。出于安全性考虑，在产品进行设计时应该尽可能规避这些风险点，如果最终确认有新的风险点产生，终端安全软件作为用户的最后一道防线也应该尽快跟进检测防御，以确保其安全性。

当然，漏洞在钓鱼攻击中也表现出一定特点，如文档漏洞常常被钓鱼攻击所使用。近来，邮件服务器漏洞频出也表现出了攻击者对其的关注度，加强对此类漏洞的防范和维护有助于我们阻止钓鱼攻击。

攻击事件视角

犯罪团伙忽视内部风险：Conti组织内部数据泄露曝光事件

关键词 Conti、Ransomware

Conti 勒索软件于 2020 年 2 月左右首次被发现，其使用勒索软件即服务（RaaS）攻击模型运作，与下属分支机构合作，购买已受控主机后便开始后续的数据加密 + 数据泄露双重勒索行动，对全球上千名受害者实施了勒索攻击，受害者支付的赎金截至 2022 年 1 月累计已高达 15 亿美元。

Conti 组织的网络渗透培训手册曾于 2021 年 8 月被下属分支机构曝光，也揭示了 Conti 组织一部分关于如何渗透目标网络、使用网络渗透工具、使用勒索软件加密器等攻击手法，为安全研究员分析其惯用的攻击手法以及如何在企业内部署防御措施方面给予了一定的攻击视角思路和借鉴。

名称	大小
bot	531 903
injector	196 596
management	31 916
misc	36 024
modules	359 374
быстрый старт исследователя.txt	109 028
быстрый старт хакера.txt	30 953
дух старой школы.txt	3 145
скоростные вычисления.txt	13 584

此前泄露的 Conti 组织技术手册

在 2022 年 2 月末，某自称安全研究员的推特账号截图发文称其获取了 Conti 组织内部基础设施网络的访问权限，并分多次发帖公布了 Conti 组织及其他关联合作犯罪团伙之间两年内的俄语聊天记录、屏幕截图、网络渗透工具集，以及 Conti 勒索软件的源代码。经全球安全研究员积极地深入挖掘协同分析，Conti 组织泄露的一系列内部聊天日志揭示了 Conti 组织的人员规模、组织层次结构、业务运营模式等详细信息。

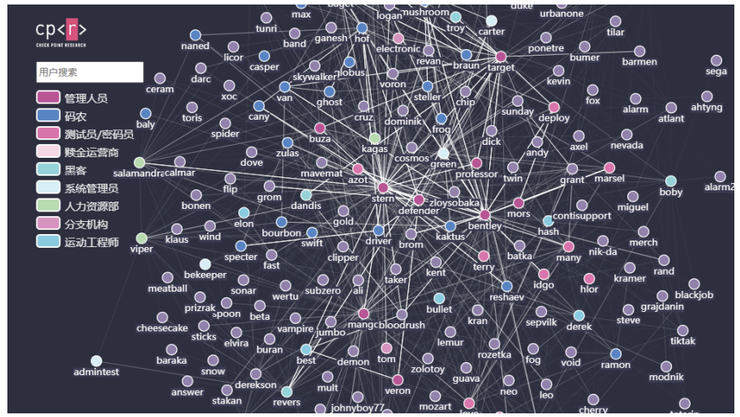
vx-underground

Directory: Conti/

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Documentation Leak.7z	234714	2022-03-01 05:29:38
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1160294	2022-03-02 13:10:39
Conti Locker Leak.7z	6852466	2022-03-05 04:29:03
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Source Code Version 3.7z	619761	2022-03-20 09:34:51
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Conti Trickbot Leaks.7z	955850	2022-03-01 06:52:40
Training Material Leak	0	1969-12-31 18:00:00

Conti 组织内部数据泄露内容

Conti 组织内部的运作方式类似于一家普通的网络科技公司。根据 Check Point 公司的 Conti 泄露分析报告，Conti 组织组织层次结构中拥有清晰的管理、财务和人力资源职能部门，以及线下办公场所、完整的招聘流程、薪酬支付流程等。团队领导和部门负责招聘网络渗透人员、网络渗透工具研发、网络渗透培训和进行网络渗透，每位团队领导会向高层管理人员报告各团队的工作进展。



Check Point 根据聊天日志绘制的 Conti 组织人员关系图

此次泄露事件过后，2022 年 5 月，Conti 勒索软件组织官网“Conti News”页面被关闭，随之 Conti 组织其他的勒索服务站点、服务器也被悉数关闭或重置，代表“Conti”的勒索软件品牌已经落下帷幕。但是根据已公开的勒索软件关联分析情况，其背后的组织者本身并未就此收手，而是在经历人员重组后重新成立其他勒索运营机构。勒索软件团体层出不穷，全球企业仍要在运营流程中加强安全控制措施。

参考资料

- https://www.cnbc.com/2022/04/14/conti-ransomware-leak-shows-group-operates-like-normal-tech-company.html
- https://www.trellix.com/en-gb/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html
- https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru
- https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/
- https://flashpoint.io/blog/history-of-conti-ransomware/
- https://share.vx-underground.org/Conti/
- https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
- https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/
- 泄露时间线：https://www.malwarebytes.com/blog/threat-intelligence/2022/03/the-conti-ransomware-leaks
- https://malpedia.caad.fkie.fraunhofer.de/details/win.conti

这个木马有点粗心：Patchwork组织自曝式“远控”了自己

关键词 Patchwork

Patchwork 组织（又称摩诃草、白象）最早在 2013 年由 Norman 安全公司曝光，是一个疑似来源于南亚某国的 APT 组织。该组织主要对巴基斯坦、中国、孟加拉国等国和其他中东和东南亚各国展开攻击，以窃取政府机构、国防机构、科研教育、医疗体系等领域机密信息为主要目的。

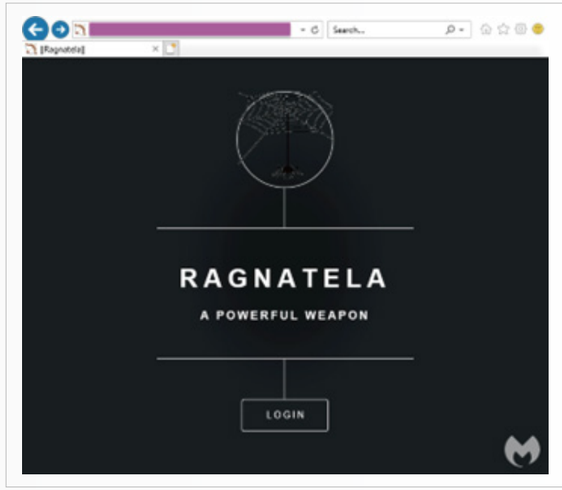
从攻击技巧看，历年来 Patchwork 最常使用鱼叉式网络钓鱼攻击投递恶意漏洞利用文档、VBA 宏代码文档作为主要打点方式，也有尝试使用水坑攻击、鱼叉钓鱼链接等进行打点攻击的手段。为提升攻击成功率，Patchwork 在持续提升其社会工程学能力，包括应对不同的攻击场景，使用当前时事热点话题来制定不同的精准钓鱼诱饵，针对特定目标人群实施定向攻击。

根据 2013 年国外安全公司 Norman 对 Patchwork 组织的分析报告，在 Patchwork 早期的攻击行动“Operation HANGOVER”中，Norman 通过挪威 CERT 公布的 IOCs 进行深入挖掘，发现这是一个疑似起源于南亚某国的 APT 组织，其目的主要是监视国家安全利益目标（例如巴基斯坦、中国），除此之外还针对了挪威电信公司 Telenor 和其他民用公司，实施了一系列工业间谍活动。

在 2016 年，国外安全公司 Forcepoint 揭露了 Patchwork 组织的另一场大范围的攻击行动“Operation MONSOON”，有许多特征标明了 MONSOON 背后的攻击者与 HANGOVER 很可能是同一个组织，这些特征包括攻击使用相同的基础设施、类似的 TTPs、相似的攻击目标和受害者群体以及基础设施疑似关联到印度的地理位置特征。

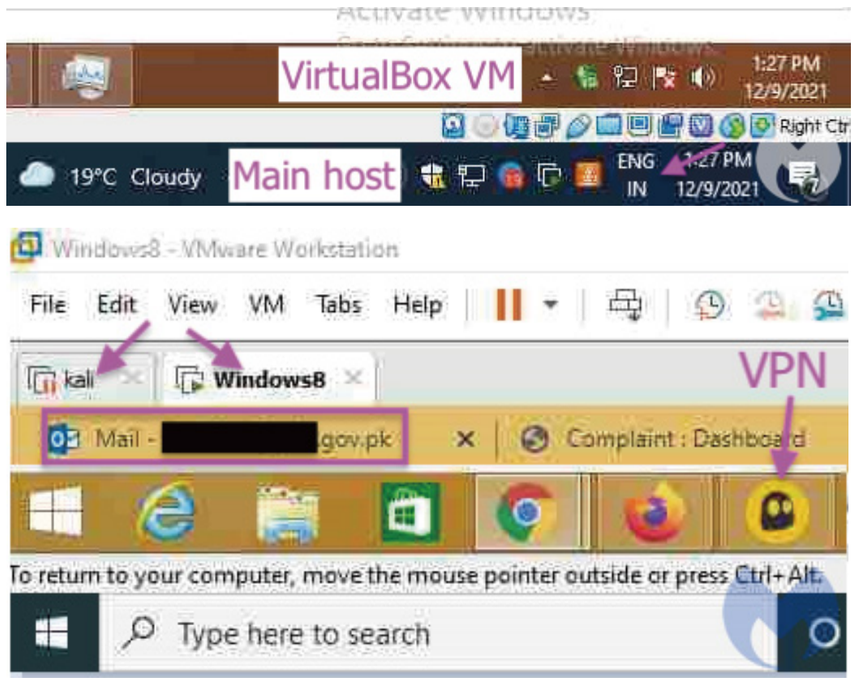
2022 年 1 月，MalwareBytes 威胁情报团队公开了 Patchwork 组织的溯源调查结果，该组织在 2021 年 12 月针对巴基斯坦分子医学和生物科学研究人员的一次攻击行动中，一台攻击者实际使用的物理机器不小心感染了本次行动的 BADNEWS 后门木马，并将这台机器的屏幕截图、键盘记录等信息上传到了攻击者自己搭建的 C&C 服务器。同时，攻击者疑似在 11 月，攻击活动开始前或攻击前期，在虚拟机中编译、调试和测试自己的攻击载荷是否正常运行。

MalwareBytes 团队成功捕获了攻击者自己的计算机和虚拟机的键盘记录和屏幕截图等信息，猜测 MalwareBytes 团队已经获得了攻击者 C&C 服务器的操作权限，能够登录到 BADNEWS 后门木马的 Web 操作控制台，如下图所示：



