# 安全事件周报

安全事件周报 (05.31-06.06)



360CERT
北京奇虎科技有限公司

# 报告信息

| | | | |
|---|---|---|---|
| 报告名称 | 安全事件周报 (05.31-06.06) | | |
| 报告类型 | 安全事件周报 | 报告编号 | |
| 报告版本 | 1 | 报告日期 | 2021-06-07 |
| 报告作者 | 360CERT | 联系方式 | g-cert-report@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 | 2021-06-07 | 360CERT | 360CERT | 撰写报告 |

# 目录

# 1 事件导览

本周收录安全热点13项，话题集中在恶意软件、漏洞信息方面，涉及的组织有：JBSFoods、VMware、HUAWEI、瑞典卫生局等。勒索软件重创食品加工行业，APT 式特定目标勒索如何防护是重中之重。对此，360CERT 建议使用360安全卫士进行病毒检测、使用360安全分析响应平台进行威胁流量检测，使用360城市级网络安全监测服务QUAKE进行资产测绘，做好资产自查以及预防工作，以免遭受黑客攻击。

| 恶意程序 |
| --- |
| 食品巨头 JBS Foods 遭受勒索软件攻击后停产 |
| 美国：JBS 遭受勒索软件攻击背后可能是俄罗斯攻击者 |
| Android 恶意软件窃取银行信息 |
| FBI 将 JBS 遭受的勒索软件攻击归咎于 REvil |
| 马萨诸塞州最大的渡轮服务遭遇勒索软件攻击 |
| 俄罗斯黑客利用新的 SkinnyBoy 恶意软件入侵敏感组织 |

| 网络攻击 |
| --- |
| 研究人员发现了针对韩国政府的黑客行动 |
| 瑞典卫生局在黑客攻击后关闭 SmiNet |

| 其它事件 |
| --- |
| 拜登敦促俄罗斯停止窝藏勒索团伙 |
| 攻击者扫描未修补的 VMware vCenter 服务器，PoC 可用 |
| 华为 USB LTE 加密狗易受权限提升攻击 |
| CODESYS 工业自动化软件中发现 10 个严重漏洞 |
| 谷歌发现改变芯片内存的新漏洞 |

# 2 恶意程序

## 2.1 食品巨头 JBS Foods 遭受勒索软件攻击后停产

```
日期：2021 年 05 月 31 日
等级：高
作者：Sergiu Gatlan
标签：JBS Foods, Meat
行业：制造业
```

JBS 目前是全球最大的牛肉和家禽生产商，也是全球第二大猪肉生产商，在美国、澳大利亚、加拿大、英国等地都有业务。在一次网络攻击后，该公司不得不在全球多个地点停产。这起事件影响了包括美国、澳大利亚和加拿大在内的全球多家 JBS 生产设施。

**详情**

Food giant JBS Foods shuts down production after cyberattack

## 2.2 美国：JBS 遭受勒索软件攻击背后可能是俄罗斯攻击者

1 日期：2021 年 06 月 01 日
2 等级：高
3 作者：Sergiu Gatlan
4 标签：White House, JBS, Russia
5 行业：制造业
6 涉及组织：JBS

白宫证实，世界最大的牛肉生产商 JBS 遭到勒索软件袭击，袭击者可能来自俄罗斯。虽然该公司已经发表了一份官方声明，称其北美和澳大利亚的一些 IT 系统受到网络攻击的影响，但并未称之为勒索软件攻击。不过白宫首席副新闻秘书皮埃尔对记者说，总部设在巴西的 JBS 证实收到了可能来自俄罗斯的袭击者的赎金要求。联邦调查局已经开始调查这一事件，美国政府已经开始与俄罗斯政府联系。

**详情**

US: Russian threat actors likely behind JBS ransomware attack

## 2.3 Android 恶意软件窃取银行信息

1 日期：2021 年 06 月 01 日
2 等级：高
3 作者：Danny Palmer
4 标签：Android, TeaBot, Anatsa
5 行业：信息传输、软件和信息技术服务业

TeaBot（也称为 Anatsa）能够完全远程控制 Android 设备，允许网络犯罪分子借助键盘记录和窃取身份验证码来窃取银行信息和其他敏感信息。该恶意软件于去年 12

月首次出现，至今仍然在传播。TeaBot 还试图通过伪装成流行应用程序诱骗受害者下载恶意软件。

**详情**

This Android trojan malware is using fake apps to infect smartphones, steal bank details

