安全事件周报

安全事件周报 (03.08-03.14)

360CERT
北京奇虎科技有限公司 | 2021-03-15

报告信息

报告名称	安全事件周报（03.08-03.14）		
报告类型	安全事件周报	报告编号	B6-2021-031501
报告版本	1.0	报告日期	2021-03-15
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	2021-03-15	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 10 项

话题集中在`漏洞`、`恶意软件`方面，涉及的组织有：`Microsoft`、`OVH`、`施耐德`、`Powerhouse`等。黑客利用 Exchange 漏洞扫描全球，各厂商务必尽快修复。

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**
Ryuk 勒索软件袭击了 700 个西班牙政府劳工局办公室	★★★★
新的 ZHtrap 僵尸网络恶意软件部署蜜罐来寻找更多的目标	★★★★
Metamorfo 银行木马滥用 AutoHotKey	★★★★
网络攻击	**等级**
全球已有 3 万台服务器遭到 Microsoft Exchange 0day 攻击	★★★★★
伊朗黑客利用远程工具攻击中东和邻近地区	★★★★
其他事件	**等级**
至少有 10 个 APT 组织利用 Microsoft Exchange 漏洞进行攻击	★★★★★
OVH 数据中心火灾，大量数据损毁	★★★★★
微软 3 月补丁日修复了 82 个漏洞，2 个 0day	★★★★
网络攻击者利用严重的 WordPress 插件漏洞	★★★★
严重的安全漏洞会导致智能电表离线	★★★★

三、 事件详情

(一) 恶意程序

Ryuk 勒索软件袭击了 700 个西班牙政府劳工局办公室

日期: 2021-03-10

等级: 高

来源: Sergiu Gatlan

标签: ['SEPE', 'Spanish', 'Spain', 'Ryuk', 'Ransomware']

SEPE 是西班牙政府的劳工机构，在遭到勒索软件攻击之后，该系统被关闭，此次攻击袭击了西班牙 700 多家代理商。
该机构网站上的一份声明称:"目前，正在努力尽快恢复优先服务，其中包括国家公共就业服务门户，然后逐步向公民、公司、福利和就业办公室提供其他服务。"
SEPE 主管 Gerado Guitérrez 证实，事件发生后，该机构的网络系统被 Ryuk 勒索软件运营商加密。

详情

Ryuk ransomware hits 700 Spanish government labor agency offices

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-hits-700-spanish-government-labor-agency-offices/

新的 ZHtrap 僵尸网络恶意软件部署蜜罐来寻找更多的目标

日期: 2021-03-12

等级: 高

来源: Sergiu Gatlan

标签: ['UPnP', 'ZHtrap', 'Honeypots']

新的僵尸网络正在将受感染的路由器、dvr 和 UPnP 网络设备转化为蜜罐，帮助它找到其他感染目标。这个被 360 Netlab 安全研究人员称为 ZHtrap 的恶意软件基于 Mirai 的源代码构建，并支持 x86、ARM、MIPS 和其他 CPU 架构。僵尸网络的主要功能包括 DDoS 攻击和扫描更易受感染的设备。但是，它还具有后门功能，允许操作员下载和执行其他恶意有效负载。ZHtrap 使用了类似蜜罐的技术，以此来进行 IP 收集。

详情

New ZHtrap botnet malware deploys honeypots to find more targets

https://www.bleepingcomputer.com/news/security/new-zhtrap-botnet-malware-deploys-honeypots-to-find-more-targets/

Metamorfo 银行木马滥用 AutoHotKey

日期: 2021-03-12

等级: 高

来源: Tara Seals

标签: ['Metamorfo', 'AutoHotKey', 'Phishing']

Metamorfo 银行特洛伊木马正在滥用 AutoHotKey（AHK）和 AHK 编译器来逃避检测并窃取用户信息。AHK 是一种 Windows 脚本语言，最初是为创建快捷键而开发的。据科芬斯网络钓鱼防御中心（PDC）称，该恶意软件以西班牙语用户为目标，使用两封单独的电子邮件作为初始感染媒介。一个是所谓的下载受密码保护的文件的请求；另一个是关于未决法律文件的精心伪造的通知，带有下载.ZIP 文件的链接。在这两种情况下，恶意代码都包含在最终下载到受害计算机的.ZIP 文件中。

详情

Metamorfo Banking Trojan Abuses AutoHotKey
https://threatpost.com/metamorfo-banking-trojan-autohotkey/164735/

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. 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
4. 减少外网资源和不相关的业务，降低被攻击的风险
5. 条件允许的情况下，设置主机访问白名单
6. 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) 网络攻击

全球已有 3 万台服务器遭到 Microsoft Exchange 0day 攻击

日期: 2021-03-08
等级: 高
来源: Liam Tung
标签: ['Microsoft Exchange Server', 'Zero-Day', 'Hafnium']