BADNEWS 后门控制面板“Ragnatela”

在后门控制台上，MalwareBytes 团队观测到了 Patchwork 组织在此次行动中攻击成功的受害者主要来自巴基斯坦地区。通过 BADNEWS 后门上传的受害者屏幕截图可以发现，攻击者同时运行 VirtualBox 和 VMWare 虚拟机来进行 Web 开发和测试，其物理主机使用了英语和印度语的双键盘布局。从 MalwareBytes 公布的溯源过程来看，Patchwork APT 组织会利用虚拟机并配合 VPN 来开发、推送更新和从受害者机器上搜集信息。



Patchwork 组织的一名攻击者使用的虚拟机

在 2022 年，Patchwork 的攻击重心依旧在巴基斯坦、中国等亚洲地区的相关国，主要针对政府、国防、医疗等领域的特定目标进行鱼叉钓鱼攻击，攻击手法上依旧以目标群体关注的时事热点话题来制作钓鱼诱饵，实施鱼叉钓鱼攻击为主。总体上来说，Patchwork 组织多年来使用的攻击技术并不复杂，但是为了最终能够达到成功窃密的目的，Patchwork 组织也在不断利用时事热点以及目标群体可能高度感兴趣的主题去构造一些精准鱼叉钓鱼文件。“技术简单粗暴、攻击卓有成效”的运作模式也是该组织这么多年来依旧活跃的原因之一。

参考资料

- https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/
- https://malpedia.caad.fkie.fraunhofer.de/actor/quilted_tiger

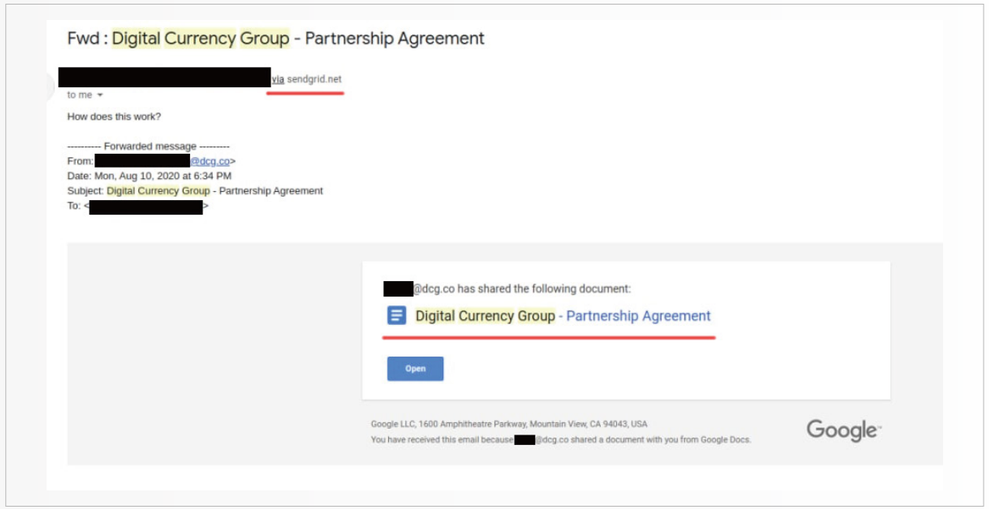
社工+漏洞两手抓：Lazarus组织对全球机构情报的贪婪觊觎

关键词 Lazarus、phishing、log4j

Lazarus 组织（也称为拉撒路、APT38）最早可追溯到 2009 年，其攻击目标主要是全球范围内的金融机构、银行、加密货币、证券、IT 等行业，出于网络经济犯罪动机对这些行业目标进行选定和侦察，通过社会工程学或基于漏洞利用方式的网络渗透攻击对目标系统进行初始打点，在了解其目标内部系统后便会窃取有经济价值的数据或数字货币。

Lazarus 组织在 2022 年仍旧十分活跃，持续使用专有网络渗透工具集，配合其独特的攻击技术和战术为全球组织带来高级持续性威胁。在今年，Lazarus 最常使用的鱼叉式网络钓鱼诱饵类型是以工作或企业招聘需求为原型设计的伪装木马，使用远程模板注入技术和携带 VBA 宏代码的诱饵文档，或是携带了加密 pdf 文档的伪装成打开密码 .txt.lnk 文件的压缩包，还有可能是经过篡改或捆绑木马的合法软件，在社交或招聘平台上配合精湛的社会工程学话术骗取受害者的信任，从而使受害者打开诱饵并安装恶意软件。

2022 年 1 月，安全厂商卡巴斯基报道了疑似为 Lazarus 攻击者组织中的一个单位 BlueNoroff 对加密货币行业进行的攻击，其使用的社会工程学规模、网络基础设施、恶意软件和漏洞利用能力等都揭示着 Lazarus 组织背后的庞大资源集合。在此轮攻击中，BlueNoroff 会伪装成其他数字货币或投资公司的管理人员，使用冒充的社交媒体帐户和电子邮件对受害者进行信任欺骗，诱使受害者打开攻击者发送的钓鱼诱饵。这种社会工程学攻击的成本远远小于使用 0day 或 nday 漏洞对目标系统进行直接攻击，并且攻击成功率会更高。在受害者系统失陷后，攻击者会对目标进行长期监控并制定金融盗窃策略，比如篡改加密货币钱包浏览器组件的交易流程以盗取受害者的加密货币。在 2022 年 3 月，卡巴斯基揭露了 Lazarus 组织使用的捆绑了后门木马的 DeFi Wallet 加密货币钱包程序，通过鱼叉式网络钓鱼电子邮件或通过社交媒体联系受害者进行攻击载荷投递，这同样展示了近两年 Lazarus 组织对于加密货币在内的金融行业的浓厚兴趣。



Lazarus 组织社会工程学邮件案例

在漏洞利用方面，Lazarus 也拥有着与时俱进的高可利用漏洞积累能力。2022 年 9 月，Cisco Talos 威胁情报团队观测到 Lazarus 组织在 2022 年 2 月至 2022 年 7 月期间使用的三款专有远程控制木马 VSingle、YamaBot、MagicRAT，部署于 VMware Horizon 产品上，Log4Shell 漏洞利用成功之后的初步立足阶段。同年 9 月，ESET Security 安全研究人员发现并分析了 Lazarus 组织在 2021 年秋季攻击行动中使用的一组恶意软件，其中记录了 Lazarus 首次滥用戴尔 DBUtil 驱动程序漏洞 CVE-2021-21551，利用该漏洞以禁用受感染机器上的终端安全软件监控。2022 年 10 月 AhnLab 公司报道称，Lazarus 组织首先会利用 INISAFECrossWebEX 服务漏洞制造水坑攻击场景来分发 Lazarus 后门木马，通过水坑攻击成功进入目标系统后，会利用 Dream Security 公司 MagicLine4NX 产品的缓冲区溢出漏洞 CVE-2021-26606 进一步黑入受害者的内网系统，同时利用该漏洞在受害主机上植入 RootKit，配合 BYOVD 技术使用存在漏洞的第三方驱动程序来禁用系统的安全产品。

参考资料

- https://mp.weixin.qq.com/s/HWJF_9yKCYIjmAfwjU2ehg
- https://mp.weixin.qq.com/s/w-KF5HUNe8-KlmFl6zLkZw
- https://malpedia.caad.fkie.fraunhofer.de/actor/lazarus_group
- https://candid.technology/lazarus-apt38-north-korea-profile-history-2014-2022/
- https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
- https://securelist.com/lazarus-trojanized-defi-app/106195/
- https://research.nccgroup.com/2022/05/05/north-koreas-lazarus-and-their-initial-access-trade-craft-using-social-media-and-social-engineering/
- https://blog.talosintelligence.com/lazarus-three-rats/
- https://blog.talosintelligence.com/lazarus-magicrat/
- https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/
- https://asec.ahnlab.com/ko/40495/

赛博空间的无硝烟暗战：俄乌冲突下的网络情报刺探行动

关键词 APT28、APT29、Gamaredon

2022 年年初，俄罗斯和乌克兰之间的地缘政治紧张局势急剧升级，随之而来的是双方黑客针对彼此政府网站的一系列网络攻击行动，许多政府网站遭到破坏或遭受了 DDoS 攻击无法访问，其动机是打击并破坏重要信息系统基础设施的可用性。在此期间，包括 APT28、APT29、Gamaredon 在内的多个 APT 组织活跃程度有明显增加。

APT28（也被称为 Fancy Bear、Sofacy Group）组织可能自 2007 年开始运作，主要针对目标为西方国家的政府、国防、军队、能源、航空以及媒体等行业，近年来的攻击行动也波及到了亚洲地区。2022 年 5 月，谷歌 TAG 团队观测到 APT28 组织的活动样本，通过钓鱼电子邮件分发内含浏览器窃密程序的加密 ZIP 附件。同在 5 月，APT28 组织使用网络钓鱼活动传播 CredoMap_v2 恶意软件进行网络攻击的活动被披露，2022 年 6 月，MalwareBytes 发现了 APT28 组织设计的一份利用 Follina（CVE-2022-30190）漏洞的钓鱼文档，该文档同样会在宿主机上运行浏览器窃密程序。

APT29（也称为 Cozy Bear、The Dukes）至少从 2008 年开始活跃，主要目标为西方政府和相关组织，例如政府部委和机构、政治智囊团和政府分包商，善用鱼叉攻击、水坑攻击、网络渗透、供应链攻击。从 2022 年 1 月中旬开始，Mandiant 持续监测并响应了 APT29 组织针对欧洲和西方各国外交实体的网络钓鱼活动，揭示了 APT29 对从世界各国政府获取外交情报和外交政策信息的长期兴趣。2022 年 7 月，Palo Alto 报道了 APT29 组织针对几个西方外交使团分发 EnvyScout 构建的网络钓鱼 HTML 文件，其会使用在线存储服务 DropBox 和 Google Drive 来部署 C&C 进行通信，这种使用合法云存储服务的行为能够加大基于网络流量的检测难度。

Gamaredon（也称为 Primitive Bear、Shuckworm）APT 组织最早可追溯到 2013 年，主要针对西方政府实体中的特定高价值目标群体进行鱼叉式钓鱼攻击，在目标系统中植入远控和窃密木马以窃取目标组织人员的机密文档和数据。在俄乌冲突进一步加剧后，Gamaredon 活跃度大幅度提高，其常使用的钓鱼诱饵包括远程模板注入的恶意文档、伪装文档图标的 SFX 自解压文件、恶意 LNK 下载器等。

