# 安全事件周报

## 安全事件周报 (01.04-01.10)



360CERT
北京奇虎科技有限公司 | 2021-01-11

# 报告信息

| | | | |
|---|---|---|---|
| 报告名称 | 安全事件周报（01.04-01.10） | | |
| 报告类型 | 安全事件周报 | 报告编号 | B6-2021-011101 |
| 报告版本 | 1.0 | 报告日期 | 2021-01-11 |
| 报告作者 | 360CERT | 联系方式 | cert@360.cn |
| 提供方 | 北京奇虎科技有限公司 | | |
| 接收方 | | | |

# 报告修订记录

| 报告版本 | 日期 | 修订 | 审核 | 描述 |
|---|---|---|---|---|
| 1.0 | 2021-01-11 | 360CERT | 360CERT | 撰写报告 |

# 目录

# 一、 事件概览


本周收录安全事件 40 项

话题集中在`勒索软件`、`黑客攻击`方面，涉及的组织有：`Zyxel`、`JustPay`、`Nvidia`、`达索航空公司`等。勒索策略瞄准高层信息，个人工作站防护不可忽视。

对此，360CERT 建议：

1. 使用 360 安全卫士进行病毒检测、
2. 使用 360 安全分析响应平台进行威胁流量检测，
3. 使用 360 城市级网络安全监测服务 QUAKE 进行资产测绘，
4. 做好资产自查以及预防工作，以免遭受黑客攻击。

# 二、 事件档案

| **恶意程序** | **等级** |
| --- | --- |
| 新的基于 Golang 的恶意软件蠕虫 | ★★★★★ |
| 新的网络钓鱼攻击传递 Windows 恶意软件 | ★★★★★ |
| Ryuk Gang 约从勒索软件攻击中获得了超过 1.5 亿美元的收入 | ★★★★★ |
| 恶意软件使用 WiFi BSSID 识别受害者 | ★★★★ |
| TransLink 确认遭到勒索软件攻击，数据被盗 | ★★★★ |
| 新的 ElectroRAT 恶意软件锁定加密货币用户 | ★★★★ |
| 攻击者冒充澳大利亚网络安全中心传播恶意软件 | ★★★★ |
| Babuk Locker 是 2021 年第一款新的企业勒索软件 | ★★★★ |
| 研究人员披露了 FIN7 黑客组织恶意软件的细节 | ★★★★ |
| 朝鲜黑客利用 RokRat 木马发动针对韩国的网络攻击 | ★★★★ |
| Linux 恶意软件作者使用 Ezuri Golang 加密程序绕过检测 | ★★★★ |
| 一个加密挖掘僵尸网络正在窃取 Docker 和 AWS 的证书 | ★★★★ |
| 一些勒索软件团伙正在持续追踪高级管理人员信息，以迫使公司付款 | ★★★★ |
| 网络钓鱼活动传播 IcedID 恶意软件 | ★★★ |
| 朝鲜 APT37 黑客使用 VBA 自解码技术 | ★★★ |
| **数据安全** | **等级** |
| 意大利移动运营商在海量数据泄露后更换 SIM 卡 | ★★★★★ |
| 由于 Git 配置错误，尼桑公司的源代码在网上泄露 | ★★★★★ |
| 伦敦议会被盗数据遭黑客泄漏 | ★★★★★ |
| 黑客公开了 1 万个美国运通账户的数据 | ★★★★ |
| 血液检测实验室遭数据泄露 | ★★★★ |
| 遭勒索软件攻击后，Dassault Falcon Jet 报告数据泄露 | ★★★★ |

| 网络攻击 | 等级 |
| --- | --- |
| APT 黑客转向勒索软件攻击 | ★★★★★ |
| 朝鲜软件供应链攻击的目标是股票投资者 | ★★★★★ |
| 250 个组织受到 SolarWinds 黑客攻击的影响 | ★★★★★ |
| 印度支付平台 JustPay 被入侵 | ★★★★★ |
| SolarWinds 黑客访问了美国司法部的电子邮箱 | ★★★★★ |
| 领先游戏发行商遭数据泄露 | ★★★★ |
| 新的 SMS 网络钓鱼活动针对 PayPal 用户 | ★★★★ |
| 针对医疗行业的网络攻击增加 | ★★★★ |
| **其他事件** | **等级** |
| 10 万个 Zyxel 设备易受后门攻击 | ★★★★★ |
| 英国法官否认美国引渡阿桑奇 | ★★★★ |
| Zend Framework 远程代码执行漏洞 | ★★★★ |
| Google 警告严重的 Android 远程代码执行漏洞 | ★★★★ |
| 前副总裁恶意入侵公司，并破坏个人防护用品供应 | ★★★★ |
| 新加坡警方可以获取 COVID-19 联系人追踪数据进行刑事调查 | ★★★ |
| Slack 在 2021 年遭遇首次大规模停机 | ★★★ |
| Citrix 更新 ADC 产品以修复 DDoS 攻击 | ★★★ |
| Fortinet FortiWeb WAF 中的多个漏洞可让黑客攻击企业网络 | ★★★ |
| Nvidia 发布了针对 GPU 显示驱动程序和 vGPU 漏洞的安全更新 | ★★★ |
| 摩根大通黑客被判 12 年监禁 | ★★ |

