安全事件周报

安全事件周报 (2.22-2.28)

360CERT
北京奇虎科技有限公司 | 2021-03-01

报告信息

报告名称	安全事件周报（2.22-2.28）		
报告类型	安全事件周报	报告编号	B6-2021-030101
报告版本	1.0	报告日期	2021-03-01
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	2021-03-01	360CERT	360CERT	撰写报告

目录

一、 事件概览 1
二、 事件档案 2
三、 事件详情 3
(一) 恶意程序 3
(二) 网络攻击 5
(三) 其他事件 7
四、 产品侧解决方案 9
(一) 360 网络空间测绘系统 9
(二) 360 安全分析响应平台 9
(三) 360 安全卫士 10
附录 A 事件等级说明 11
附录 B 事件类型说明 13

一、 事件概览

本周收录安全事件 12 项

话题集中在`网络攻击`、`勒索软件`方面，涉及的组织有：`Accelion`、`Cisco`、`VMware`、`Powerhouse`等。黑客利用 0day 漏洞威胁全球，老旧系统切勿开放在公网。

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**
Clop 勒索软件利用 Accelion 漏洞威胁全球	★★★★★
Silver Sparrow 恶意软件感染 3 万台 Mac 设备	★★★★
恶意的 Mozilla Firefox 扩展能够接管用户 Gmail 账户	★★★★
勒索软件团伙入侵厄瓜多尔最大私人银行及财政部	★★★★
网络攻击	**等级**
Powerhouse VPN 产品可被用以进行大规模 DDoS 攻击	★★★★
俄罗斯对乌克兰国防网站进行 DDoS 攻击	★★★★
联邦快递网络钓鱼攻击中，1 万 Microsoft 电子邮件用户遭袭	★★★★
俄罗斯黑客组织部署 IronPython 恶意软件加载程序	★★★★
四个针对关键基础设施的黑客组织	★★★★
攻击者积极利用 PoC 扫描易受攻击的 VMware 服务器	★★★★
其他事件	**等级**
npm 组件程序包 systeminformation 发现代码注入漏洞	★★★★
Cisco 修复了 MSO 严重身份验证绕过漏洞	★★★★

三、 事件详情

(一) 恶意程序

Clop 勒索软件利用 Accelion 漏洞威胁全球

日期: 2021-02-22

等级: 高

来源: Ionut Ilascu

标签: ['Accellion', 'File Transfer Appliance', 'Clop', 'Vulnerability']

Clop 勒索软件将多个 0day 漏洞与一个新的 Web Shell 结合在一起，破坏了多达 100 家公司的 Accellion FTA (文件传输设备)，并窃取了敏感文件。目前已知受害者包括：超市巨头 Kroger，Singtel，QIMR Berghofer 医学研究所，新西兰储备银行，澳大利亚证券和投资委员会（ASIC）和华盛顿州审计师办公室（" SAO"）、技术服务公司 ABS 集团、琼斯律师事务所、Danaher、科罗拉多大学等。目前 Accellion 已更新 FTA 安全补丁，相关信息可访问: https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/

详情

Global Accellion data breaches linked to Clop ransomware gang

https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

Silver Sparrow 恶意软件感染 3 万台 Mac 设备

日期: 2021-02-22

等级: 高

来源: Catalin Cimpanu

标签: ['Mac', 'Silver Sparrow']

安全研究人员发现了一种针对 Mac 设备的新恶意软件--`Silver Sparrow`，根据 Malwarebytes 提供的数据，截至 2021 年 2 月 17 日，`Silver Sparrow`已经感染了包括美国、英国、加拿大、法国、德国等 153 个国家的 29139 个 macOS 终端。但尽管感染设备众多，但有关恶意软件如何传播和感染用户的详细信息仍然很少，目前还不清楚 Silver Sparrow 是否隐藏在恶意广告、盗版应用程序或假冒 Flash 更新程序等经典传播载体中，此外，这种恶意软件的目的也不清楚。

详情

30,000 Macs infected with new Silver Sparrow malware

https://www.zdnet.com/article/30000-macs-infected-with-new-silver-sparrow-malware/

恶意的 Mozilla Firefox 扩展能够接管用户 Gmail 账户

日期: 2021-02-25

等级: 高

来源: Lindsey O'Donnell

标签: ['Gmail', 'Mozilla Firefox', 'FriarFox', 'TA413']

最近发现的一种网络攻击正在控制受害者的`Gmail`账户，它使用的是一种定制的恶意`Mozilla Firefox`浏览器扩展--名为`FriarFox`。
研究人员说，在 1 月和 2 月观察到的威胁运动针对的是西藏组织，并与`TA413`有关，`TA413`是一个已知的高级持续威胁（APT）组织。
此次攻击的幕后组织旨在通过窥探受害者的`Firefox`浏览器数据和`Gmail`邮件来收集受害者的信息。