数据擦除器病毒在俄乌冲突中尤其活跃，与以窃取机密信息为主要目的的 APT 攻击行动不同，数据擦除器主要被用于打击破坏目标系统使其机器和内网机器瘫痪，以彻底破坏信息系统的可用性。攻击者试图大范围瘫痪乌克兰的网络基础设施，在今年的俄乌冲突中，被检测到的活跃数据擦除器样本有 WhisperGate、HermeticWiper、IsaacWiper 等。

据 CrowdStrike 对历史上和俄乌冲突期间出现的多款数据擦除器的分析，数据擦除器常具有主机文件遍历、文件覆写破坏、文件删除、系统驱动破坏、主引导记录破坏等使主机数据和系统无法正常恢复的一种或多种功能，还会使用 BYOVD 技术滥用第三方驱动程序来绕过安全机制和安全防护软件的可见性和检测拦截功能。

参考资料

- https://mp.weixin.qq.com/s/TexTSGe9Jx6RIuUXf7CstA
- https://www.freebuf.com/articles/network/323392.html
- https://malpedia.caad.fkie.fraunhofer.de/actor/apt28
- https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/
- https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine
- https://cert.gov.ua/article/40106
- https://malpedia.caad.fkie.fraunhofer.de/actor/apt29
- https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns
- https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/
- https://malpedia.caad.fkie.fraunhofer.de/actor/gamaredon_group
- https://blog.talosintelligence.com/gamaredon-apt-targets-ukrainian-agencies/
- https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
- https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
- https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-2/
- https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/
- https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-4/

RaaS模式的持续性威胁：勒索软件仍是全球企业的主要威胁

关键词 RaaS、Ransomware、Conti、LockBit、BlackCat、Black Basta

勒索软件黑色产业链恶潮在近年来逐渐兴起。随着数字经济的发展，勒索软件已逐渐成为全球企业最具威胁性的组织风险，每年会给全球企业、政府单位和基础设施运营商造成数十甚至上百亿美元的经济损失。在以往的攻击模式中，一些勒索软件团体会直接选定勒索目标进行攻击，而近两年来另一些勒索软件团伙则运行流行的勒索软件即服务（以下简称 RaaS）模式。这种模式将勒索软件运营商和附属机构之间形成合作关系，附属机构能够自行购买用于实施勒索的一系列勒索软件工具包和使用教程，从而在不需要自行掌握大量工具开发能力的情况下轻松获得勒索特定组织的能力。

2022 年，各 RaaS 勒索软件组织继续频繁使用“加密 + 泄密”双重勒索模式对受害者进行威胁。勒索组织在潜入受害者网络后会对其内部网络进行横向移动并尽可能隐蔽地收集受害者敏感数据，这个过程根据受害者内部网络的复杂程度和数据价值，有可能持续数周到数月甚至更长时间。在数据窃取阶段告一段落后，勒索团体便会批量在已受控主机上运行勒索病毒对受害者数据执行加密并留下勒索信息。采用上述双重勒索方式进行攻击的方式的确卓有成效，勒索软件执行的高强度 + 长密钥加密算法会使依靠蛮力解密数据黔驴技穷，受害者迫于双重压力必须选择支付赎金解密数据，以及防止勒索团体泄露受害者不愿公开的重要数据，拒不支付赎金的情况下勒索团体便会在其运营的数据泄露站点上发布被盗的数据。

RaaS 勒索运营模式能够为想要进行勒索犯罪但自身没有勒索软件编码能力的潜在黑客提供勒索软件工具包付费购买和订阅服务，这种模式大大降低了实施勒索的技术门槛、个人风险和勒索难度。2022 年 IBM 安全数据泄露报告显示，已知的首次实施的 RaaS 模式攻击发生在 2016 年，截至 2022 年 RaaS 模式勒索攻击在所有网络安全攻击中占比已经增长到 11%，每次勒索成功会给受害企业造成平均四百多万美元的损失。根据趋势科技对 2022 年三个季度的勒索软件趋势分析报告，著名的 RaaS 运营商 LockBit、Conti 和 BlackCat 勒索组织在活跃的 RaaS 和勒索团体中处于领先地位，而 Conti 勒索软件组织在今年 5 月份停止运营后以新的 Black Basta 和 Karakurt 勒索软件品牌重出江湖，其涉及的非法获利十分丰厚。

其中值得注意的是，LockBit 3.0 勒索软件于 2022 年第四季度推出，与此同时 LockBit 勒索软件团体还首创性地推出了勒索软件漏洞赏金概念。其运作方式与产品漏洞众测概念类似，对发现 LockBit 组织基础设施网络和勒索工具集中的漏洞的安全研究人员或黑客提供高达 100 万美元的奖金。今年上半年的 Conti 勒索组织内部数据泄露并被迫停运事件为其他勒索软件团体敲响了警钟，LockBit 此举也印证了 RaaS 勒索软件团体在今后实施勒索攻击行动的同时，也会更加愿意投入部分非法营收到组织安全控制措施的建设中，目的是保护组织自身和附属机构成员、网络基础设施和敏感数据的安全。

参考资料

- https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022
- https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-and-black-basta-are-the-most-active-raas-groups-as-victim-count-rises-ransomware-in-q2-and-q3-2022
- https://securelist.com/new-ransomware-trends-in-2022/106457/
- https://www.pingidentity.com/en/resources/cybersecurity-fundamentals/threats/ransomware-as-a-service-raas.html
- https://www.ibm.com/security/data-breach
- https://www.techrepublic.com/article/lockbit-ransomware-bounty/

从CobaltStrike到NightHawk：后渗透利用框架未来何去何从

关键词 Cobalt Strike、Brute Ratel C4、Sliver、Nighthawk

通过利用漏洞或网络钓鱼等方式成功在目标系统建立初始立足点之后，攻击者会在受害者系统中安装一种或多种后渗透利用工具集，以便于在主机上实现更多的可扩展远程控制功能。2022 年最被全球红队和黑客青睐的后渗透利用框架仍是 Cobalt Strike。Cobalt Strike 本来是商业化的攻击模拟和红队渗透测试工具，具有功能丰富、可扩展性良好、高度可定制化等优点，在其源代码遭到泄露后已经为全球 APT 及热门威胁组织所热衷使用。

由于越来越多的威胁组织在攻击行动中使用 Cobalt Strike 框架，各大厂商的网络安全解决方案也积极开发了对 Cobalt Strike 框架的检测能力。这种“猫捉老鼠”的游戏持续上演，迫使攻击者在继续魔改 Cobalt Strike 框架以绕过安全产品，和更换更为小众、隐蔽且能绕过最新版本安全产品的后渗透利用框架这两条路中做出抉择。在 2022 年，一部分网络威胁组织和红队人员已在探索并投入使用除 Cobalt Strike 以外的其他几款各具特点的后渗透利用框架。

Sliver 于 2019 年底由网络安全公司 BishopFox 首次公开，是一个基于 Go 的开源跨平台后渗透利用框架，支持可扩展的、自定义后门程序生成，支持多种回调协议和其他可用选项，但 Sliver 框架本身并没有在反病毒软件规避方面制定策略，比较依赖加壳、加密、多阶段调用等常用免杀技术实现反病毒程序绕过。2022 年 8 月，微软观察到已经有包括 APT 及勒索软件犯罪集团在内的威胁行为团体在其攻击行动中将 Sliver 框架和 Cobalt Strike 一起投入使用，或直接使用 Sliver 替代 Cobalt Strike 以来控制目标系统，例如 RaaS 勒索团伙 DEV-0237（又称为 FIN12）和 Bumblebee 恶意软件团伙。各团伙正在考虑是否从 Cobalt Strike 转变为包括 Sliver 框架在内的开源后渗透利用框架，这些足够新颖且具备高度可定制化属性的后渗透工具集，能够降低受害者和安全软件发现其持久化隐蔽行动的可能性。

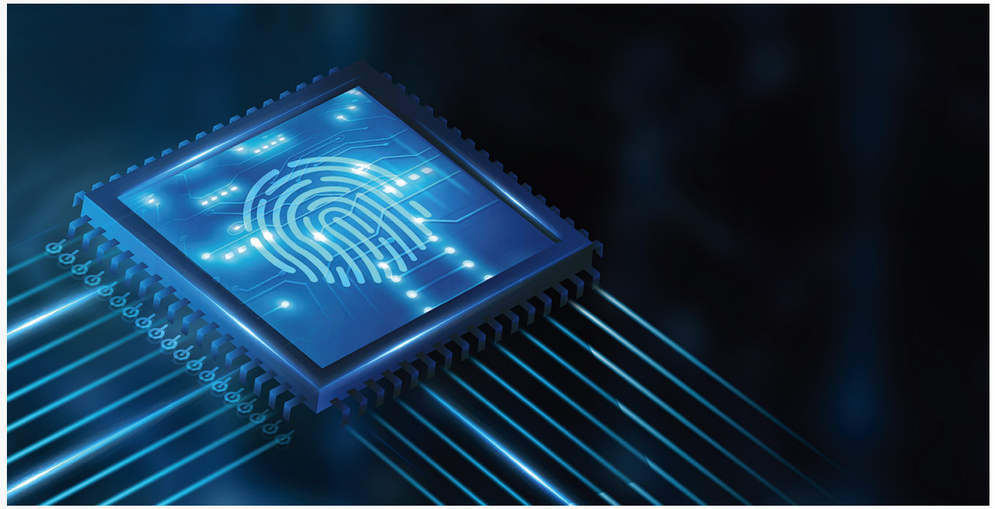
Brute Ratel C4（以下简称 BRC4）是由 Mandiant 和 CrowdStrike 的前红队成员 Chetan Nayak 于 2020 年 12 月创建的商业化攻击模拟工具包，其在终端检测响应、反病毒软件对抗、系统日志记录机制绕过等恶意软件隐蔽性方面具有不俗的能力。此后，BRC4 被破解，并在地下黑客论坛中免费传播，很快就有已知的 APT 及热门威胁组织将 BRC4 加入自己的攻击武器库。2022 年 7 月，Unit42 团队追踪到了一起具有俄罗斯背景的 APT29 组织使用 EnvyScout 打包攻击载荷的诱饵文件，其在目标系统中安装 BRC4 框架生成的定制化 Badger。2022 年 10 月，趋势科技公布了 Black Basta 勒索软件团伙在渗透目标组织的过程中，通过 QAKBOT 恶意软件建立初始连接后部署 BRC4 和 Cobalt Strike 框架对目标系统进行渗透和横向移动的案例。

Nighthawk 框架由一家名为 MDSec 的公司于 2021 年 12 月推出，为红队提供商业化的网络攻击模拟工具集，植入程序具有强大的安全防护规避、高可定制化等原生功能。2022 年 11 月，Proofpoint 研究人员观察到可能的红队人员，在 2022 年 9 月首次使用 Nighthawk 框架实施渗透测试。截至目前，并没有观测到其他在野的威胁团队投入使用，目前也尚未观察到 Nighthawk 已被黑客破解并传播。由此可见，Nighthawk 与其他后渗透利用框架 CobaltStrike、Sliver 和 BRC4 框架一样，其具有的安全软件绕过技术和其在渗透测试业界的相对未知性，是全球威胁组织试图破解并将其加入自己武器库的迫切需求。