# 三、 事件详情

## (一) 恶意程序

### 新的基于 Golang 的恶意软件蠕虫

日期: 2021-01-04

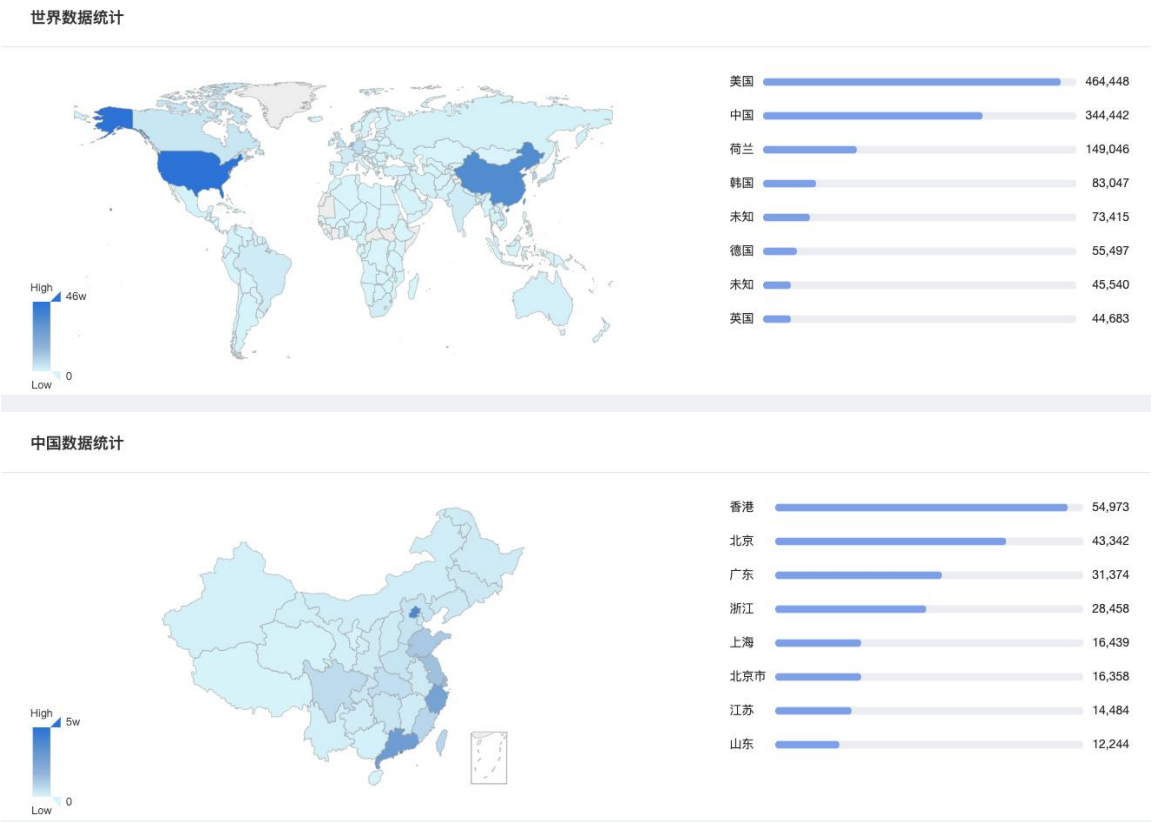
等级: 高

来源: Prajeet Nair

标签: ['Intezer', 'Monero', 'Cryptomining', 'XMRig', 'Weak Passwords']

安全公司`Intezer`的研究人员发现了一种新的基于`Golang`的蠕虫，该蠕虫针对`Windows`和`Linux`服务器。
该蠕虫自 2020 年 12 月以来一直活跃，会将`XMRig`恶意软件（用于挖掘`Monero`等加密货币）注入易受攻击的服务器中。
它的目标是使用弱口令的、面向公众的服务，例如`MySQL`，`Tomcat`管理面板和开源自动化`Jenkins`服务器。
此外，它还利用`Oracle WebLogic`中的漏洞，编号为 CVE-2020-14882。

目前 Weblogic 的具体分布如下图，数据来自于 360 QUAKE




详情

New Golang-Based Worm Targets Servers to Mine Monero

https://www.databreachtoday.com/new-golang-based-worm-targets-servers-to-mine-monero-a-15692

## 新的网络钓鱼攻击传递 Windows 恶意软件

日期: 2021-01-06

等级: 高

来源: Danny Palmer

标签: ['QRat', 'Trustwave', 'Donald Trump', 'Windows', 'Phishing']

一个新的网络钓鱼活动正在试图诱使受害者下载恶意软件，这使网络攻击者可以完全控制受感染的`Windows`计算机。
Quaverse 远程访问木马（QRat）首次出现在 2015 年，并一直保持成功，是因为它难以在多层混淆下被检测到，同时为恶意黑客提供了对受感染受害者计算机的远程访问。
如今`Trustwave`的网络安全研究人员又发现了一个新的`QRat`活动，该活动试图引诱人们下载最新版本的恶意软件，这个恶意附件是声称包含唐纳德·特朗普总统的恶性视频。

详情

This new phishing attack uses an odd lure to deliver Windows trojan malware

https://www.zdnet.com/article/this-new-phishing-attack-uses-an-odd-lure-to-deliver-windows-trojan-malware/

## Ryuk Gang 约从勒索软件攻击中获得了超过 1.5 亿美元的收入

日期: 2021-01-07

等级: 高

来源: Catalin Cimpanu

标签: ['Ryuk gang', 'Bitcoin', 'Ransomware']

据称，由于对全世界公司的入侵，Ryuk 勒索软件的运营商已经从勒索中获得了价值超过 1.5 亿美元的比特币。
在 2021 年 1 月 7 日发布的一份联合报告中，威胁情报公司`Advanced Intelligence`和网络安全公司`HYAS`表示，他们跟踪了先前归因于`Ryuk`勒索软件攻击并与之相关的 61 个比特币地址的付款。
两家公司表示，`Ryuk`从一家知名的经纪人那里收到了大量赎金，该经纪人代表勒索软件受害者付款。这些付款有时达数百万美元，通常在数十万美元之间。

详情

Ryuk gang estimated to have made more than $150 million from ransomware attacks

https://www.zdnet.com/article/ryuk-gang-estimated-to-have-made-more-than-150-million-from-ransomware-attacks/

## 恶意软件使用 WiFi BSSID 识别受害者

日期: 2021-01-04

等级: 高

来源: Catalin Cimpanu

标签: ['WIFI BSSID', 'GeoIP', 'Trojans', 'Malware']

恶意软件运营商想要知道他们感染的受害者的位置，通常依靠一种简单的技术，他们获取受害者的 IP 地址，并对照 IP 映射地理位置的数据库，以获得受害者的大致地理位置，比如 MaxMind 的 GeoIP 数据库。
安全研究人员`Xavier Mertens`在 2020 年 12 月表示，他发现了一种新的恶意软件病毒，该病毒使用了新的技术，该技术依赖于获取受感染用户的`BSSID`。
`BSSID`被称为基本服务集标识符，基本上是用户用来通过`WiFi`连接的无线路由器或接入点的`MAC`物理地址。

详情

Malware uses WiFi BSSID for victim identification
https://www.zdnet.com/article/malware-uses-wifi-bssid-for-victim-identification/

## TransLink 确认遭到勒索软件攻击，数据被盗

日期: 2021-01-04
等级: 高
来源: Sergiu Gatlan
标签: ['TransLink', 'Egregor', 'Data Theft', 'Cyberattack', 'Ransomware']

温哥华交通运输公司`TransLink`已确认，`Egregor`勒索软件运营商在 2020 年 12 月破坏了其网络，并且已窃取了员工的银行和社会保障信息。
TransLink 于 2020 年 12 月 1 日宣布，网络攻击后，交通网络的计算系统出现问题。
这些信息技术问题影响了公司的电话和在线服务，以及客户用信用卡或借记卡付款的能力。

详情

TransLink confirms ransomware data theft, still restoring systems
https://www.bleepingcomputer.com/news/security/translink-confirms-ransomware-data-theft-still-restoring-systems/

