# 安全事件周报

## 安全事件周报 (05.03-05.09)



360CERT
北京奇虎科技有限公司 | 2021-05-10

# 报告信息

| | | | |
|---|---|---|---|
| 报告名称 | 安全事件周报（05.03-05.09） | | |
| 报告类型 | 安全事件周报 | 报告编号 | B6-2021-051001 |
| 报告版本 | 1.0 | 报告日期 | 2021-05-10 |
| 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 | 2021-05-10 | 360CERT | 360CERT | 撰写报告 |

# 目录

# 一、 事件概览


本周收录安全事件 13 项

话题集中在`漏洞修复`、`勒索软件`方面，涉及的组织有：`Apple`、`VMware`、`Intel`、`AMD`等。多个严重漏洞曝光，各厂商注意及时修复。

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 Windows"Pingback"恶意软件使用 ICMP 进行隐蔽通信 | ★★★★ |
| Panda Stealer 放入 Excel 文件中，通过 Discord 传播以窃取用户加密货币 | ★★★★ |
| 新的 rootkit 后门瞄准 Windows 系统 | ★★★★ |
| **数据安全** | **等级** |
| 到目前为止，勒索团伙已经泄露了 2100 家公司的被盗数据 | ★★★★ |
| **网络攻击** | **等级** |
| DDoS 攻击使比利时政府网站离线 | ★★★★ |
| 俄罗斯间谍黑客利用的 12 大安全漏洞 | ★★★★ |
| Colonial Pipeline 遭遇网络攻击并关闭运营 | ★★★★ |
| **其他事件** | **等级** |
| 苹果紧急发布 0day 漏洞安全补丁 | ★★★★★ |
| 严重的 Exim 漏洞使数百万台服务器受到攻击 | ★★★★★ |
| VMware 修复了 vRealize Business for Cloud 中严重漏洞 | ★★★★★ |
| 英特尔和 AMD CPU 中的新幽灵漏洞影响了数十亿台计算机 | ★★★★★ |
| 高通芯片漏洞影响大量安卓主流手机 | ★★★★★ |
| 微软发现针对数十个组织的商业电子邮件泄露攻击 | ★★★★ |

# 三、 事件详情

## (一) 恶意程序

### 新的 Windows“Pingback”恶意软件使用 ICMP 进行隐蔽通信

日期: 2021-05-04

等级: 高

来源: Ax Sharma

标签: ['Windows', 'Pingback']

研究人员公布了他们在一个新的 Windows 恶意软件样本上的发现，该样本使用互联网控制消息协议（ICMP）进行命令和控制（C2）活动。这个被称为“Pingback”的恶意软件以 Microsoft Windows 64 位系统为目标，利用 DLL 劫持获得持久性。

详情

New Windows 'Pingback' malware uses ICMP for covert communication

https://www.bleepingcomputer.com/news/security/new-windows-pingback-malware-uses-icmp-for-covert-communication/

### Panda Stealer 放入 Excel 文件中，通过 Discord 传播以窃取用户加密货币

日期: 2021-05-05

等级: 高

来源: Charlie Osborne

标签: ['Trend Micro', 'Panda Stealer', 'Excel']

Panda Stealer，一个盗取加密货币的恶意软件，正在通过钓鱼邮件进行传播。Trend Micro 的研究人员称，Panda Stealer 的目标是美国、澳大利亚、日本和德国等国家的个人。Panda Stealer 通过网络钓鱼邮件开始其感染链，上传到 VirusTotal 的样本还表明，受害者一直通过链接从恶意网站下载可执行文件。

详情

Panda Stealer dropped in Excel files, spreads through Discord to steal user cryptocurrency

https://www.zdnet.com/article/panda-stealer-dropped-in-discord-to-steal-user-cryptocurrency/

### 新的 rootkit 后门瞄准 Windows 系统

日期: 2021-05-06

等级: 高

来源: Sergiu Gatlan

标签: ['TunnelSnake', 'Windows']

一个未知的攻击者使用了一个新的 rootkit 后门攻击 Windows 系统，这似乎是一项秘密进行的间谍活动，被称为 TunnelSnake，至少可以追溯到 2018 年。rootkit 是一种恶意工