种种网络攻击案例和恶意软件趋势表明，APT 及热门威胁组织和红队未来对后渗透利用框架的功能性需求并不亚于 Cobalt Strike，同时也会寻求其他更加具备攻击隐蔽性和恶意代码免杀能力、杀软 / 沙箱对抗能力的可定制化后渗透利用框架。最关键的是得走在最新版本的安全防护产品前面，以在整个攻击行动中达到最终的目的。

参考资料

- Sliver：https://github.com/BishopFox/sliver
- Sliver：https://thehackernews.com/2022/08/cybercrime-groups-increasingly-adopting.html
- Sliver：https://www.microsoft.com/en-us/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks/
- BRC4：https://www.bleepingcomputer.com/news/security/hackers-now-sharing-cracked-brute-ratel-post-exploitation-kit-online/amp/
- BRC4：https://mp.weixin.qq.com/s/Nnag6DSf_wx2YrnTXEwNug
- BRC4：https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/
- BRC4：https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html
- Nighthawk：https://thehackernews.com/2022/11/nighthawk-likely-to-become-hackers-new.html
- Nighthawk：https://www.proofpoint.com/us/blog/threat-insight/nighthawk-and-coming-pentest-tool-likely-gain-threat-actor-notice
- Nighthawk：https://www.mdsec.co.uk/2022/11/nighthawk-with-great-power-comes-great-responsibility/
- Nighthawk：https://www.mdsec.co.uk/nighthawk/



全球APT组织视角

东亚	东南亚	南亚	东欧	北美
Lazarus	海莲花	Bitter	Gamaredon	hunt forward
Kimsuky		Patchwork	APT28	Equation Group
KONNI		Confucius	APT29	Bvp47
毒云藤		SideWinder	SandWorm	TAO
		Donot		

东亚

东亚的 APT 组织的攻击活动，在 2022 年仍较为活跃，其典型代表是 Lazarus。

Lazarus：公开情报认为该组织具有东亚某国政府背景，该组织的攻击目标遍及全球，攻击行业多种多样，包括但不限于数字货币、金融机构、IT 公司、政府机构以及军事机构等，其“初始打点”阶段主要利用社会工程技术，通过邮件、推特、领英、脸书以及 whatsapp 等社交媒体向目标发送恶意文件或链接，诱导目标执行恶意文件或引导目标至漏洞网站、虚假网站以触发对应的漏洞利用，实现恶意文件植入。

在披露的攻击活动中，Lazarus 组织在漏洞积累以及利用方面一直展现出较为先进的研究能力，曾利用 chrome 远程代码执行漏洞 CVE-2022-0609 对多国的新闻媒体、IT 基础设施服务商进行攻击。除此之外，该组织自 2021 年到 2022 年正在对合法的开源软件进行木马化，主要利用 Putty、Kitty、TightVNC 远程连接工具以及 PDF 阅读器等开源工具，插入恶意代码用于部署 ZetaNile（BLINDINGCAN）后门。

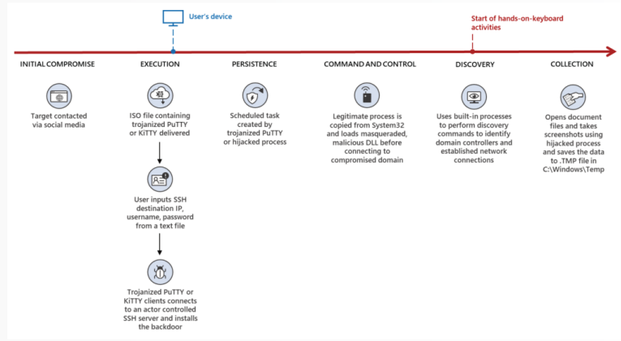


图 lazarus-01，来源于互联网

Kimsuky

该组织是比较活跃的东亚组织之一，其又名 Mystery Baby、Baby Coin、Smoke Screen、BabySahrk，据分析其可能为 2012 年开始活动的与东亚某国政府有关的 APT 组织，其与 Konni 组织疑似存在联系。

该组织的攻击手法在 2022 年并没有发生较大的变化，仍是采取发送携带“外交”、“安全”、“国防”、“朝鲜核问题”以及“统一部”等关键字的恶意附件对目标发起鱼叉攻击。

图 kimsuky-01，来源于互联网

在 2022 年披露的 Kimsuky 组织 GoldDragon 攻击小组针对半岛相关单位的攻击链中，研究人员发现其配置了多级命令和控制服务器，攻击感染链较为复杂，主要感染逻辑如下：

- 攻击者向潜在受害者发送鱼叉式网络钓鱼电子邮件。
- 如果受害者单击钓鱼链接，则会连接到第一阶段的 C2 服务器，并使用电子邮件地址作为参数。
- 第一阶段 C2 服务器验证传入的电子邮件地址参数是否符合预期，如果它在目标列表中，则传递恶意文档。第一阶段脚本还将受害者的 IP 地址转发到下一阶段服务器。
- 第二阶段 C2 服务器上的相应脚本检查从第一阶段服务器转发的 IP 地址，以检查它是否为来自同一受害者的预期请求。使用此 IP 验证方案，参与者可以验证传入请求是否来自受害者。

KONNI

KONNI 是一类木马病毒，后被发现与东亚的 APT 组织存在一定的关系，此后被当作疑似具有东亚背景的 APT 组织的标识。该组织同样利用疫情相关热点事件对亚洲多个国家进行鱼叉攻击。其外，还通过仿制 APP 针对移动平台用户开展攻击。

2022 年其攻击行动似乎并不是很活跃，主要针对目标为俄罗斯以及半岛地区相关国家，攻击方式没有多大变化，主要还是通过鱼叉攻击对相关机构进行攻击。

毒云藤

其在国内同时也被称为绿斑、穷奇、APT-C-01，该组织对我国国防、政府、科技、教育以及海事机构等重点单位和部门进行了多年的网络间谍活动，其主要关注军工、中美关系、两岸关系和海洋相关领域。

毒云藤在初始攻击环节主要采用鱼叉式钓鱼邮件攻击，在进行攻击之前，其会对目标进行深入调研，开展信息搜集。通过分析信息，仿冒国内最常使用的社交软件、邮箱系统（126、163 邮箱）、政府机构网站、军工网站、高等院校等网站进行大规模钓鱼，以此获取定向群体的精确情报。

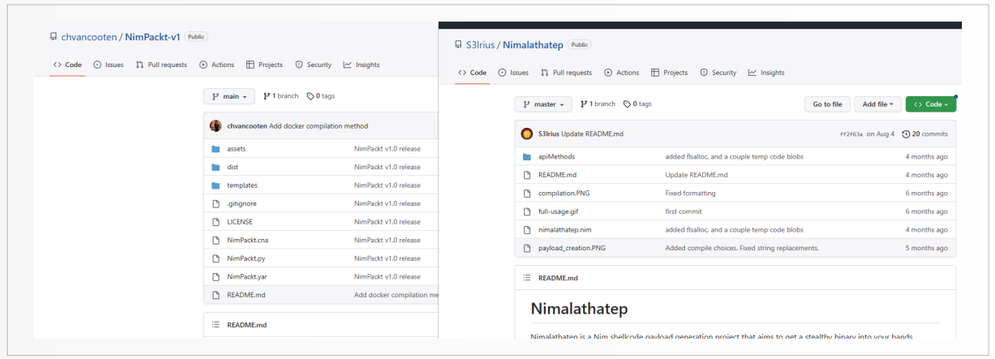
在 2022 年，该组织通过持续购买国内邮箱账号，从中筛选出具有一定价值的邮箱账号，进行扩散式钓鱼，对我国航天、海事、军队、教育、政府机构、多行业领域专家持续进行邮件钓鱼活动，下图为多次攻击活动的钓鱼邮件截图。

图毒云藤 -01

东南亚

海莲花 (OceanLotus) 是一个长期针对中国、东南亚地区国家政府、科研机构、海运企业等领域开展定向攻击的 APT 组织。

海莲花组织 2022 年在打点阶段大量使用 Nday 以及少量 0day 对目标进行攻击；在通信基础设施构建方面，大量使用被攻陷设备或网站作为其流量中转节点，外部披露其长时间运营物联网僵尸网络 Torii；在工具开发方面，除了以往使用的 C/C++ 开发木马外，2022 年开始逐步偏向使用小众语言开发实现木马功能，例如 2022 年已经在取证中发现的 nim 编写的相关木马，如使用的 NimPackt-v1 与 Nimalathatep，都是近期活跃的开源项目。除了以往攻击活动针对 x86 架构平台外，该组织对于多平台架构环境也部署植入了相关木马，以此来适应国产化趋势，例如已为 ARM 与 MIPS 架构部署植入了 Torii 木马。



在后渗透阶段，依然采用多组件执行与植入定制化恶意木马的攻击策略，避免暴露相关的攻击目标以及痕迹，阻碍分析人员的持续追踪。在最终的木马执行中，会采用无文件攻击手法并利用单个插件执行来实现特定功能，避免恶意文件落地，实现规避检测以及防止被内存扫描取证的功能。

南亚

南亚 APT 组织 2022 年处于较为活跃的状态，活跃地区主要集中在巴基斯坦与印度，包括了 BITTER、Patchwork、Confucius、SideWinder、Donot 等，这几个 APT 组织很多方面信息存在着交叉，包括但不限于基础设施、攻击手法与战术、相似样本等，不排除这 5 个组织背后存在一定关联性。

Bitter

该组织拥有多个别名，如蔓灵花、APT-C-08、T-APT-17 及苦象，该组织其主要攻击目标为亚洲国家，主要针对政府（外交、国防）、军工、核工业、航空工业、船舶工业以及海运等行业开展攻击，窃取敏感资料，疑似为南亚次大陆某国政府背景的 APT 组织，其攻击流程主要为下图。