## 新的 ElectroRAT 恶意软件锁定加密货币用户

日期: 2021-01-05
等级: 高
来源: Catalin Cimpanu
标签: ['ElectroRAT', 'Malware', 'Cryptocurrency']

安全公司 Intezer Labs 表示，他们发现了一个长达一年的秘密恶意软件操作，网络攻击者创建了伪造的加密货币应用程序，以诱骗用户在其系统上安装新的恶意软件，最终目的是窃取受害者的资金。
这些伪造的应用分别命名为`Jamm`，`eTrade/Kintum`和`DaoPoker`，分别托管在`jamm.to`，`kintum.io`和`daopker.com`的专用网站上。
前两个应用程序声称提供了一个简单的交易加密货币的平台，而第三个应用程序是一个加密货币扑克应用程序。

详情

Hackers target cryptocurrency users with new ElectroRAT malware

https://www.zdnet.com/article/hackers-target-cryptocurrency-users-with-new-electrorat-malware/

## 攻击者冒充澳大利亚网络安全中心传播恶意软件

日期: 2021-01-05

等级: 高

来源: Sergiu Gatlan

标签: ['the Australian Cyber Security Centre', 'TeamViewer', 'AnyDesk', 'Malware']

澳大利亚政府警告称，有网络攻击运动冒充澳大利亚网络安全中心（ACSC）传播恶意软件。
攻击者发送的电子邮件伪装成 ACSC 传递的官方消息，试图说服接收方通过恶意链接下载防病毒软件。
攻击者甚至说服受害者安装远程管理和桌面共享软件，以窃取目标用户的银行信息。

详情

Australian cybersecurity agency used as cover in malware campaign

https://www.bleepingcomputer.com/news/security/australian-cybersecurity-agency-used-as-cover-in-malware-campaign/

## Babuk Locker 是 2021 年第一款新的企业勒索软件

日期: 2021-01-05

等级: 高

来源: Lawrence Abrams

标签: ['Babuk Locker', 'Bitcon', 'Ransomware', 'Enterprise']

2021 年，出现了一款名为`Babuk Locker`的新型勒索软件，它的目标是通过人为操作来攻击企业受害者。
`Babuk Locker`是一项新的勒索软件，于 2021 年初启动，此后收集了来自世界各地的一小部分受害者名单。
该勒索软件要求受害者支付的比特币赎金范围在 6 万美元到 8 万 5 千美元不等。

详情

Babuk Locker is the first new enterprise ransomware of 2021

https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

## 研究人员披露了 FIN7 黑客组织恶意软件的细节

日期: 2021-01-05

等级: 高

来源: Prajeet Nair

标签: ['JSSLoader', 'Morphisec', 'Hacking Group', 'Malware', 'Spear Phishing']

`Morphisec Labs`的研究人员公布了一个名为 JSSLoader 的恶意软件变种的最新细节，该恶意软件被`FIN7`黑客组织使用了几年。

`FIN7`是一个有经济动机的黑客组织，据信在东欧活动，并以鱼叉式网络钓鱼攻击受害者而闻名。
尽管`FIN7`被怀疑在几次活动中使用`JSSLoader`，但有关该恶意软件的详细信息却难以捉摸。
但是，在 2020 年 12 月一次失败的攻击中，`Morphisec`研究人员恢复了`FIN7`使用的`.NET`编程语言编写的远程访问木马。

详情

Researchers Disclose Details of FIN7 Hacking Group's Malware

https://www.databreachtoday.com/researchers-disclose-details-fin7-hacking-groups-malware-a-15703

## 朝鲜黑客利用 RokRat 木马发动针对韩国的网络攻击

日期: 2021-01-07

等级: 高

来源: Charlie Osborne

标签: ['North Korean', 'RokRat', 'South Korean', 'Remote Access Trojan']

一个朝鲜黑客组织正在利用`RokRat`木马发动新一轮针对韩国政府的攻击。
远程访问特洛伊木马（RAT）与基于韩国常用韩语文字处理器的攻击有关，这种攻击已有数年之久。
RokRat 木马被认为是属于`APT37`（也称为 ScarCruft，Reaper 和 Group123）组织的，该组织至少从 2012 年开始活跃。

详情

North Korean hackers launch RokRat Trojan in campaigns against the South

https://www.zdnet.com/article/north-korean-hackers-launch-rokrat-trojan-in-campaigns-against-the-south/

## Linux 恶意软件作者使用 Ezuri Golang 加密程序绕过检测

日期: 2021-01-07

等级: 高

来源: Ax Sharma

标签: ['Ezuri', 'Golang', 'GitHub', 'Crypter']

多个恶意软件作者正在使用`Ezuri`加密器和内存加载器，使他们的代码无法被防病毒产品检测到。
GitHub 上提供了用 Golang 编写的 Ezuri 源代码，任何人都可以使用。
Ezuri 用 Go 语言编写，同时充当 ELF（Linux）二进制文件的加密器和加载器。
它使用`AES`加密恶意软件代码，解密后直接在内存中执行恶意有效负载，而不会在磁盘上生成任何文件。

详情

Linux malware authors use Ezuri Golang crypter for zero detection

https://www.bleepingcomputer.com/news/security/linux-malware-authors-use-ezuri-golang-crypter-for-zero-detection/

## 一个加密挖掘僵尸网络正在窃取 Docker 和 AWS 的证书

日期: 2021-01-08

等级: 高

来源: Catalin Cimpanu

标签: ['Docker', 'AWS', 'Credentials', 'Botnet']

安全研究人员发现了一个收集和窃取 Docker 和 AWS 证书的恶意僵尸网络，研究人员将其与一个名为 TeamTNT 的网络犯罪行动联系起来；该组织在 2020 年夏天首次发现在配置错误的容器平台上安装加密货币挖掘恶意软件。当时的初步报告称，TeamTNT 正在寻找 Docker 系统，这些系统在没有密码的情况下在线暴露其管理 API 端口，从而破坏了集装箱平台。研究人员表示，TeamTNT 集团将访问暴露的 Docker 容器，安装加密挖掘恶意软件，但也会窃取亚马逊网络服务（AWS）服务器的凭据，以便转向一家公司的其他 IT 系统，感染更多服务器，部署更多加密挖掘者。

详情

A crypto-mining botnet is now stealing Docker and AWS credentials

https://www.zdnet.com/article/a-crypto-mining-botnet-is-now-stealing-docker-and-aws-credentials/

## 一些勒索软件团伙正在持续追踪高级管理人员信息，以迫使公司付款

日期: 2021-01-09

等级: 高

来源: Catalin Cimpanu

标签: ['Clop', 'Ransomware', 'Top Execs']