具，旨在通过深入操作系统来逃避检测，攻击者利用它在逃避检测的同时完全接管受感染的系统。

详情

New Moriya rootkit used in the wild to backdoor Windows systems

https://www.bleepingcomputer.com/news/security/new-moriya-rootkit-used-in-the-wild-to-backdoor-windows-systems/

## 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

# (二) 数据安全

## 到目前为止，勒索团伙已经泄露了 2100 家公司的被盗数据

日期: 2021-05-08

等级: 高

来源: Lawrence Abrams

标签: ['DarkTracer', 'Ransomware', 'Dark Net']

自 2020 年初以来，勒索团伙开始实施一种称为双重勒索的新策略。双重勒索是指勒索软件在加密网络之前窃取未加密的文件。如果受害者不支付赎金，他们将在暗网上公开发布被盗文件。到 2021 年 5 月，勒索团伙已经泄露了 2103 个组织的数据。

详情

Ransomware gangs have leaked the stolen data of 2,100 companies so far

https://www.bleepingcomputer.com/news/security/ransomware-gangs-have-leaked-the-stolen-data-of-2-100-companies-so-far/

## 相关安全建议

1. 及时备份数据并确保数据安全
2. 合理设置服务器端各种文件的访问权限
3. 严格控制数据访问权限
4. 及时检查并删除外泄敏感数据

5. 发生数据泄漏事件后，及时进行密码更改等相关安全措施
6. 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

## (三) 网络攻击

### DDoS 攻击使比利时政府网站离线

日期: 2021-05-05

等级: 高

来源: AmerOwaida

标签: ['Belgium', 'Belnet']

比利时公共部门的互联网服务提供商 Belnet 遭到大规模分布式拒绝服务（DDoS）攻击后，比利时许多政府网站和服务被迫下线。此次攻击影响了使用 Belnet 服务的大约 200 个机构和组织。公共办公室、大学和研究机构都部分或全部无法上网，其网站几乎无法访问。

详情

DDoS attack knocks Belgian government websites offline

https://www.welivesecurity.com/2021/05/05/belgium-government-websites-offline-ddos-attack/

### 俄罗斯间谍黑客利用的 12 大安全漏洞

日期: 2021-05-08

等级: 高

来源: CISA

标签: ['NCSC', 'SVR', 'CISA']

根据英国和美国情报机构联合发布的新咨询报告，称隶属于俄罗斯外国情报局（SVR）的网络特工已改变其攻击策略，利用以下漏洞对各国单位进行网络攻击。

详情

Top 12 Security Flaws Russian Spy Hackers Are Exploiting in the Wild

https://us-cert.cisa.gov/ncas/current-activity/2021/05/07/joint-ncsc-cisa-fbi-nsa-cybersecurity-advisory-russian-svr

### Colonial Pipeline 遭遇网络攻击并关闭运营

日期: 2021-05-08

等级: 高

来源: Larry Dignan

标签: ['Colonial Pipeline', 'Fuel']

5 月 7 日，Colonial Pipeline 遭遇网络攻击并关闭运营。该公司为美国军方提供汽油、柴油、喷气燃料、家用取暖油和燃料等精炼石油产品，占东海岸 45%燃料供应量。这次攻击凸显了勒索软件和其他网络攻击对现实世界基础设施的威胁越来越大。

详情

Colonial Pipeline cyberattack shuts down pipeline that supplies 45% of East Coast's fuel
https://www.zdnet.com/article/colonial-pipeline-cyberattack-shuts-down-pipeline-that-supplies-45-of-east-coasts-fuel/

### 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

## (四) 其他事件

### 苹果紧急发布 0day 漏洞安全补丁

日期: 2021-05-03

等级: 高

来源: The Hacker News

标签: ['Apple', 'iOS', 'macOS', 'WatchOS']

苹果发布了 iOS、macOS 和 watchOS 的安全更新，以解决三个 0day 漏洞，并扩展了第四个漏洞的修补程序。这些漏洞都与 WebKit 有关，WebKit 是一个浏览器引擎，在 iOS 中为 Safari 和其他第三方 web 浏览器提供动力。这些漏洞允许攻击者在目标设备上执行任意代码。

详情

Apple Releases Urgent Security Patches For Zero-Day Bugs Under Active Attacks
https://thehackernews.com/2021/05/apple-releases-urgent-security-patches.html