详情

Malicious Mozilla Firefox Extension Allows Gmail Takeover
https://threatpost.com/malicious-mozilla-firefox-gmail/164263/

勒索软件团伙入侵厄瓜多尔最大私人银行及财政部

日期: 2021-02-26

等级: 高

来源: Lawrence Abrams

标签: ['Ecuador', 'Ministry of Finance', 'Banco Pichincha', 'Hotarus Corp']

一个名为"Hotarus Corp"的黑客组织入侵了厄瓜多尔财政部和该国最大的银行 B`anco Pichinch`a，他们声称在那里窃取了"敏感的部委信息、电子邮件、雇员信息、合同"。勒索软件团伙首先锁定厄瓜多尔财政部`Economia y Finanzas de Ecuador`，在那里他们部署了一个基于 PHP 的勒索软件，对一个托管在线课程的网站进行加密。攻击发生后不久，黑客在一个黑客论坛上发布了一个包含 6632 个登录名和哈希密码组合的文本文件。

详情

Ransomware gang hacks Ecuador's largest private bank, Ministry of Finance
https://www.bleepingcomputer.com/news/security/ransomware-gang-hacks-ecuadors-largest-private-bank-ministry-of-finance/

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. 软硬件提供商要提升自我防护能力，保障供应链的安全
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. 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) 网络攻击

Powerhouse VPN 产品可被用以进行大规模 DDoS 攻击

日期: 2021-02-22

等级: 高

来源: Catalin Cimpanu

标签: ['VPN', 'Powerhouse Management', 'DDOS']

僵尸网络运营商正在滥用 VPN 提供商 Powerhouse Management 提供的 VPN 服务器，以此来反弹和放大 DDoS 攻击中的垃圾流量。研究人员说，被利用服务在 Powerhouse VPN 服务器上的 UDP 端口 20811 上运行，攻击者可以使用一个字节的请求来 ping 通此端口，并且该服务通常会以最大为原始数据包大小 40 倍的数据包进行响应。由于这些数据包基于 UDP，因此也可以对其进行修改以包含错误的返回 IP 地址。这意味着攻击者可以将单字节 UDP 数据包发送到 Powerhouse VPN 服务器，然后将其放大并发送到 DDoS 攻击的受害者的 IP 地址，安全研究人员称之为反射/放大 DDoS 攻击。

详情

Powerhouse VPN products can be abused for large-scale DDoS attacks

https://www.zdnet.com/article/powerhouse-vpn-products-can-be-abused-for-large-scale-ddos-attacks/

俄罗斯对乌克兰国防网站进行 DDoS 攻击

日期: 2021-02-23

等级: 高

来源: Prajeet Nair

标签: ['Ukraine', 'Russia', 'DDos', 'Botnet']

乌克兰指责俄罗斯将乌克兰政府服务器变成僵尸网络，并利用被控服务器实施大规模分布式拒绝服务攻击。乌克兰国家安全和国防委员会称，这些攻击瞄准了乌克兰安全局、乌克兰国家安全和国防委员会的网站以及其他国家机构和战略企业的系统，这些服务器感染病毒，成为僵尸网络的一部分，用于对其他资源进行分布式拒绝服务攻击。由此，互联网供应商的安全系统将乌克兰政府服务器识别为攻击源，并自动将其列入访问黑名单。因此，即使在 DDoS 阶段结束后，用户仍然无法访问被攻击的乌克兰政府网站。

详情

Ukraine Blames Russia for DDoS Attack on Defense Websites

https://www.databreachtoday.com/ukraine-blames-russia-for-ddos-attack-on-defense-websites-a-16048

联邦快递网络钓鱼攻击中，1 万 Microsoft 电子邮件用户遭袭

日期: 2021-02-23

等级: 高

来源: Lindsey O'Donnell

标签: ['Microsoft', 'FedEx', 'DHL Express', 'Phishing']

2021 年 2 月底发现两起针对至少 10000 名微软电子邮件用户的网络钓鱼攻击，攻击者假装来自邮件快递公司，其中包括联邦快递（FedEx）和 DHL Express。这两个骗局的目标都是微软的电子邮件用户，目的是刷他们的工作电子邮件帐户凭据。他们还使用了合法域名（包括 Quip 和 googlefirebase 的域名）来放置钓鱼网页。

详情

10K Microsoft Email Users Hit in FedEx Phishing Attack

https://threatpost.com/microsoft-fedex-phishing-attack/164143/

俄罗斯黑客组织部署 IronPython 恶意软件加载程序

日期: 2021-02-24

等级: 高

来源: Akshaya Asokan

标签: ['Russian', 'Turla', 'IronNetInjector']