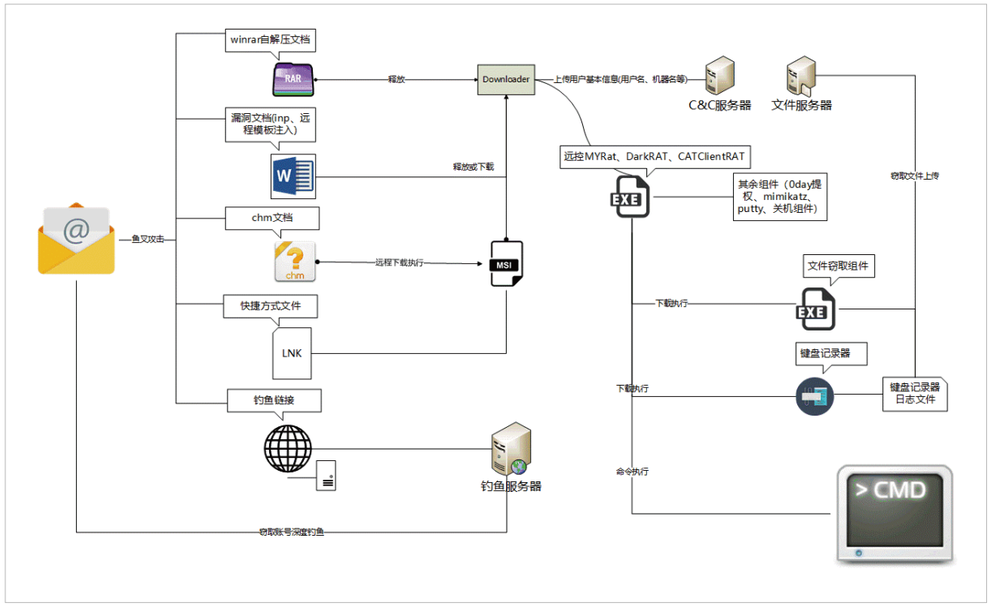


图 BITTER-01

该组织 2022 年对中国和巴基斯坦发起了多起鱼叉攻击活动，攻击目标涉及中国与巴基斯坦多个行业，整体攻击方式未发生较大改变，主要是向相关攻击目标大量发送恶意 chm 压缩包或 office 漏洞文档、宏文档作为邮件附件，并对相关目标进行钓鱼攻击以窃取对应的账号密码。另外，在分析多起攻击事件过程中，发现 BITTER 组织疑似对攻击目标国家相关 wordpress 网站进行攻击，用于托管载荷或作为控制节点。

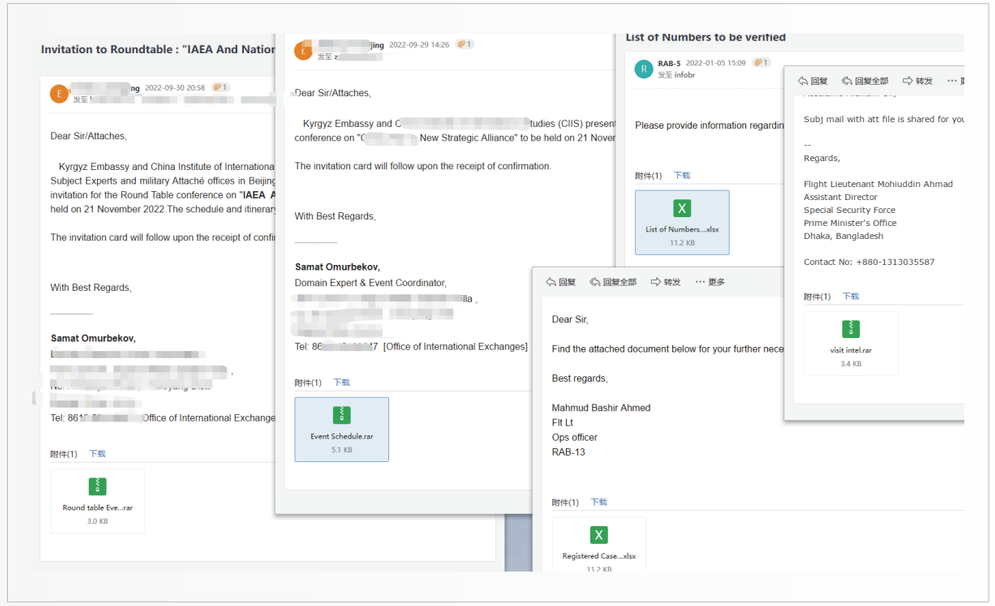


图 BITTER-02

下表为 Bitter 相关攻击事件中使用到的附件名称。

事政策分析和对南亚的港口安全影响 .chm
List of participants for Ops training.chm
20220629.doc
AGENDA POINTS FOR WORKING LEVEL MEETING BETWEEN PMSA AND CSTC.doc .chm
MoM APSCO and SUPARCO Meeting_09 Sept 2022.chm
Event Schedule.chm
Event Schedule.chm
Event Schedule.xlsx
Addl SP Hafizur Rahman.xlsx
List of Numbers to be verified.xlsx
Registered Cases List.xlsx

表 BITTER-01

Patchwork

该组织的其他名称包括 APT-C-09、白象、PatchWork、angOver、VICEROY TIGER、The Dropping Elephant 等，在 2022 年其重心与其他几个组织一样，主要聚焦于巴基斯坦。

该组织对于热点事件的敏感度很高，并且能够快速将攻击活动与热点事件结合。Patchwork APT 组织在不断扩大自己的武器库，并通过鱼叉式网络钓鱼攻击瞄准其目标，诱导目标执行恶意文件。下图为该组织 2022 年的部分鱼叉攻击文件。

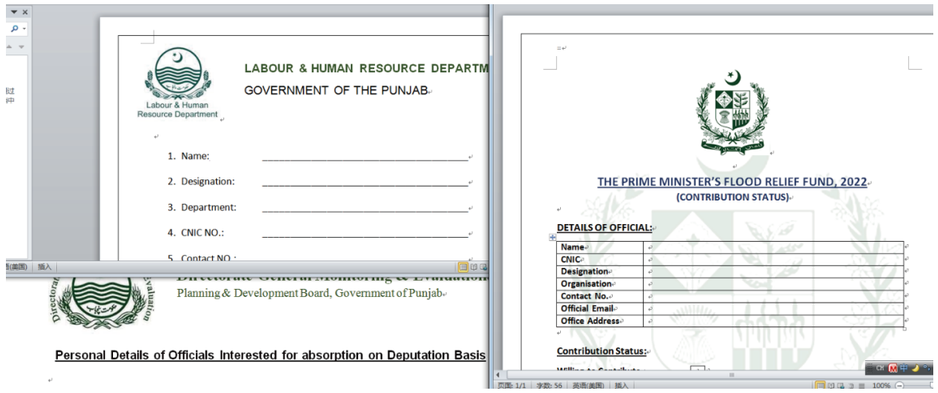


图 Patchwork-01

Confucius

该组织自 2013 年起开始活跃，同时也被国内安全厂商称为魔罗杪。其与许多其他南亚 APT 组织团伙一样，主要对中国和巴基斯坦等国的关键基础设施部门发起网络攻击，其中包括政府机构、军工企业、核工业等。

2022 年该组织使用了多种攻击手法，包括但不限于邮件结合钓鱼网站、邮件结合木马附件、单一投放木马等，其除了使用自身的特种木马外，疑似还使用了一些商业、开源木马，其投递样本基本都使用 rar 或者 zip 进行压缩。部分攻击 payload 采用诱饵宏文档，欺骗用户执行宏以便于显示隐藏内容的方式，在用户启用宏后执行初始恶意代码。通过对其攻击目标开展分析，今年其攻击涉及中国、巴基斯坦、俄罗斯、斯里兰卡以及尼泊尔等国家。下图为部分攻击事件钓鱼邮件截图。

图 Confucius-01

SideWinder

该组织其他名称为响尾蛇、T-APT-04，是一个疑似具有南亚次大陆某国政府背景的 APT 组织，该组织主要目标为巴基斯坦和东南亚国家，主要以窃取政府、能源、军事等领域的机密信息为主要目的。

该组织的攻击目标一直着重聚焦于巴基斯坦，在 2022 年其通过伪造“工作安排”、“网络安全”、“新冠信息”、“军事信息”“会议”相关话题文档或文件对东亚及南亚地区多个国家的的政府机构、外交、军事、电力、通信等部门进行鱼叉攻击。

图 sidewinder-01

该组织除了投递恶意文件之外，还大量仿冒巴基斯坦政府相关域名用于网络钓鱼攻击，安全人员将其追踪为 SideWinder.AntiBot.Script，下图为部分仿冒域名。

Phishing link	Redirect to a legitimate domain	Possible target of a phishing link
http://faujifoundation.bitlyy.me/offer-55f9918f	https://applicants.fauji.org.pk/	Mimicry of the Fauji Foundation - https://www.fauji.org.pk/
https://finance.pakgov.net/salary-a4222e91	https://www.finance.gov.pk/circulars/circular_14042022_2.pdf	Mimicry of the Ministry of Finance of Pakistan - finance.gov.pk
https://finance.govpk-mail.net/financecircular-38149cbd	https://www.finance.gov.pk/	Mimicry of the Ministry of Finance of Pakistan - finance.gov.pk
http://smstest.kdf-mail.com/147632-86182096	https://www.example.com/	Possible Kashmir Development Foundation mimicry
https://askari.bitlyy.me/offer-eaec3587	https://askaribank.com/	Mimicry of the Askari Bank - askaribank.com

图 sidewinder-02，该图来自互联网

Donot

又称肚脑虫组织（APT-C-35），是一个针对巴基斯坦、斯里兰卡等印度周边国家政府机构等领域进行网络间谍活动，以窃取敏感信息为目的的攻击组织，该组织具备针对 Windows 与 Android 双平台的攻击能力。

在 2022 年，其攻击方式与之前并无太大区别。通过鱼叉邮件的方式向目标投递远程模板注入文档或者宏文档来完成攻击活动的第一步，其主要攻击目标集中于南亚的孟家拉国、斯里兰卡、巴基斯坦以及尼泊尔等。

东欧

自 2022 年俄乌战争以来，东欧地区的 APT 组织攻击活动一直处于非常活跃的状态，主要以俄罗斯、中东、欧洲地区为主要目标，尤其是处于战争中心的俄罗斯、乌克兰和北约组织，比较活跃的组织有 Gamaredon、SandWorm、APT28 以及 APT29（WellMess）组织。

Gamaredon

也被称为 Primitive Bear 组织，该 APT 组织疑似具有东欧背景，其最早的攻击活动可以追溯到 2013 年，主要针对乌克兰政府机构官员、反对党成员和新闻工作者，以窃取情报为目的。

2022 年，Gamaredon 组织使用包含军事信息、网络安全信息类的恶意 sxf 自解压文件、html 附件、lnk 文件、远程模板文件钓鱼邮件对目标地区的政府机构、外交、军事部门进行攻击，最终下发窃密组件窃取信息，下图为部分诱饵文件内容。