### 严重的 Exim 漏洞使数百万台服务器受到攻击

日期: 2021-05-04

等级: 高

来源: Sergiu Gatlan

标签: ['Exim', 'MTA']

Exim 邮件传输代理（MTA）软件中新发现的严重漏洞，允许未经验证的远程攻击者在具有默认或通用配置的邮件服务器上执行任意代码，并获得 root 权限。Qualys 研究小组发现并报告的安全漏洞（10 个可远程利用，11 个可本地利用）统称为 21A。Exim 4.94.2 之前发布的所有版本都容易受到攻击。

详情

Critical 21Nails Exim bugs expose millions of servers to attacks

https://www.bleepingcomputer.com/news/security/critical-21nails-exim-bugs-expose-millions-of-servers-to-attacks/

## VMware 修复了 vRealize Business for Cloud 中严重漏洞

日期: 2021-05-05

等级: 高

来源: Sergiu Gatlan

标签: ['VMware', 'vRealize', 'RCE']

VMware 发布了安全更新，以解决 vRealize Business for Cloud 中的一个严重漏洞，该漏洞使未经验证的攻击者能够在易受攻击的服务器上远程执行恶意代码。vRealize Business for Cloud 是一个自动化的云业务管理解决方案，旨在为 IT 团队提供云规划、预算和成本分析工具。该安全漏洞被跟踪为 CVE-2021-21984，它会影响运行 VMware vRealize Business for Cloud 7.6.0 之前版本的虚拟设备。

详情

VMware fixes critical RCE bug in vRealize Business for Cloud

https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-vrealize-business-for-cloud/

## 英特尔和 AMD CPU 中的新幽灵漏洞影响了数十亿台计算机

日期: 2021-05-06

等级: 高

来源: The Hacker News

标签: ['Spectre', 'ARM', 'AMD']

2018 年 1 月，影响现代处理器的一类严重幽灵漏洞（Spectre）被公开披露。研究人员表示，“由于不易修复，它将存在相当长一段时间”。事实上，已经过去三年多了，这一漏洞仍旧没有解决。来自弗吉尼亚大学和加州大学圣地亚哥分校的一组学者发现了一条新的攻击线，它绕过了芯片中内置的当前所有保护，可能使几乎所有系统——台式机、笔记本电脑、云服务器和智能手机——再次像三年前一样面临风险。其间数年来，尽管英特尔、ARM 和 AMD 等芯片制造商一直在争先恐后地加入防御系统，各种各样的攻击仍然层出不穷。

详情

New Spectre Flaws in Intel and AMD CPUs Affect Billions of Computers

https://thehackernews.com/2021/05/new-spectre-flaws-in-intel-and-amd-cpus.html

## 高通芯片漏洞影响大量安卓主流手机

日期: 2021-05-07

等级: 高

来源: Jonathan Greig

标签: ['Qualcomm', 'Android']

以色列网络安全公司 Checkpoint 的研究人员称，全球数百万部手机受到普遍存在的高通芯片组漏洞的影响。Check Point 的 Slava Makkaveev 发表了一篇博客文章，强调了高通

公司移动站调制解调器接口中的一个安全漏洞。这使得攻击者能够访问用户的通话记录和短信息，以及监听用户对话。

详情

Qualcomm chip vulnerability found in millions of Google, Samsung, and LG phones

https://www.zdnet.com/article/qualcomm-chip-vulnerability-found-in-millions-of-google-samsung-and-lg-phones/

## 微软发现针对数十个组织的商业电子邮件泄露攻击

日期: 2021-05-07

等级: 高

来源: Sergiu Gatlan

标签: ['Microsoft', 'BEC', 'Email']

微软发现了一个大规模的商业电子邮件妥协（BEC）活动，目标是 120 多个组织，使用的是在攻击开始前几天注册的拼写错误域名。BEC 诈骗者使用各种策略（包括社会工程、网络钓鱼或黑客攻击）来危害商业电子邮件帐户，后来用于将付款重定向到其控制下的银行帐户。

详情

Microsoft: Business email compromise attack targeted dozens of orgs

https://www.bleepingcomputer.com/news/security/microsoft-business-email-compromise-attack-targeted-dozens-of-orgs/

## 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

# 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 |