安全事件周报

安全事件周报 (02.01-02.07)

360CERT
北京奇虎科技有限公司 | 2021-02-08

报告信息

报告名称	安全事件周报（02.01-02.07）		
报告类型	安全事件周报	报告编号	B6-2021-020801
报告版本	1.0	报告日期	2021-02-08
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	2021-02-08	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 15 项

话题集中在`恶意程序`、`网络攻击`方面，涉及的组织有： `VMWare`、`Stormshield`等。供应链攻击再起，各大用户注意防范。

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**
巴西最大电力公司遭遇勒索袭击	★★★★★
新的 Trickbot 模块使用 Masscan 进行本地网络侦察	★★★★
勒索软件滥用 VMWare ESXi 漏洞来加密虚拟硬盘	★★★★
勒索团伙在 2020 年至少赚了 3.5 亿美元	★★★★
超十个 Chrome 扩展程序劫持了数百万人的 Google 搜索结果	★★★★
新的恶意软件劫持 Kubernetes 集群来挖掘 Monero	★★★★
网络攻击	**等级**
安全公司 Stormshield 源代码被盗	★★★★★
新的网络钓鱼攻击使用摩尔斯电码隐藏恶意网址	★★★★
恶意软件 kobalos 针对高性能计算（HPC）集群	★★★★
Internet Explorer 0day 分析	★★★★
Plex 媒体服务器可被用于放大 DDoS 威胁	★★★★
其他事件	**等级**
Libgcrypt 开发人员发布紧急更新以解决严重的漏洞	★★★★
Sudo 漏洞可能影响 macOS	★★★★
SolarWinds 软件中发现 3 个新的严重安全漏洞	★★★★
Cisco 小型企业 VPN 路由器存在远程代码执行漏洞	★★★★

三、 事件详情

(一) 恶意程序

巴西最大电力公司遭遇勒索袭击

日期: 2021-02-05

等级: 高

来源: Ionut Ilascu

标签: ['Eletrobras', 'Copel', 'DarkSide', 'Ransomware']

巴西两大电力公司 Centrais Eletricas Brasileiras（Eletrobras）和 Companyhia Paranaense de Energia（Copel）遭受勒索软件攻击。勒索团队声称窃取了超过 1000GB 的数据，包括敏感的基础设施访问信息以及高层管理人员和客户的个人详细信息、网络地图、备份方案和时间表、Copel 主站点的域区域和 intranet 域。他们还声称获取了存储 Active Directory（AD）数据的数据库-NTDS.dit 文件，其中包含有关域中所有用户的用户对象、组、组成员身份和密码哈希的信息。

详情

Eletrobras, Copel energy companies hit by ransomware attacks

https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/

新的 Trickbot 模块使用 Masscan 进行本地网络侦察

日期: 2021-02-01

等级: 高

来源: Catalin Cimpanu

标签: ['Trickbot', 'Masscan', 'Port Scan']

安全人员发现了一个新的 Trickbot 恶意软件的组件，主要功能为执行本地网络侦察。该组件名为 masrv，它包含了 Masscan 开源实用程序的一个副本，masrv 将组件放到新感染的设备上，发送一系列 Masscan 命令，让组件扫描本地网络，并将扫描结果上传到 Trickbot 命令和控制服务器。如果扫描发现内部网络中有敏感或管理端口未关闭的系统（这在大多数公司中非常常见），则 Trickbot 团伙可以部署专门利用这些漏洞的其他模块，并横向移动以感染新系统。

详情

New Trickbot module uses Masscan for local network reconnaissance

https://www.zdnet.com/article/new-trickbot-module-uses-masscan-for-local-network-reconnaissance/

勒索软件滥用 VMWare ESXi 漏洞来加密虚拟硬盘

日期: 2021-02-02

等级: 高

来源: Catalin Cimpanu

标签: ['VMWare', 'ESXi', 'SLP']

勒索软件团伙正在滥用 VMWare ESXi 产品中的漏洞，接管部署在企业环境中的虚拟机并加密其虚拟硬盘驱动器。攻击者使用了 VMware ESXi 中的两个漏洞 CVE-2019-5544 和 CVE-2020-3992。如果公司依赖 VMWare ESXi 来管理其虚拟机使用的存储空间，请务必安装必要的 ESXi 修补程序，或者禁用 SLP 支持以防止攻击（如果不需要该协议）。

详情

Ransomware gangs are abusing VMWare ESXi exploits to encrypt virtual hard disks

https://www.zdnet.com/article/ransomware-gangs-are-abusing-vmware-esxi-exploits-to-encrypt-virtual-hard-disks/

勒索团伙在 2020 年至少赚了 3.5 亿美元

日期: 2021-02-02

等级: 高

来源: Catalin Cimpanu

标签: ['Chainalysis', 'Ransomware', 'Ransom Payments']

区块链分析公司 ChainAnalysis 在一份报告中称，勒索软件团伙在 2020 年至少获得了 3.5 亿美元的赎金。这一数字是通过追踪与勒索软件攻击有关的区块链地址的交易而得出的。尽管 ChainAnalysis 拥有与加密货币相关的网络犯罪方面最完整的数据集，但该公司表示，其估计值仅为实际应付总额的下限，并非所有受害者都披露了去年的勒索攻击和随后的支付情况，实际总额比该公司所能看到的要多出许多倍。