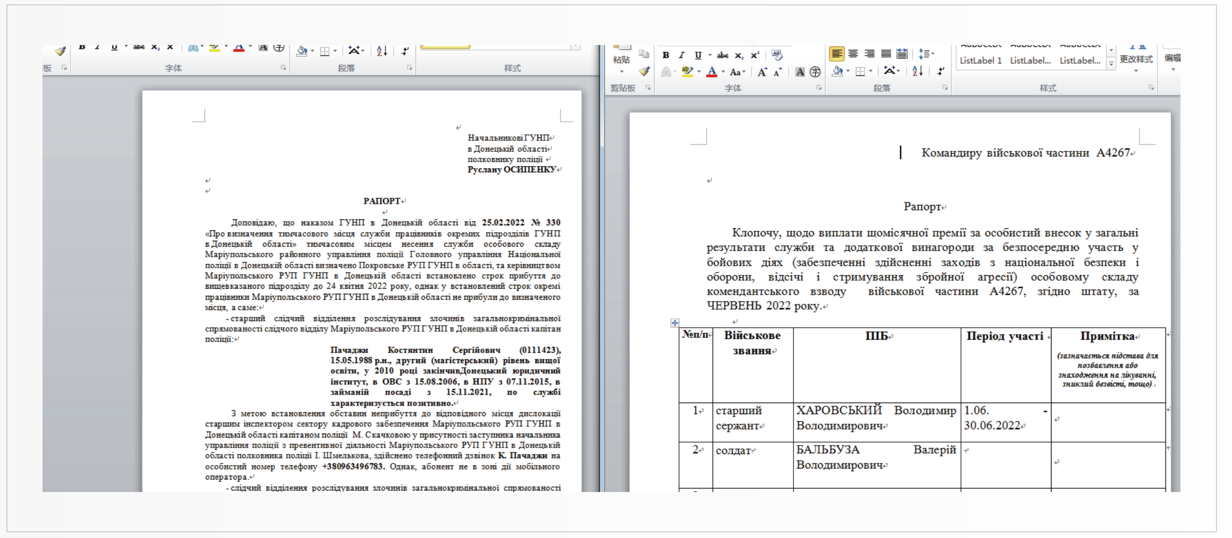
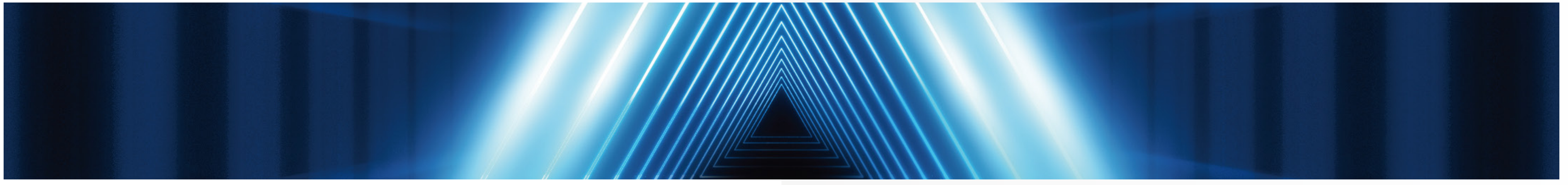


图 gamaredon-01



APT28

“奇幻熊”（Fancy Bear，T-APT-12）组织，也被称作 APT28, Pawn Storm, Sofacy Group, Sednit 或 STRONTIUM，是一个长期从事网络间谍活动的 APT 组织，从该组织的历史攻击活动可以看出，获取情报一直是该组织的主要攻击目的。据国外安全公司报道，该组织最早的攻击活动可以追溯到 2004 年至 2007 年期间。

在 2022 年，APT28 组织聚焦在乌克兰、欧洲以及北美地区，针对该地区的政府、国防、军工、能源行业进行攻击。其攻击方式多种多样，包括但不限于鱼叉攻击、网页钓鱼、漏洞攻击、DDoS 等。

APT29

该组织目前被网络安全界归因于俄罗斯政府情报组织，APT29 至少从 2008 年开始运作，具有 YTTRIUM、The Dukes、Cozy Duke、Cozy Bear、Office Monkeys 等别名，主要攻击目标为美国和东欧的一些国家。

APT29 一直是东欧地区 APT 组织中较为顶尖的，无论从微软报告的 Nobelium 事件或 SolarWinds 事件，该组织一直保持着较高的攻击能力。在 2022 年，APT29 组织持续对意大利、英国、美国等国家进行攻击，通过社会工程学或直接渗透的方式入侵目标机构，在某次攻击事件中，其使用 CVE-2022-30170 漏洞对欧洲外交实体进行攻击。

SandWorm

该组织别名“沙虫”，由 iSIGHT 于 2014 年 10 月首次发现，iSIGHT 认为该组织与俄罗斯有关，该组织使用漏洞和恶意软件对感兴趣的目标进行攻击，主要的目标包括：北大西洋公约组织、乌克兰政府组织、西欧的政府组织、能源部门（特别是波兰）、欧洲电信公司、美国学术组织等。

2022 年俄乌战争期间，SandWorm 组织被认为是 Cyclops Blink 僵尸网络的幕后操控者，对乌克兰能源设施进行攻击。作为疑似参战方，其还通过投递针对电力工控系统的恶意软件 Indystroyer2、CaddyWiper 数据擦除工具等对电力系统进行攻击，实现瘫痪基础设施的目标。

北美

在 2022 错综复杂的国际形势下，北美地区 APT 组织的网络攻击活动一直没有停止。2009 年美国创立了美国网络司令部（USCYBERCOM），在奥巴马政府的推动下，其于 2018 年升级为独立的作战指挥部，由情报机构国家安全局（NSA）局长兼任领导，这种打通情报与战略性网络行动之间界限的任命方式使全球网络空间军事化程度进一步加深。

2022 年 10 月，美国网络司令部发布纲领性文件《主宰网络领域战略》，文件将“提前防御”和“持续交战”定义为网络作战关键战略。[4]“提前防御”指预判到来自网络空间的威胁后先发制人，在对手发动攻击前完成反制，“持续交战”指除网络攻击外，综合利用信息战、电子战和认知战等现代对抗手段。值得注意的是，这是美国网络司令部和国家网络任务部队（CNMF）建立以来，首次公开具有网络打击意图的战略文件，网络军备竞赛持续加深，相关 APT 组织在全球网络空间中势必将留下更多痕迹。

美在俄乌冲突中

2022年4月5日，美国国家安全局局长兼网络司令部司令保罗·中曾根在一场听证会中透露，美方曾于21年底将“前往狩猎”（hunt forward）行动组派遣至乌克兰，6 月 1 日保罗接受英国记者采访时再次承认美国网络司令部的“网络安全专家”从 21 年 12 月起，在乌克兰驻扎达三个月，在此期间对俄罗斯进行了“进攻性和防御性网络行动以及信息情报行动”。对于这种美宣称的不介入俄乌冲突与美对俄发动网络攻击的矛盾、危险行为，外交部发言人赵立坚要求美方向国际社会做出解释。

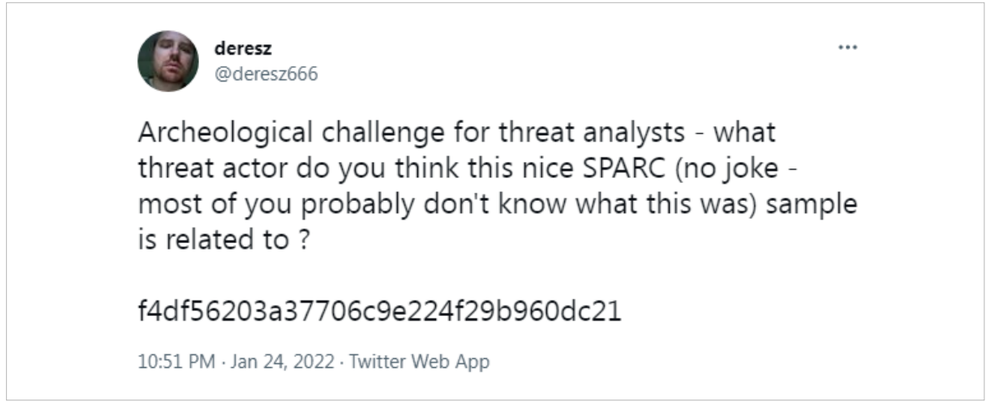
所谓“前往狩猎”行动框架 [5] 由美国网络司令部于 2018 年部署，主要指国家网络任务部队“应邀”前往他国，支持他国进行“防御性网络行动及情报行动”，同时了解对手的信息、技术、恶意程序和意图。根据美国网络司令部发布的统计数据，至 2022 年底，网络司令部已向全球 16 个国家部署过超“两打”次的“前往狩猎”行动组。

[4] http://www.81.cn/w-j/2022-11/25/content_10201501.htm

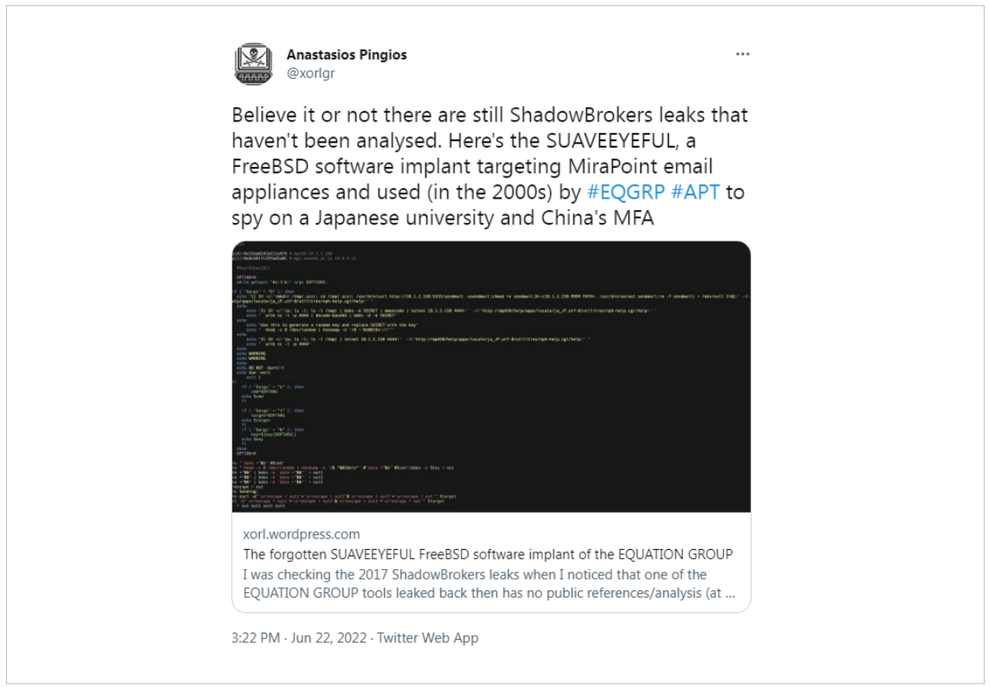
武器库分析

2022 年 1 月 24 日，一个复杂的 Solaris SPARC 恶意软件的哈希值被安全研究人员“deresz666”发布在 Twitter 上，卡巴斯基安全研究人员对其分析后认为该样本来自方程式组织（Equation Group）[6]。研究人员识别到该样本的 Windows 版本，攻击者内部称其为 SBZ，它支持多种数据窃取方式和复杂的网络寻址、路由、重定向方式以隐藏恶意行为。据分析，SBZ 很可能是方程式组织使用的 STRAITBIZZARE 工具，且 SBZ 与方程式组织此前已被披露的样本的接口 ID 存在重合。