勒索软件集团中出现了一种新的趋势，他们优先从高管和管理人员使用的工作站窃取数据，然后利用这些信息向公司高层施压和勒索，以勒索巨额赎金。安全公司与一家公司通电话时首次得知了这一新策略，该公司向 Clop 勒索软件团伙支付了数百万美元的赎金。后来，与其他 Clop 受害者的类似电话和对网络安全公司的电子邮件采访证实，这不仅仅是一次侥幸，而是 Clop 团伙在过去几个月一直使用的一种技术。

详情

Some ransomware gangs are going after top execs to pressure companies into paying

https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/

## 网络钓鱼活动传播 IcedID 恶意软件

日期: 2021-01-07

等级: 中

来源: Bradley Barth

标签: ['TA551', 'Ursnif', 'Valak', 'IcedID', 'Phishing']

一个网络钓鱼活动一直试图将垃圾邮件伪装成一个电子邮件链，使用的是从以前受到攻击的主机上的电子邮件客户端获取的真实邮件。如果收件人打开文档并启用其中的恶意宏，

就会安装`IcedID`恶意软件。
来自`Palo Alto Networks`的`Unit 42`威胁研究小组 2021 年 1 月 7 日发表的一篇博客文章称，网络犯罪集团`TA551`（又名`Shathak`）是此次行动的幕后黑手，该行动传播窃取信息的恶意软件，如 Ursnif，Valak 和 IcedID。

详情

TA551 malspam campaign spoofs email chains to install IcedID info

https://www.scmagazine.com/home/security-news/phishing/malspam-campaign-spoofs-email-chains-to-install-icedid-info-stealer/

## 朝鲜 APT37 黑客使用 VBA 自解码技术

日期: 2021-01-09

等级: 中

来源: GURUBARAN S

标签: ['North Korean', 'VBA', 'RokRat', 'APT37']

一个名为 ScarCruft、Reaper 和 Group123 的朝鲜黑客组织利用 VBA 自解码技术注入 RokRat，参与了针对韩国政府的攻击。RokRat 是一个远程访问特洛伊木马（RAT），是一个复杂的后门程序，通常以编码二进制文件的形式分发，在攻击武器化文档后，由外壳代码下载并解密。RokRat 攻击的有趣点在于恶意文件中包含一个嵌入宏，它使用 VBA 自解码技术在 Microsoft Office 的内存空间中对自身进行解码，而不写入磁盘。完成后，它会将 RokRat 的一个变体嵌入到记事本中。

详情

North Korean APT37 Hackers Use VBA Self Decode Technique

https://gbhackers.com/north-korean-apt37-hackers/

## 相关安全建议

1. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
2. 各主机安装 EDR 产品，及时检测威胁
3. 及时对系统及各个服务组件进行版本升级和补丁更新
4. 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
5. 网段之间进行隔离，避免造成大规模感染
6. 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

# (二) 数据安全

## 意大利移动运营商在海量数据泄露后更换 SIM 卡

日期: 2021-01-05

等级: 高

来源: Catalin Cimpanu

标签: ['Italian', 'SIM', 'Ho Mobile', 'Data Breach', 'Dark Web']

2020 年 12 月 28 日，一名安全分析人员在一个暗网论坛上发现了出售的电信公司数据库，该数据库是意大利移动运营商`Ho Mobile`的。
沃达丰（Vodafone）旗下的意大利移动运营商`Ho Mobile`已于 2021 年 1 月 4 日证实了大规模的数据泄露，采取的措施是替换所有受影响客户的 SIM 卡。
据信，该漏洞目前已经已影响了大约 250 万客户。

详情

Italian mobile operator offers to replace SIM cards after massive data breach

https://www.zdnet.com/article/italian-mobile-operator-offers-to-replace-sim-cards-after-massive-data-breach/

## 由于 Git 配置错误，尼桑公司的源代码在网上泄露

日期: 2021-01-06

等级: 高

来源: Catalin Cimpanu

标签: ['Source Code', 'Git repo', 'Misconfiguration', 'Leaked']

尼桑北美公司开发使用的移动应用程序和内部工具的源代码被泄漏，原因是该公司错误配置了一台`Git`服务器。
瑞士软件工程师`Tillie Kottmann`表示，泄漏源于一台`Git`服务器，该服务器以默认的用户名和密码组合（默认为`admin`/`admin`）暴露在互联网上。
`Kottmann`称`Git`存储库包含以下源代码：

- 尼桑`ASIST`诊断工具的某些部分
- 其他各种后端和内部工具

详情

Nissan source code leaked online after Git repo misconfiguration

https://www.zdnet.com/article/nissan-source-code-leaked-online-after-git-repo-misconfiguration/

## 伦敦议会被盗数据遭黑客泄漏

日期: 2021-01-07

等级: 高

来源: Daphne Leprince-Ringuet

标签: ['Hackney Council', 'Dark Web', 'Leaked ', 'Cyberattack']

2020 年，针对伦敦市议会的一次网络攻击中被盗的数据已被黑客泄漏。
哈克尼委员会（Hackney Council）为英国首都的 28 万居民提供服务，2020 年 10 月被标为严重的网络攻击的重创，使许多 IT 系统无法运行，有些系统目前仍在中断。
现在看来，在攻击过程中被盗的信息已经被犯罪分子发布到了暗网上，尽管该委员会表示

只有有限的一组数据处于危险之中。

详情

Data stolen in cyber-attack has been leaked online by hackers, says council

https://www.zdnet.com/article/data-stolen-in-cyber-attack-has-been-leaked-online-by-hackers-says-council/

## 黑客公开了 1 万个美国运通账户的数据

日期: 2021-01-05

等级: 高

来源: Ax Sharma

标签: ['American Express', 'Hacker Forum', 'Leaked Data', 'Credit Card']

有黑客在一个黑客论坛上免费发布了 1 万名美国运通信用卡持有者的数据。
在同一篇论坛帖子中，这位攻击者声称出售了更多美国运通(American Express)、桑坦德银行(Santander)和 Banamex 等墨西哥银行客户的数据。
泄漏的 10,000 条记录的样本数据集会暴露完整的美国运通帐户（信用卡）号和客户的个人身份信息（PII），包括姓名，完整地址，电话号码，出生日期，性别等。

详情

Hacker posts data of 10,000 American Express accounts for free

https://www.bleepingcomputer.com/news/security/hacker-posts-data-of-10-000-american-express-accounts-for-free/

## 血液检测实验室遭数据泄露

日期: 2021-01-06

等级: 高

来源: Prajeet Nair

标签: ['Apex', 'Data Leaked', 'Blood Testing Lab']