俄罗斯黑客组织 Turla 正在部署一个基于 IronPython 的恶意软件加载程序，名为“IronNetInjector”，“IronNetInjector 由一个 IronPython 脚本组成，该脚本包含一个.NET 注入器，使用.NETFramework API 和 Python 库来远程访问特洛伊木马 ComRAT。相关研究报告指出当运行 IronPython 脚本时，会加载.NET 注入器，从而将有效负载注入到自己的进程或远程进程中。

详情

Russian Hacking Group Deploys IronPython Malware Loader

https://www.databreachtoday.com/russian-hacking-group-deploys-ironpython-malware-loader-a-16044

四个针对关键基础设施的黑客组织

日期: 2021-02-25

等级: 高

来源: Danny Palmer

标签: ['APT', 'Infrastructure', 'Industrial Systems']

网络安全研究人员称，在 2020 年发现了四个针对工业系统的新黑客组织，而且针对工业和工业控制系统的网络攻击者也在不断增加。在过去的一年里，研究人员发现了四个新的黑客组织，分别是`Stibnite`, `Talonite`, `Kamacite`, 和 `Vanadinite`。该四个组织分工明确，Stibnite 专注于在阿塞拜疆发电的风力涡轮机公司，而 Talonite 几乎只专注于美国的电力供应商。Kamacite 将目标锁定在北美和欧洲能源公司的工业运营上。Vanadinite 在北美、欧洲、澳大利亚和亚洲开展针对能源、制造和运输的业务，重点是信息收集和运输。

详情

These four new hacking groups are targeting critical infrastructure, warns security company

https://www.zdnet.com/article/these-four-new-hacking-groups-are-targeting-critical-infrastructure-warns-security-company/

攻击者积极利用 PoC 扫描易受攻击的 VMware 服务器

日期: 2021-02-25

等级: 高

来源: Sergiu Gatlan

标签: ['RCE', 'VMware', 'vCenter']

在安全研究人员开发并发布了针对严重 vCenter 远程代码执行（RCE）漏洞的概念验证（PoC）攻击代码之后，攻击者正积极利用该 poc 扫描易受攻击的 VMware 服务器。就在 VMware 修补了严重漏洞的一天后，安全公司发现了这一扫描活动。根据 BinaryEdge（超过 14000 个暴露服务器）和 Shodan（超过 6700 个）提供的信息，成千上万个未修补的 vCenter 服务器仍然可以通过互联网访问。

详情

Attackers scan for vulnerable VMware servers after PoC exploit release

https://www.bleepingcomputer.com/news/security/attackers-scan-for-vulnerable-vmware-servers-after-poc-exploit-release/

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. 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. 不盲目信任云端文件及链接
6. 注重内部员工安全培训

(三) 其他事件

npm 组件程序包 systeminformation 发现代码注入漏洞

日期: 2021-02-24

等级: 高

来源: Ax Sharma

标签: ['npm', 'Code Injection']

该漏洞被追踪为 CVE-2021-21315，影响了“systeminformation”npm 组件，该组件每周下载量约为 80 万次，自发布以来，下载量已接近 3400 万次。简单地说，“systeminformation”是一个轻量级的 node.js 库，是开发人员可以在其项目中包含的库，用于检索与 CPU、硬件、电池、网络、服务和系统进程相关的系统信息。“systeminformation”用户应升级至 5.3.1 及以上版本，以解决其应用程序中的漏洞。

详情

Heavily used Node.js package has a code injection vulnerability

https://www.bleepingcomputer.com/news/security/heavily-used-nodejs-package-has-a-code-injection-vulnerability/

Cisco 修复了 MSO 严重身份验证绕过漏洞

日期: 2021-02-24

等级: 高

来源: Sergiu Gatlan

标签: ['Cisco', 'Cisco ACI', 'MSO']

Cisco 已解决在 Application Services 引擎上安装的 Cisco ACI 多站点 Orchestrator（MSO）的 API 终结点中发现的最大严重性身份验证绕过漏洞。未经身份验证的攻击者可以通过发送精心编制的请求，远程绕过受影响设备上的身份验证。成功的攻击使攻击者能够获得具有管理员级权限的身份令牌。

详情

Cisco fixes maximum severity MSO auth bypass vulnerability

https://www.bleepingcomputer.com/news/security/cisco-fixes-maximum-severity-mso-auth-bypass-vulnerability/

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. 不盲目安装官方代码仓库的第三方 Package
4. 软硬件提供商要提升自我防护能力，保障供应链的安全

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