2022 年 6 月 22 日，安全研究员“xorlgr”在推特公开了一条方程式组织曾攻击我国外交相关单位的线索 [7]。据深信服安全研究人员分析，攻击者定制化的开发了黑客工具 SUAVEEYEFUL 以攻击相关单位邮箱系统，并在后续开发攻击其他单位的恶意程序时，意外通过代码备注泄露了曾对我国相关单位进行网络攻击的计划或事实。



[5] https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/
[6] https://twitter.com/deresz666/status/1485626389407703044
[7] https://twitter.com/xorlgr/status/1539509091168669698



自 2022 年 2 月方程式组织后门“Bvp47”被公开起，国家计算机应急处理中心与国内安全厂商公开了多个顶级北美 APT 组织的黑客工具分析报告，包括“NOPEN”远控木马、“蜂巢”（HIVE）平台、“量子”（Quantum）平台、“酸狐狸”（FoxAcid）平台和“饮茶”（suctionchar）窃密工具等。随着分析细节的不断深入，越来越多针对我国的网络攻击被披露。

美国 NSA 针对西工大网络攻击事件

2022 年 6 月 22 日，西北工业大学发布《公开声明》称其遭受境外网络攻击。陕西省西安市公安局碑林分局随即发布《警情通报》，证实在西北工业大学的网络设备中发现了多款源于境外的木马样本，西安警方已对此正式立案调查。

9月5日和9月27日，国家计算机病毒应急处理中心分别发布《西北工业大学遭美国NSA网络攻击事件调查报告报告（之一）》和《报告（之二）》[8][9]，确认西工大网络安全事件的攻击活动源自美国国家安全局（NSA）下属机构“特定入侵行动办公室”（简称 TAO），TAO 近年对我国实施上万次恶意网络攻击，控制了数以万计的网络设备，窃取超过 140GB 的高价值数据。

根据美军网络司令部 2022 年 10 月发布的《网络战部队使命任务》，美国网络战部队共有 133 支小队，共 6200 余人，分布在各军种。北美地区顶级 APT 组织的活动有以下特点：

拥有领先的攻击技术和极强的攻击能力。具有国家情报机构背景的 APT 组织与网络军火商、国防承包商以及其他国家情报机构进行合作，使用定制化的工具集完成针对特定目标的网络攻击。

[8] https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm
[9] https://www.cverc.org.cn/head/zhaiyao/news20220927-NPU2.htm

具有高隐蔽的特征。这些 APT 组织掌握大量 0Day 漏洞，行动时遵循完善的 OpSec 指南，目前发现的入侵活动都可以追溯至数年前，可以推测还有大量未被披露的网络攻击正在发生。

中国一直都是其攻击目标。除了西北工业大学事件，2017 年曝光的 Vault7 中包含多个“Panda”相关的项目，这些项目以华为路由器等中国厂商的设备为攻击目标。2020 年 360 安全大脑发布的报告详细说明了与 CIA 有关的 APT 组织对中国进行至少长达 11 年的秘密渗透。

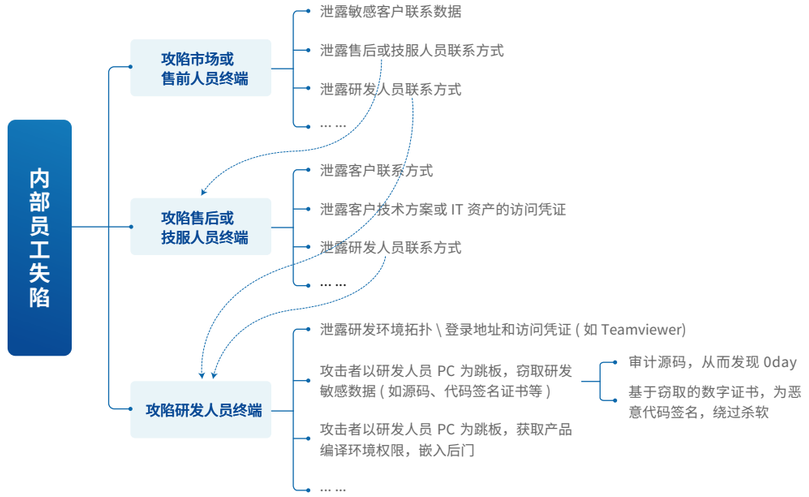
APT攻击防御视角

APT防御体系框架

基于大量已经发生的 APT 攻击事件分析，深信服安全蓝军发现攻击者获得初始落脚点的关键环节有三大类，分别是：

内部员工失陷　管理疏失的数字资产　非预期篡改的依赖组件

内部员工失陷对应的攻击场景和攻击后果：

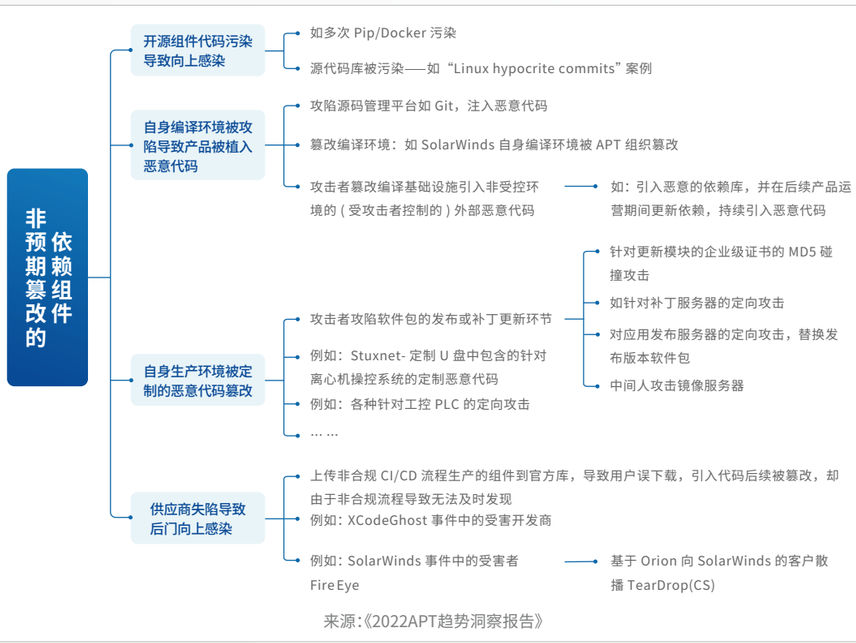


来源:《2022APT趋势洞察报告》

管理疏失的数字资产对应的攻击场景和攻击后果：

来源:《2022APT趋势洞察报告》

非预期篡改的依赖组件对应的攻击场景和攻击后果：



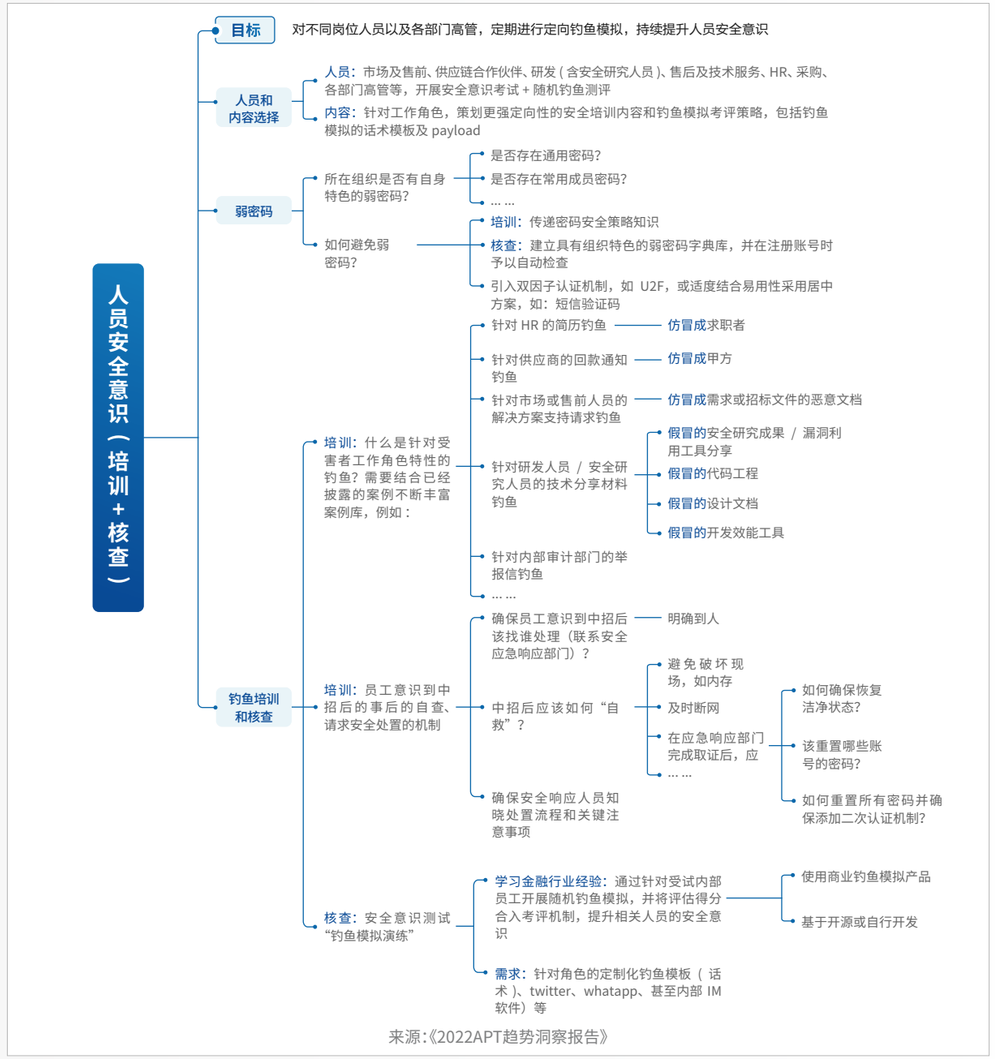
来源:《2022APT趋势洞察报告》

基于对上述三大类 APT 攻击关键落脚点的分析，深信服安全蓝军认为一个在 IT 建设时考虑应对 APT 攻击的组织需开展的安全建设应包括：人员意识安全、资产管理和保护、网域管理与安全设施部署、建立研发供应链安全机制、建立企业级安全运营和事件响应中心等，总体框架和各个模块的使命如下图。