总部位于纽约法明代尔的血液检测机构`Apex`实验室通知患者他们的信息遭到了泄露。
虽然最初的调查并未显示数据丢失或受到破坏，但`Apex`于 2020 年 12 月 15 日发现黑客已开始在线发布患者信息。
泄露的数据包括患者姓名、出生日期、检测结果，有些还包括社会保险号码和电话号码。

详情

Blood Testing Lab Data Leaked

https://www.databreachtoday.com/blood-testing-lab-data-leaked-a-15710

## 遭勒索软件攻击后，Dassault Falcon Jet 报告数据泄露

日期: 2021-01-08

等级: 高

来源: Sergiu Gatlan

标签: ['Dassault Falcon Jet', 'Dassault Aviation', 'aerospace']

`Dassault Falcon Jet`公司披露了一项数据泄露事件，可能导致现任和前任员工及其配偶和家属的个人信息被曝光。`Dassault Falcon Jet`是法国达索航空公司的美国子公司，该公司设计和制造军用飞机、公务机和航天系统。Dassault 的子公司有 2453 名员工，专注于为美洲大陆的猎鹰飞机提供航空和维修服务。

详情

Dassault Falcon Jet reports data breach after ransomware attack

https://www.bleepingcomputer.com/news/security/dassault-falcon-jet-reports-data-breach-after-ransomware-attack/

## 相关安全建议

1. 及时备份数据并确保数据安全
2. 发生数据泄漏事件后，及时进行密码更改等相关安全措施
3. 及时检查并删除外泄敏感数据
4. 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
5. 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

# (三) 网络攻击

## APT 黑客转向勒索软件攻击

日期: 2021-01-04

等级: 高

来源: Ionut Ilascu

标签: ['APT27', 'Remote Access Trojan', 'Ransomware', 'Gambling Sector']

安全研究人员在调查多家公司发生的一系列勒索软件事件时，发现了一种恶意软件。
尽管此次攻击没有 APT 攻击的复杂性，但有强有力的证据将它们与 APT27 相关联，APT27 通常参与网络间谍活动。
这些攻击发生在 2020 年，直接针对至少五家在全球运营的在线博彩行业公司，并成功加密了几台核心服务器。

详情

China's APT hackers move to ransomware attacks

https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/

## 朝鲜软件供应链攻击的目标是股票投资者

日期: 2021-01-05

等级: 高

来源: Ax Sharma

标签: ['North Korean', 'Stock Investors', 'Thallium', 'Supply Chain Attack']

根据 2021 年 1 月 5 日发布的一份报告，朝鲜黑客组织`Thallium`（又名`APT37`）在软件供应链攻击中将私人股票投资通讯服务的用户作为目标。
到目前为止，该组织主要依靠网络钓鱼攻击（例如通过`Microsoft Office`文档）来针对受害者。

详情

North Korean software supply chain attack targets stock investors

https://www.bleepingcomputer.com/news/security/north-korean-software-supply-chain-attack-targets-stock-investors/

## 250 个组织受到 SolarWinds 黑客攻击的影响

日期: 2021-01-05

等级: 高

来源: Mathew J. Schwartz

标签: ['SolarWinds', 'Organizations', 'Supply Chain', 'Sunburst']

随着调查人员对 SolarWinds 黑客行为的调查，他们发现供应链活动似乎比最初想象的要更加严重。
《纽约时报》报道称，多达 250 个组织可能受到了更高级的黑客攻击。
已确认的`Sunburst`后门受害者包括美国商务部、国土安全部、国务院和能源部，以及五角大楼的一些分支机构。、
其他目标组织包括科技巨头贝尔金、思科、英特尔、英伟达和 VMware，以及爱荷华州立大学、亚利桑那州皮马县和希尔顿大度假酒店等。

详情

Severe SolarWinds Hacking: 250 Organizations Affected?

https://www.databreachtoday.com/severe-solarwinds-hacking-250-organizations-affected-a-15699

## 印度支付平台 JustPay 被入侵

日期: 2021-01-05

等级: 高

来源: Akshaya Asokan

标签: ['JustPay', 'Indian', 'Amazon Web Services', 'Dark Web', 'Leaked Data']

印度在线支付平台 JustPay 在 2021 年 1 月 4 日确认，该公司 8 月份的客户数据遭到泄露，有数百万`JustPay`客户的数据在一个暗网论坛上出售。
该公司表示，该漏洞似乎源于回收的`Amazon Web Services`访问密钥，该密钥允许未经

授权访问其数据库。

详情

Indian Payment Platform JustPay Breached

https://www.databreachtoday.com/indian-payment-platform-justpay-breached-a-15697

## SolarWinds 黑客访问了美国司法部的电子邮箱

日期: 2021-01-06

等级: 高

来源: Pierluigi Paganini

标签: ['SolarWinds', 'The US DoJ ', 'OCIO', 'O365 Mailboxes']

美国司法部（DoJ）发布了一份新闻稿，确认`SolarWinds`供应链攻击背后的攻击者能够访问其数千个员工的邮箱。
2020 年 12 月 24 日，美国司法部首席信息官办公室（OCIO）了解到与全球`SolarWinds`事件有关的先前未知的恶意活动，该事件已影响到多个联邦机构和技术承包商。
这项活动涉及访问该部门的`Microsoft O365`电子邮件环境，能访问的`O365`邮箱数量似乎限制在 3%左右，目前没有迹象表明任何机密系统都受到了影响。

详情

SolarWinds hackers had access to roughly 3% of US DOJ O365 mailboxes

https://securityaffairs.co/wordpress/113108/data-breach/solarwinds-hackers-o365-mailboxes.html

## 领先游戏发行商遭数据泄露

日期: 2021-01-04

等级: 高

来源: Tom Spring

标签: ['Kela', 'Ubisoft', 'Game Publishers', 'Leaked']

育碧等领先的游戏公司已成为网络犯罪分子的主要目标，这些网络犯罪分子旨在通过出售与顶级游戏发行商相关的内部凭证来获利。
研究人员表示，从在线泄露的数据缓存中发现了与前 25 家游戏公司相关的超过 50 万份被盗的凭证，这些凭证在犯罪市场上被出售。
正如`Threatpost`的 2020 年网络安全回顾所概述的那样，过去一年对游戏行业来说是困难的一年。

详情

Leading Game Publishers Hit Hard by Leaked

https://threatpost.com/game-publishers-hit-by-leaked-credentials/162725/

## 新的 SMS 网络钓鱼活动针对 PayPal 用户

日期: 2021-01-04

等级: 高

来源: AmerOwaida

标签: ['SMS', 'PayPal', 'Phishing', 'Smishing']