## 2.4 FBI 将 JBS 遭受的勒索软件攻击归咎于 REvil

1 日期：2021 年 06 月 03 日
2 等级：高
3 作者：Chris Duckett
4 标签：JBS, REvil, FBI
5 行业：制造业
6 涉及组织：JBS

美国联邦调查局（FBI）发表简短声明，将最近发生的 JBS 遭受勒索软件事件归咎于 REvil。作为打击网络威胁的主要联邦调查机构，打击网络犯罪是联邦调查局的最高优先事项之一。目前已经将 JBS 的攻击归咎于 REvil 和 Sodinokibi，并正在努力将攻击者绳之以法。

**详情**

FBI attributes JBS ransomware attack to REvil

## 2.5 马萨诸塞州最大的渡轮服务遭遇勒索软件攻击

1 日期：2021 年 06 月 03 日
2 等级：高

3 作者：Sergiu Gatlan
4 标签：Steamship Authority, Attack
5 行业：交通运输、仓储和邮政业

---

马萨诸塞州最大的渡轮服务公司轮船管理局（SteamshipAuthority）遭到勒索软件攻击，导致售票和预订中断。在发布的最新消息中，轮船管理局表示，他们仍在努力恢复服务。

**详情**

Massachusetts' largest ferry service hit by ransomware attack

## 2.6 俄罗斯黑客利用新的 SkinnyBoy 恶意软件入侵敏感组织

1 日期：2021 年 06 月 03 日
2 等级：高
3 作者：Ionut Ilascu
4 标签：SkinnyBoy, Fancy Bear
5 行业：政府机关、社会保障和社会组织

---

安全研究人员发现了一个名为 SkinnyBoy 的新恶意软件，该软件用于俄语黑客组织 APT28 的鱼叉式网络钓鱼活动。在早些时候，这个名为"花式熊"（FancyBear）的恐怖分子在针对军方和政府机构的攻击中使用了 SkinnyBoy。SkinnyBoy 用于攻击的中间阶段，用于收集有关受害者的信息，并从指挥与控制（C2）服务器检索下一个有效负载。

**详情**

New SkinnyBoy malware used by Russian hackers to breach sensitive orgs

## 2.7 ** 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. 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
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. 各主机安装 EDR 产品，及时检测威胁
6. 注重内部员工安全培训
7. 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
8. 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

# 3 网络攻击

## 3.1 研究人员发现了针对韩国政府的黑客行动

```
日期：2021 年 06 月 02 日
等级：高
作者：The Hacker News
标签：North Korean, Android, Kimsuky
行业：政府机关、社会保障和社会组织
```

一名自 2012 年以来活跃的朝鲜攻击者一直在幕后策划一场新的间谍活动，目标是与韩国相关的高级政府官员，通过安装安卓和 Windows 后门以收集敏感信息。网络安全公司 Malwarebytes 追踪这一活动并定位到一名叫 Kimsuky 的攻击者，其攻击目标包括韩国互联网与安全局（KISA）、外交部、斯里兰卡驻斯里兰卡大使馆大使、国际

原子能机构（IAEA）核安全官员、韩国驻香港总领事馆副总干事、国立首尔大学和大信证券。

**详情**

Researchers Uncover Hacking Operations Targeting Government Entities in South Korea

## 3.2 瑞典卫生局在黑客攻击后关闭 SmiNet

```
日期：2021 年 05 月 31 日
等级：高
作者：Sergiu Gatlan
标签：The Swedish Public Health Agency, SmiNet, COVID-19
行业：卫生和社会工作
```

瑞典公共卫生署（SwedishPublicHealthAgency）关闭了该国传染病数据库 SmiNet，SmiNet 也被用来存储有关 COVID-19 感染的电子报告，此前该数据库曾多次遭到黑客攻击。瑞典公共卫生署发现，2021 年 5 月底有人试图入侵 SmiNet 数据库。因此，该数据库已暂时关闭。

**详情**

Swedish Health Agency shuts down SmiNet after hacking attempts

## 3.3 ** 相关安全建议 **

1. 积极开展外网渗透测试工作，提前发现系统问题
2. 减少外网资源和不相关的业务，降低被攻击的风险
3. 做好产品自动告警措施

4. 及时对系统及各个服务组件进行版本升级和补丁更新
5. 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
6. 注重内部员工安全培训