来源:《2022APT趋势洞察报告》

人员意识安全

从大量 APT 攻击实例可见，攻击目标人员的安全意识弱点是初始落脚点中最被攻击者重视的环节之一，提高组织内人员的安全意识，是投入产出比很高的防御策略。在此，人员安全意识培训和核查的使命在于：对不同岗位人员以及各部门高管，定期进行定向钓鱼模拟，持续提升人员安全意识。



来源:《2022APT趋势洞察报告》

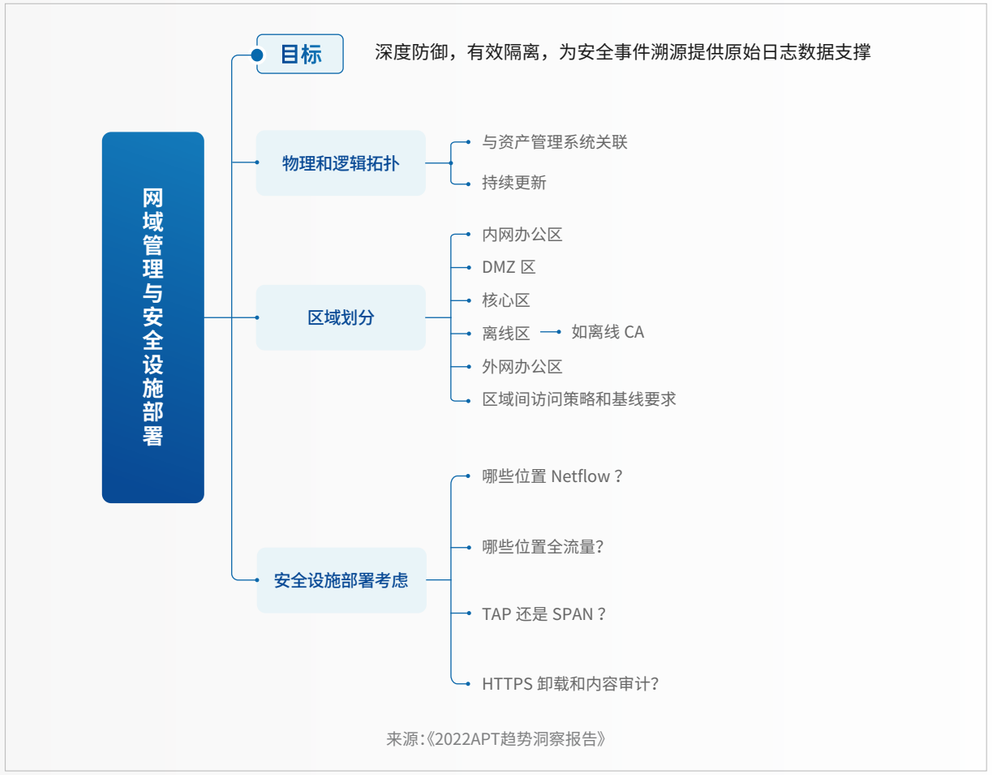
资产管理和保护

资产管理和保护的目标是：持续管理资产 - 人员 - 业务 - 脆弱性的对应关系，基于零信任理念设定资产安全隔离和准入策略，推动漏洞缓解 / 修复闭环，并对高权限账号持续梳理，并对其行为动态持续跟踪审计。关键考虑的因素和框架如下图。

来源：《2022APT趋势洞察报告》

网域管理与安全设施部署

网域管理与安全设施部署的使命在于：建立深度防御和有效隔离的机制，为安全事件溯源提供原始日志数据支撑。



来源：《2022APT趋势洞察报告》

建立研发供应链安全机制

建立研发供应链安全机制的目标：推动产品线安全架构体系化设计及软件供应链安全管理流程落地，实现产品从代码研发到上线运营全生命周期的安全可控。

2021 年 6 月，Google 基于自身供应链安全管理实践，发布了 SLSA 框架 (Supply chain Levels for Software Artifacts)。SLSA 来源于 Google 内部基于容器化基础架构的 Borg 二进制授权 (BinaryAuthorization)。基本思想在于关注 DevOps 场景中各个研发环节 (SCM[source]->CI/CD[Build]->Distribution[Package]) 的完整性和可追溯性。

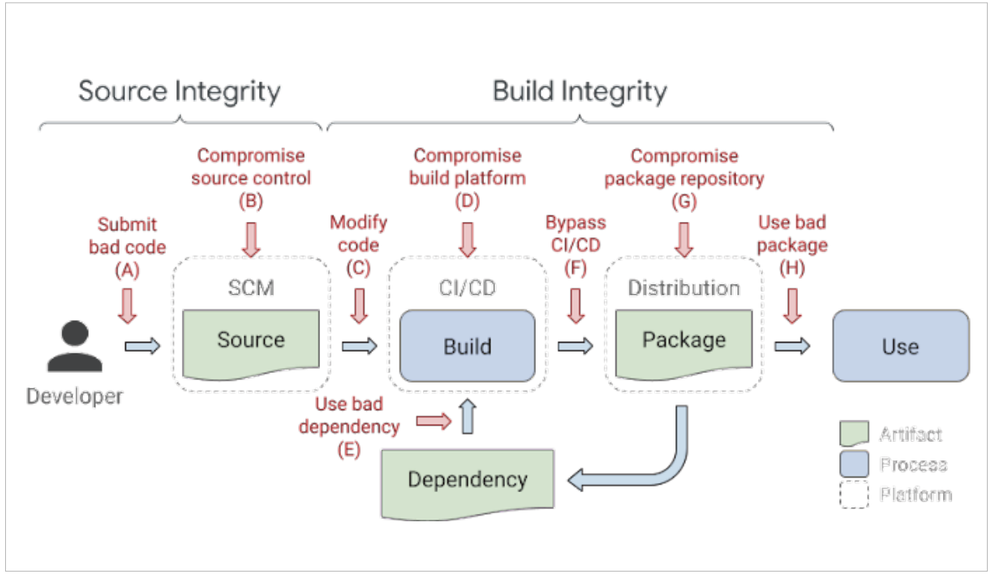


图 SLSA流程

在 SLSA 框架中，对不同层次的安全级别定义如下：

SLSA1

构建过程完全自动化，并生成出处。出处是关于如何构建中间件的元数据，包括构建过程、顶级源代码和依赖关系。基于对产品出处的理解，可以让软件用户做出合理安全决策。SLSA1 不能防篡改，但提供了基本的源代码识别，并有助于漏洞管理。

SLSA2

使用版本控制，并在构建阶段生成经过身份验证的出处 (译注：基于经过验证的依赖完成编译)。从而让消费者提升对软件来源的信心。在编译环节可信的前提下，该层次能达到防篡改的效果。SLSA2 还提供了到 SLSA3 的简便升级路径。

SLSA3

保证源代码可审计性和完整性的一系列要求。SLSA3 通过防止特定类型的威胁（如交叉构建污染），提供了比前两个级别更强大的防篡改保护。

SLSA4

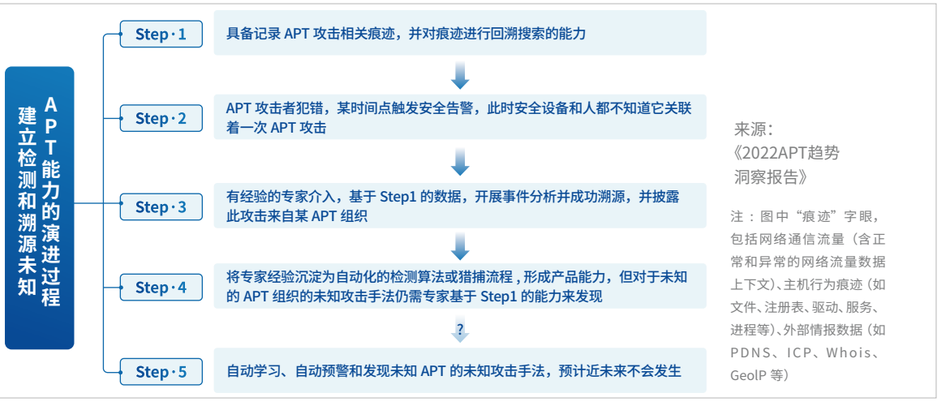
需有两人对所有变更进行审查，且需提供一个密封、可复制的构建过程。双人评审是行业最佳实践，可发现错误并阻止不良行为。封闭性的构建保证源代码依赖列表的完整性。可复制构建，虽不必须，但提供了可审计性和可靠性。SLSA4 确保用户的高信任。

然而对于提供的产品或服务非容器化基础架构的场景，则需要考虑对产品架构开展分层的安全设计和管理，降低产品开发运营的技术债，从而有效提高攻击成本，建议的技术框架请见下图。

来源：《2022APT趋势洞察报告》

建立安全运营和事件响应中心

深信服安全蓝军认为，APT 防御的技术基础是多阶段递进的，参考威胁猎捕能力成熟度模型，将基础设施和威胁猎捕能力层次分为如下多个阶段。



来源：
《2022APT趋势洞察报告》

注：图中“痕迹”字眼，包括网络通信流量（含正常和异常的网络流量数据上下文）、主机行为痕迹（如文件、注册表、驱动、服务、进程等）、外部情报数据（如 PDNS、ICP、Whois、GeoIP 等）

可见数据痕迹的存留和数据检索能力的构建是 APT 猎捕能力建设的基础。建立安全运营和事件响应中心的目标就是推动组织逐步构建上述 Step 4 阶段的能力，实现针对所在组织 IT 基础设施及人员、产品或服务的定向攻击事件的持续挖掘及快速响应机制，保证对所在组织的网络攻击风险的可视、可控。

来源：《2022APT趋势洞察报告》

附1：深信服威胁情报中心

站点地址： https://ti.sangfor.com.cn/analysis-platform

深信服威胁情报中心应用大数据、AI、图数据等最新尖端技术，在海量的表网、深网、暗网数据中进行多维度的数据聚合、威胁分析与研判，生产多种战术情报和战略情报，并赋能给深信服各类安全产品，打造“云 - 网 - 端”联动的纵深检测防御体系。

附2：
深信服千里目安全技术中心深瞻情报实验室

深信服千里目安全技术中心深瞻情报实验室专注于高级威胁攻防、APT 事件响应及取证溯源技术研究，团队由多名高级威胁情报分析、恶意样本分析、红队技术研究专家构成。

微信公众号：Further_eye/ 深信服千里目安全技术中心 - 安全情报 - 高级威胁持续性追踪 (公众号截图如下)