`BleepingComputer`报告称，一个新的基于`SMS`的网络钓鱼活动正在尝试将`PayPal`用户从其帐户凭据和敏感信息中分离出来。
该策略由`SMS`短信组成，这些短信模拟了流行的付款处理程序，并通知潜在的受害者其帐户已永久受到限制，并且他们需要单击链接来验证其身份。
如果单击该链接，受害者将被重定向到一个登录页面，该页面将要受害者提供登陆凭据。
如果受害者登录，凭据会被发送给攻击者，而钓鱼网站将试图收集更多信息，包括全名，出生日期和银行详细信息。

详情

PayPal users targeted in new SMS phishing campaign
https://www.welivesecurity.com/2021/01/04/paypal-users-targeted-new-sms-phishing-campaign/

## 针对医疗行业的网络攻击增加

日期: 2021-01-05

等级: 高

来源: Charlie Osborne

标签: ['Check Point', 'DDos', 'Cyberattacks', 'COVID-19', 'Healthcare']

在未来几个月中，医疗保健行业应该做好应对网络攻击和各种攻击媒介增加的准备。
网络安全公司`Check Point`发布了新的数据统计，显示自 2020 年 11 月以来对全球医疗保健行业的网络攻击增加了 45%，而同期所有全球行业的网络攻击增加了 22%。
攻击者所采用的攻击媒介范围很广，包括分布式拒绝服务（DDoS）攻击，社会工程，僵尸网络，网络钓鱼和勒索软件。

详情

As coronavirus cases surge, so do cyberattacks against the healthcare sector
https://www.zdnet.com/article/as-coronavirus-cases-surge-so-do-cyberattacks-against-the-healthcare-sector/

## 相关安全建议

1. 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
2. 积极开展外网渗透测试工作，提前发现系统问题
3. 域名解析使用 CDN
4. 域名解析使用 CDN
5. 条件允许的情况下，设置主机访问白名单

6. 注重内部员工安全培训

## (四) 其他事件

### 10 万个 Zyxel 设备易受后门攻击

日期: 2021-01-04

等级: 高

来源: Prajeet Nair

标签: ['Zyxel', 'VPN', 'Eye Control', 'Vulnerability']

荷兰安全公司`Eye Control`称，大约 10 万种`Zyxel`产品中的固件漏洞（包括 VPN 网关，接入点控制器和防火墙）可用于安装硬编码后门，该后门可以给攻击者提供远程管理特权。
该漏洞编号为 CVE-2020-29583。
Zyxel 已经在其某些产品中发布了针对该漏洞的补丁程序，并敦促其客户立即应用它们。但是，该公司在一份通报中指出，其`NXC`接入点控制器系列产品的修复程序要到 4 月才能发布。

详情

100,000 Zyxel Devices Vulnerable to Backdoor
https://www.databreachtoday.com/100000-zyxel-devices-vulnerable-to-backdoor-a-15693

### 英国法官否认美国引渡阿桑奇

日期: 2021-01-04

等级: 高

来源: Scott Ferguson

标签: ['British', 'WikiLeaks', 'Julian Assange', 'America', 'Extradition']

一名英国法官 2021 年 1 月 4 日拒绝了美国司法部的一项请求：将维基解密创始人朱利安·阿桑奇引渡到美国，以面临与入侵政府计算机并发布机密信息有关的刑事指控。
现年 49 岁的阿桑奇（Assange）被指控违反了美国间谍法和计算机欺诈与滥用法，并获得并公布了包括国防部在内的几个美国政府机构的一系列机密文件。
根据司法部的说法，阿桑奇面临 18 项刑事罪。

详情

British Judge Denies US Extradition of Assange
https://www.databreachtoday.com/british-judge-denies-us-extradition-assange-a-15691

### Zend Framework 远程代码执行漏洞

日期: 2021-01-04

等级: 高

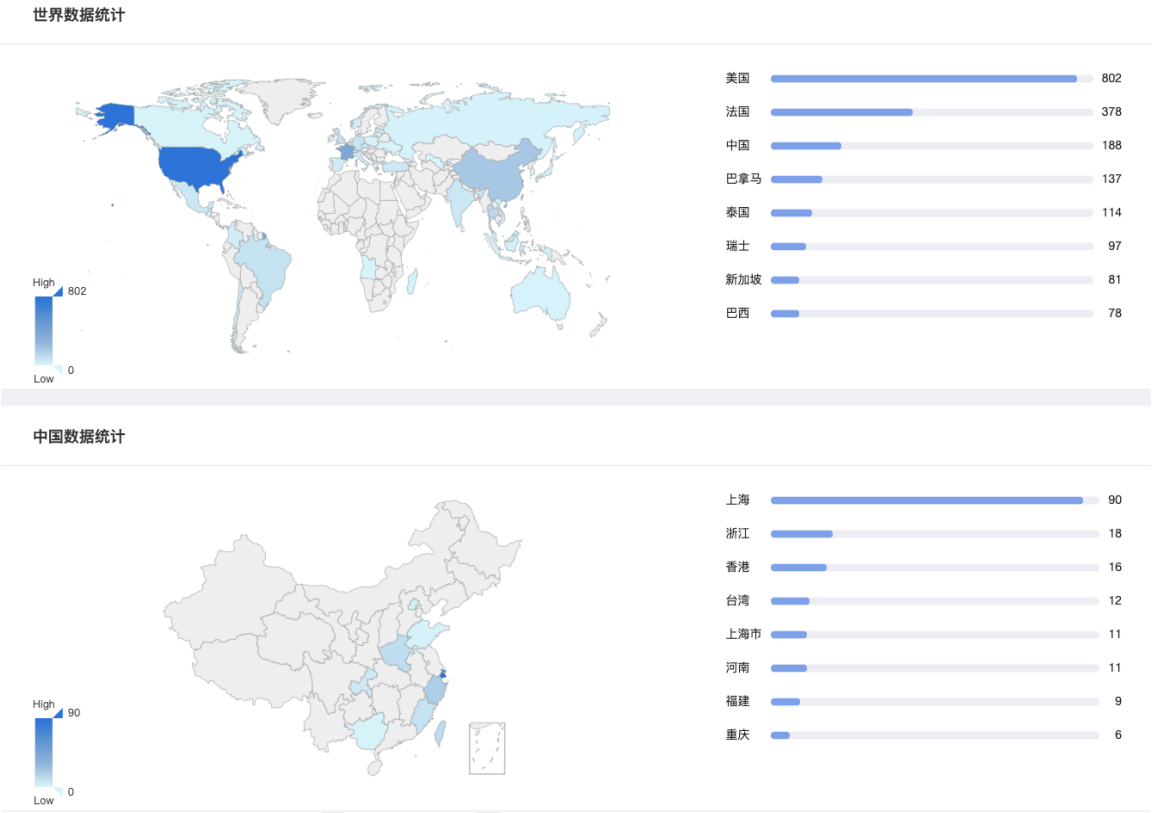
来源: Ax Sharma

标签: ['Zend Framework', 'PHP', 'Vulnerability', 'Deserialization', 'RCE']