# 4 其它事件

## 4.1 拜登敦促俄罗斯停止窝藏勒索团伙

```
日期：2021 年 06 月 03 日
等级：高
作者：Joe Uchill
标签：White House, Biden, Moscow, Russia
行业：政府机关、社会保障和社会组织
```

在白宫新闻发布会上，新闻秘书詹·普萨基告诉记者，拜登总统将在即将与俄罗斯总统普京举行的峰会上提到莫斯科对本国勒索软件业的不作为。在其他地方，美国国务卿布林肯（antonyblinken）表示，俄罗斯需要为其境内的犯罪分子承担责任。

**详情**

Biden presses Russia to stop harboring ransomware gangs

## 4.2 攻击者扫描未修补的 VMware vCenter 服务器，PoC 可用

```
日期：2021 年 06 月 04 日
等级：高
```

作者：Sergiu Gatlan
标签：VMware, RCE, vCenter
行业：信息传输、软件和信息技术服务业
涉及组织：vmware

攻击者正在大肆扫描暴露在互联网上的 VMwarevCenter 服务器，这些服务器未针对影响所有 vCenter 的严重远程代码执行（RCE）漏洞进行修补。并且安全研究人员还开发并发布了针对 VMwarevCenter 漏洞（CVE-2021-21985）的 PoC。

#### 4.2.1 涉及漏洞

- CVE-2021-21972
- CVE-2021-21985

#### 4.2.2 攻击方式

- Compromise Application Executable

**详情**

Attackers scan for unpatched VMware vCenter servers, PoC exploit available

### 4.3 华为 USB LTE 加密狗易受权限提升攻击

日期：2021 年 06 月 02 日
等级：高
作者：Ax Sharma
标签：USB, Huawei

行业：信息传输、软件和信息技术服务业
涉及组织：huawei

---

USB 加密狗是一种可以插入笔记本电脑和台式电脑的硬件，很像一个 USB 驱动器，可以访问互联网。但是，在 USB 加密狗快速分析华为 LTE 设备驱动程序的同时，Trustwave 研究人员发现了一个不正确权限的案例。Trustwave 的安全研究经理 martinrakhmanov 透露了他对华为的 USBLTE 加密狗 E3372 的特权提升漏洞的研究结果。在浏览由加密狗安装在 MacOSX 机器上的驱动程序文件时，研究人员发现每次插入 USB 加密狗时都会有一些文件会自动运行，并且这些文件是以完全权限运行的（777）。当攻击者将恶意代码写入文件，具有权限的用户访问后，就会导致本地权限提升。

**详情**

Huawei USB LTE dongles are vulnerable to privilege escalation attacks

## 4.4 CODESYS 工业自动化软件中发现 10 个严重漏洞

---

日期：2021 年 06 月 04 日
等级：高
作者：The Hacker News
标签：CODESYS, PLC, CVE
行业：跨行业事件

---

网络安全研究人员披露了多达 10 个影响 CODESYS 自动化软件的严重漏洞，这些漏洞可被利用在可编程逻辑控制器（PLC）上远程执行代码。安全技术人员说："要利用这些漏洞，攻击者不需要用户名或密码，有网络接入工业控制器就足够了。"

#### 4.4.1 涉及漏洞

- CVE-2021-30193
- CVE-2021-30189
- CVE-2021-30191
- CVE-2021-30194
- CVE-2021-30188
- CVE-2021-30186
- CVE-2021-30192
- CVE-2021-30195
- CVE-2021-30190
- CVE-2021-30187

**详情**

10 Critical Flaws Found in CODESYS Industrial Automation Software

### 4.5 谷歌发现改变芯片内存的新漏洞

```
日期：2021 年 06 月 04 日
等级：高
作者：Prajeet Nair
标签：Google, Rowhammer
行业：制造业
```

谷歌的研究人员发现了一种新的 Rowhammer 技术，称为半双工技术，它利用现代 DRAM 芯片的设计漏洞来改变内存内容。Rowhammer 于 2014 年首次发现，是一个 DRAM 漏洞，重复访问一个地址可能会篡改存储在其他地址中的数据。

**详情**

Google Finds New Exploit That Alters Chip Memory

### 4.6 ** 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

## 5 时间线

**2021-06-07** 360CERT 发布安全事件周报

# A 产品侧解决方案

## A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，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。


## A.2 360 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，对网络攻击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。


## A.3 360 安全卫士

针对以上安全事件，360cert 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。