安全研究人员称，Microsoft Exchange Server 中的 0day 漏洞正用于对数以千计的组织的广泛攻击，潜在的成千上万的组织受到影响。
这些漏洞的 CVE 编号为 CVE-2021-26855，CVE-2021-26857，CVE-2021-26858 和 CVE-2021-27065。
微软将此次攻击归因于一个新成立的黑客团队，该团队名为 Hafnium。
微软表示，这些是有限的针对性攻击，但可能会在不久的将来攻击范围更加广泛。

详情

zero-day attacks: 30,000 servers hit already, says report
https://www.zdnet.com/article/microsoft-exchange-zero-day-attacks-30000-servers-hit-already-says-report/

伊朗黑客利用远程工具攻击中东和邻近地区

日期: 2021-03-08

等级: 高

来源: The Hacker News

标签: ['Earth Vetala', 'ScreenConnect', 'MuddyWater', 'PowerShell', 'RemoteUtilities']

涉嫌与伊朗有联系的黑客正攻击中东及周边地区的学术界、政府机构和旅游实体，这是一场旨在窃取数据的间谍活动。
这一最新发现被趋势科技公司称为"Earth Vetala"，该研究发现有证据表明，有恶意活动利用`ScreenConnect`远程管理工具，针对阿联酋和科威特政府机构。
攻击者是伊朗黑客组织`MuddyWater`，该组织主要对中东国家发动攻势。

详情

Iranian Hackers Using Remote Utilities Software to Spy On Its Targets
https://thehackernews.com/2021/03/iranian-hackers-using-remote-utilities.html?m=1

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. 积极开展外网渗透测试工作，提前发现系统问题
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. 注重内部员工安全培训

(三) 其他事件

至少有 10 个 APT 组织利用 Microsoft Exchange 漏洞进行攻击

日期: 2021-03-11

等级: 高

来源: Doug Olenick

标签: ['ESET', 'Microsoft Exchange', 'APT']

据斯洛伐克安全公司 ESET 的研究人员称，在过去三个月里，至少有 10 个 APT（高级持续性威胁）组织利用未修补的 Microsoft Exchange 漏洞攻击了数千家公司。
ESET 的研究人员公布了每一次攻击的细节，并指出了 APT 所涉及的组织，或者指出了一个未知的团伙进行了这次攻击。
ESET 说，在 1 月 5 日微软收到漏洞通知之前，几个 APT 组织就已经开始攻击了。

详情

At Least 10 APT Groups Exploiting Exchange Flaws
https://www.databreachtoday.com/at-least-10-apt-groups-exploiting-exchange-flaws-a-16166

OVH 数据中心火灾，大量数据损毁

日期: 2021-03-12

等级: 高

来源: Ax Sharma

标签: ['OVH', 'UPS']

法国斯特拉斯堡 OVHCloud 是欧洲最大的主机提供商，也是世界第三大主机提供商。其数据中心遭到了大火的袭击，数据中心托管的站点服务器遭到焚毁，雪上加霜的是服务器中的实时数据并未在其他地点备份。包括巴黎艺术中心和图书馆 Pompidou 以及新闻网站 EENews 等大量公司的数据将难以恢复。火灾原因目前定义为 UPS 电源故障。

详情

OVH data center fire likely caused by faulty UPS power supply

https://www.bleepingcomputer.com/news/security/ovh-data-center-fire-likely-caused-by-faulty-ups-power-supply/

微软 3 月补丁日修复了 82 个漏洞，2 个 0day

日期: 2021-03-09

等级: 高

来源: Lawrence Abrams

标签: ['Microsoft', 'Security Updates', 'Exchange']

在 2021 年 3 月 9 日的更新中，微软已经修复了 82 个漏洞，其中 10 个是严重漏洞，72 个是高危漏洞。这些数字不包括 3 月早些时候发布的 7 个 Microsoft Exchange 和 33 个 Chromium Edge 漏洞。
3 月 9 日还修补了两个 0day 漏洞，这些漏洞已公开披露并已知可用于攻击。

详情

Microsoft March 2021 Patch Tuesday fixes 82 flaws, 2 zero-days

https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2021-patch-tuesday-fixes-82-flaws-2-zero-days/