2021 年 1 月 4 日`Zend Framework`披露了一个反序列化漏洞，该漏洞可能会被攻击者利用，成功利用能够在 PHP 站点上执行任意代码。

该漏洞编号为 CVE-2021-3007，同时影响`Zend`的`Laminas Project`的某些实例。
`Zend Framework`由 5.7 亿次安装的`PHP`软件包组成。 开发人员使用该框架来构建面向对象的 Web 应用程序。

目前 Zend Framework 的具体分布如下图，数据来自于 360 QUAKE




详情

Zend Framework remote code execution vulnerability revealed

https://www.bleepingcomputer.com/news/security/zend-framework-remote-code-execution-vulnerability-revealed/

## Google 警告严重的 Android 远程代码执行漏洞

日期: 2021-01-05

等级: 高

来源: Lindsey O'Donnell

标签: ['Google', 'Android System', 'Vulnerability', 'Qualcomm', 'Remote Code Execution']

Google 修复了两个影响其`Android`手机的严重漏洞，这些漏洞使远程攻击者可以执行任意代码。
这两个严重漏洞是 2021 年 1 月 5 日发布的`Google`一月`Android`安全公告的一部分。
该安全更新解决了`Android`操作系统的总共 43 个错误。
严重程度的漏洞包括`Google`的`Android`系统组件（CVE-2021-0316）中的远程执行代码漏洞，另一个被评为严重的漏洞是`Android`框架组件中的拒绝服务漏洞（CVE-2021-0313）

详情

Google Warns of Critical Android Remote Code Execution Bug

https://threatpost.com/google-warns-of-critical-android-remote-code-execution-bug/162756/

## 前副总裁恶意入侵公司，并破坏个人防护用品供应

日期: 2021-01-07

等级: 高

来源: Charlie Osborne

标签: ['PPE', 'Stradis Healthcare', 'Jail']

乔治亚州一家公司的一名前副总裁因恶意破坏系统和延误个人防护装备（PPE）的运送而被送进监狱。
`Christopher Dobbins`曾经在`Stradis`医疗保健公司工作，该公司是一家医疗设备包装公司，致力于提供 PPE，耗材和手术包。
在 2020 年 3 月被解雇后，这位 41 岁的年轻人访问了他在`Stradis`的工作期间创建的一个秘密的，伪造的员工帐户，并利用该账户开始破坏 `Stradis` 的电子记录。

详情

Former VP with an ax to grind hacks company, disrupts PPE supply, earns jail term

https://www.zdnet.com/article/former-vp-with-an-ax-to-grind-hacks-company-disrupts-ppe-supply-earns-jail-term/

## 新加坡警方可以获取 COVID-19 联系人追踪数据进行刑事调查

日期: 2021-01-04

等级: 中

来源: Eileen Yu

标签: ['Singapore', 'TraceTogether', 'COVID-19', 'Contact']

新加坡已经确认其执法人员将能够访问该国的`COVID-19`联系人追踪数据，以协助进行刑事调查。
迄今为止，已有 420 万居民或 78%的当地人口采用了`TraceTogether`联系人跟踪应用程序和可穿戴令牌，这是世界上普及率最高的应用之一。
`TraceTogether`于 2020 年三月推出，它利用蓝牙信号来检测其他参与移动设备。

详情

Singapore police can access COVID-19 contact tracing data for criminal investigations

https://www.zdnet.com/article/singapore-police-can-access-covid-19-contact-tracing-data-for-criminal-investigations/

## Slack 在 2021 年遭遇首次大规模停机

日期: 2021-01-04

等级: 中

来源: Lawrence Abrams

标签: ['Slack', 'Outage']

2021 年 1 月 4 日，从美国东部标准时间大约上午 10 点开始，Slack 出现了大规模宕机，用户无法连接，无法发送和接收消息，并且无法检索频道历史记录。
此次宕机将影响桌面客户端和`Web`界面，在撰写本文时，Web 界面显示了一个错误，称它们正在调查问题。

详情

Slack suffers its first massive outage of 2021

https://www.bleepingcomputer.com/news/technology/slack-suffers-its-first-massive-outage-of-2021/

## Citrix 更新 ADC 产品以修复 DDoS 攻击

日期: 2021-01-05

等级: 中

来源: Prajeet Nair

标签: ['DTLS', 'Citrix ADC', 'Gateway', 'DDos', 'Security Updates', 'Vulnerability']

2020 年 12 月，攻击者已开始滥用`Citrix`设备中的协议来放大`DDoS`攻击。
Citrix 敦促客户对其 ADC 和网关设备实施一项新提供的增强功能，该功能旨在阻止攻击者滥用数据报传输层安全性（DTLS）协议来放大分布式拒绝服务攻击。

详情

Citrix Updates ADC Products to Help Block DDoS Attacks

https://www.databreachtoday.com/citrix-updates-adc-products-to-help-block-ddos-attacks-a-15700

## Fortinet FortiWeb WAF 中的多个漏洞可让黑客攻击企业网络

日期: 2021-01-07

等级: 中

来源: Pierluigi Paganini

标签: ['Fortinet', 'FortiWeb', 'Web Application Firewall', 'Vulnerability']

Positive Technologies 的安全研究员 Andrey Medov 发现了 Fortinet 的 FortiWeb Web 应用防火墙（WAF）中存在多个严重漏洞，攻击者可能利用这些漏洞来入侵企业网络。
Fortinet 已通过发布安全修补程序修复了漏洞（漏洞编号为 CVE-2020-29015，CVE-2020-29016，CVE-2020-29018 和 CVE-2020-29019）。
这些漏洞包括 SQL 盲注，基于堆栈的缓冲区溢出问题，溢出缓冲区溢出以及格式字符串漏洞，这些漏洞可能导致执行未经授权的代码或命令或拒绝服务（DoS）。

详情

Multiple flaws in Fortinet FortiWeb WAF could allow corporate networks to hack

https://securityaffairs.co/wordpress/113129/hacking/fortinet-fortiweb-waf-flaws.html

## Nvidia 发布了针对 GPU 显示驱动程序和 vGPU 漏洞的安全更新

日期: 2021-01-08

等级: 中

来源: Pierluigi Paganini

标签: ['Nvidia', 'GPU', 'Security Updates ', 'CVE-2021-1051', 'Vulnerability']