网络攻击者利用严重的 WordPress 插件漏洞

日期: 2021-03-10

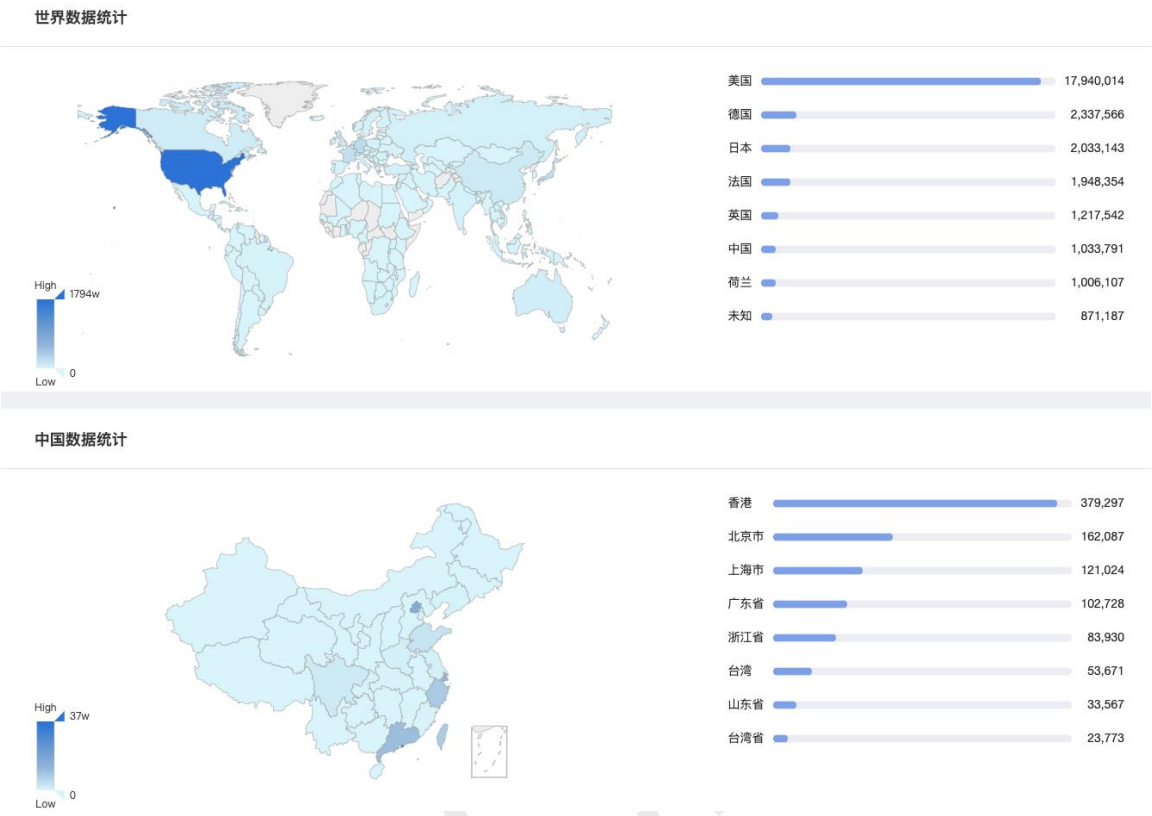
等级: 高

来源: Tara Seals

标签: ['WordPress', 'Elementor', 'CVE-2021-24175', 'Plugin']

用于 WordPress 的 Elementor 插件的 Plus 插件有一个严重的安全漏洞，攻击者可以利用该漏洞快速、轻松地远程接管网站。
研究人员称，该漏洞目前有在野利用。根据开发者的说法，这个插件有超过 30000 个安装。
该漏洞（CVE-2021-24175）是 Elementor 的 Plus Addons 的注册表单函数中存在的特权升级和身份验证绕过问题。
它的 CVSS 评分为 9.8，漏洞危害等级为严重。

目前 wordpress 的具体分布如下图，数据来自于 360 QUAKE



详情

Cyberattackers Exploiting Critical WordPress Plugin Bug

https://threatpost.com/cyberattackers-exploiting-critical-wordpress-plugin-bug/164663/

严重的安全漏洞会导致智能电表离线

日期: 2021-03-12

等级: 高

来源: Tara Seals

标签: ['Schneider Electric', 'DDos']

施耐德电气智能电表中存在严重的安全漏洞，攻击者可利用该漏洞获得远程代码执行（RCE）路径，或重新启动电表，从而在设备上造成拒绝服务（DoS）情况。施耐德电气的 PowerLogic ION/PM 智能电表产品线与其他智能电表一样，既可供消费者在家中使用，也可供部署这些电表的公用事业公司使用，以便对客户的服务进行监控和计费。它们也被工业公司、数据中心和医疗保健公司使用。

详情

Critical Security Bug Can Knock Smart Meters Offline

https://threatpost.com/critical-security-smart-meter-offline/164753/

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. 及时备份数据并确保数据安全

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 2. 事件涉及的漏洞等级为严重/高危 3. 事件涉及机密/重要/核心数据， 4. 事件涉及数据量巨大 5. 事件涉及大型/常用厂商与组件 6. 事件涉及金额数目庞大/相关受害者损失高 7. 已知/潜在受害者数量庞大 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 2. 事件涉及的漏洞等级为中危 3. 事件涉及数据机密性/重要性一般， 4. 事件涉及数据量中等 5. 事件涉及小型/常用厂商与组件 6. 事件涉及金额数目中等/相关受害者损失一般 7. 已知/潜在受害者数量中等 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 2. 事件涉及的漏洞等级为低危 3. 事件涉及数据机密性/重要性低， 4. 事件涉及数据量低 5. 事件涉及小型/非常用厂商与组件 6. 事件涉及金额数目少/相关受害者损失低 7. 已知/潜在受害者数量少 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