Nvidia 已发布安全更新，以修复影响 Nvidia GPU 显示驱动程序和 vGPU 软件的高严重性漏洞。
修复的漏洞可能导致拒绝服务攻击，权限提升，数据篡改或信息泄露。
高危漏洞的 CVSS 分数为 8.4，编号为 CVE-2021-1051，它可能导致拒绝服务或特权升级。

详情

Nvidia releases security updates for GPU display driver and vGPU flaws
https://securityaffairs.co/wordpress/113186/security/nvidia-vgpu-gpu-flaws.html

## 摩根大通黑客被判 12 年监禁

日期: 2021-01-08

等级: 中

来源: Prajeet Nair

标签: ['JPMorgan Chase', 'Andrei Tyurin']

美国司法部 4 日宣布，一名承认黑客攻击摩根大通等金融机构的俄罗斯国民被判处 12 年联邦监禁。37 岁的安德烈·图林（Andrei Tyurin）在 2019 年 9 月对联邦指控认罪，包括共谋实施电脑黑客攻击、电信欺诈、共谋违反《非法互联网赌博执法法》、共谋实施电信欺诈和银行欺诈、共谋实施电信欺诈和共谋实施电脑黑客攻击。

详情

JPMorgan Chase Hacker Sentenced to 12 Years in Prison
https://www.databreachtoday.com/jpmorgan-chase-hacker-sentenced-to-12-years-in-prison-a-15730

## 相关安全建议

1. 及时对系统及各个服务组件进行版本升级和补丁更新
2. 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
3. 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

# 四、 产品侧解决方案

## （一）360 网络空间测绘系统

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。


## （二）360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn)获取对应产品。

## （三）360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。

# 附录 A 事件等级说明

| 高 | |
|---|---|
| 星级 | ★★★★/★★★★★ |
| 评定标准 | 1. 事件影响面十分广泛，受关注度高<br>2. 事件涉及的漏洞等级为严重/高危<br>3. 事件涉及机密/重要/核心数据，<br>4. 事件涉及数据量巨大<br>5. 事件涉及大型/常用厂商与组件<br>6. 事件涉及金额数目庞大/相关受害者损失高<br>7. 已知/潜在受害者数量庞大<br>8. 与日常生活/工作联系紧密 |
| 修复建议 | 建议在 3 个工作日内采取相关安全措施，并做好资产自测及预防工作 |

| 中 | |
|---|---|
| 星级 | ★★/★★★ |
| 危害结果 | 1. 事件影响面一般，受关注度中等<br>2. 事件涉及的漏洞等级为中危<br>3. 事件涉及数据机密性/重要性一般，<br>4. 事件涉及数据量中等<br>5. 事件涉及小型/常用厂商与组件<br>6. 事件涉及金额数目中等/相关受害者损失一般<br>7. 已知/潜在受害者数量中等<br>8. 与日常生活/工作联系一般 |
| 修复建议 | 建议在 7 个工作日内采取相关安全措施，并做好资产自测及预防工作 |

| 低 |
|---|

| | |
|---|---|
| 星级 | ★ |
| 危害结果 | 1. 事件影响面局限，受关注度低<br>2. 事件涉及的漏洞等级为低危<br>3. 事件涉及数据机密性/重要性低，<br>4. 事件涉及数据量低<br>5. 事件涉及小型/非常用厂商与组件<br>6. 事件涉及金额数目少/相关受害者损失低<br>7. 已知/潜在受害者数量少<br>8. 与日常生活/工作联系较小 |
| 修复建议 | 建议在 12 个工作日内采取相关安全措施，并做好资产自测及预防工作 |

# 附录 B 事件类型说明

| 网络攻击事件 | |
|---|---|
| 描述：通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对终端设备实施攻击，并造成终端设备异常或对终端设备当前运行造成潜在危害的信息安全事件。 | |
| 网络扫描 | 对网络边界设备及终端进行批量信息探测，包括端口扫描、服务指纹探测、DNS 查询等 |
| 漏洞利用 | 黑客使用 0day 或 nday，对系统及服务进行攻击 |
| web 攻击 | 黑客使用网络攻击技术，对 web 服务进行测试，包括 sql 注入、XSS、远程命令执行、恶意程序上传等 |
| 爆破事件 | 对网络设备及终端进暴力枚举及爆破，比如弱口令爆破、数据库爆破，系统路径爆破等 |
| 社工攻击 | 通过发送欺骗性垃圾邮件，或对目标发送构造的恶意信息，意图引诱目标给出敏感信息或者控制目标系统的攻击 |
| DDos | 使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。 |

| 恶意程序事件 | |
|---|---|
| 描述：通过网络、便携式存储设备等途径散播的，故意对终端设备等造成隐私或机密数据外泄、系统损害、数据丢失等非使用预期故障及信息安全问题的程序 | |
| 后门攻击 | 利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施攻击的信息安全事件 |
| 勒索软件 | 勒索程序将受害者的电脑上锁，或系统性地加密受害者硬盘上的文件，并要求受害者缴纳赎金以取回对电脑的控制权 |
| 挖矿程序 | 程序占用终端设备资源进行虚拟货币赚取，导致服务器无法正常工作 |
| 僵尸网络 | 采用一种或多种传播手段，将大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的可一对多控制的网络 |
| 蠕虫病毒 | 无须计算机使用者干预即可运行的独立程序，通过不停的取得网络中（存在漏洞的）计算机的部分或全部控制权来进行传播 |
| 其它病毒 | 除上述类别以外，其余未经许可，向终端设备植入的恶意程序 |

| 数据安全事件 | |
|---|---|
| 描述：通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件 | |
| 信息篡改 | 指未经授权，将信息系统中的信息更换为攻击者所提供的信息，而导致的信息安全事件，比如网页篡改、网页暗链等 |
| 信息假冒 | 通过假冒他人信息系统收发信息而导致的信息安全事件 |
| 信息泄漏 | 因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者，而导致的信息安全事件 |
| 信息窃取 | 未经授权用户利用可能的技术手段，主动恶意获取信息系统中信息而导致的信息安全事件 |
| 信息丢失 | 指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件 |
| 信息内容 | 利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件 |
| 其它信息破坏事件 | 指不能被包含在以上类别之中的信息破坏事件 |

| 其它安全事件 | |
|---|---|
| 描述：除开上述安全事件类型之外的事件 | |
| 设备设施故障 | 由于信息系统自身故障或外围保障设施故障，而导致的信息安全事件，以及人为地使用非技术手段，有意或无意的造成信息系统破坏，而导致的信息安全事件 |
| 灾害性事件 | 指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。 |
| 其它事件 | 不能归类于上述事件的安全事件 |