详情

Ransomware gangs made at least $350 million in 2020

https://www.zdnet.com/article/ransomware-gangs-made-at-least-350-million-in-2020/

超十个 Chrome 扩展程序劫持了数百万人的 Google 搜索结果

日期: 2021-02-03

等级: 高

来源: The Hacker News

标签: ['Avast', 'Chrome', 'Extension']

Chrome 和 Edge 浏览器恶意扩展劫持了搜索结果的页面，并将其用作钓鱼网站和广告。恶意扩展包括：Video Downloader for Facebook, Vimeo Video Downloader, Instagram Story Downloader, VK Unblock。谷歌和微软已经关闭了所有后门浏览器加载项，以防止更多用户从官方商店下载这些加载项。根据该公司收集的遥测数据，感染率最高的三个国家是巴西、乌克兰和法国，其次是阿根廷、西班牙、俄罗斯和美国。

详情

Over a Dozen Chrome Extensions Caught Hijacking Google Search Results for Millions

https://thehackernews.com/2021/02/over-dozen-chrome-extensions-caught.html

新的恶意软件劫持 Kubernetes 集群来挖掘 Monero

日期: 2021-02-03

等级: 高

来源: Lindsey O'Donnell

标签: ['Hildegard', 'Kubernetes', 'TeamTNT', 'Monero']

研究人员发现 Hildegard 的恶意软件被 TeamTNT 威胁组织用来攻击 Kubernetes 集群。攻击者首先通过对配置错误的 kubelet 进行远程代码执行攻击，来获得初始访问权限，之后，攻击者下载并运行一个 tmate，以便建立一个反向 shell。然后，攻击者使用 masscan Internet 端口扫描仪扫描 Kubernetes 的内部网络，并找到其他不安全的 Kuberets，并部署一个恶意的加密挖掘脚本(xmr.sh)。

详情

New Malware Hijacks Kubernetes Clusters to Mine Monero
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

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. 及时对系统及各个服务组件进行版本升级和补丁更新
3. 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
4. 各主机安装 EDR 产品，及时检测威胁
5. 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

安全公司 Stormshield 源代码被盗

日期: 2021-02-04
等级: 高
来源: Catalin Cimpanu
标签: ['Stormshield', 'Source Code']

法国网络安全公司 Stormshield 是法国政府安全服务和网络安全设备的主要供应商。该公司表示，一名黑客进入其一个客户支持门户网站，窃取了客户的信息。该公司还报告说，攻击者成功窃取了 Stormshield 网络安全（SNS）防火墙的部分源代码，该产品经认证用于法国政府网络。

详情

Security firm Stormshield discloses data breach, theft of source code

https://www.zdnet.com/article/security-firm-stormshield-discloses-data-breach-theft-of-source-code/

新的网络钓鱼攻击使用摩尔斯电码隐藏恶意网址

日期: 2021-02-07
等级: 高

来源: Lawrence Abrams

标签: ['Morse', 'Phishing', 'Malicious URL']

攻击者利用摩尔斯电码在他们的网络钓鱼形式中隐藏恶意网址，以绕过安全邮件网关和邮件过滤器。网络钓鱼攻击从一封伪装成公司发票的电子邮件开始，邮件主题为“Revenue_payment_invoice February_Wednesday 02/03/2021”此电子邮件包含一个 HTML 附件，其名称看起来像是公司的 Excel 发票。这些附件以“[company_name] _invoice_ [number] ._ xlsx.hTML”的格式命名。例如，如果目标是 360CERT，则附件将命名为“360CERT_invoice_1308._xlsx.hTML”在文本编辑器中查看附件时，可以看到附件中包含将字母和数字映射到摩尔斯电码的 JavaScript。该电子表格说明他们的登录超时，并提示他们再次输入密码。一旦用户输入密码，表单就会将密码提交到远程站点，攻击者可以在那里收集登录凭据。

![enter description here](https://p403.ssl.qhimgs4.com/t01ff0ea055b0dd07af.png)

详情

New phishing attack uses Morse code to hide malicious URLs

https://www.bleepingcomputer.com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/

恶意软件 kobalos 针对高性能计算（HPC）集群

日期: 2021-02-02

等级: 高

来源: Marc-Etienne M.Léveillé

标签: ['ESET', 'Kobalos', 'HPC']

ESET 研究人员分析了针对高性能计算（HPC）集群的恶意软件，该恶意软件可移植到许多操作系统（包括 Linux，BSD，Solaris，甚至可能是 AIX 和 Windows）中。该恶意程序通过使用特定 TCP 源端口，连接到 SSH 服务器，来远程确定系统是否可以攻击。因为它的代码量很小且有许多技巧，将其命名为 Kobalos。

详情

This Linux malware is hijacking supercomputers across the globe

https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/

Internet Explorer 0day 分析

日期: 2021-02-04

等级: 高

来源: ENKI

标签: ['Internet Explorer', '0day', 'lazarus']

在 2021 年一月份朝鲜针对安全人员的攻击事件中，攻击者同时使用 IE 0day 对 ENKI 进行打击。由此，ENKI 研究人员对本次所使用的 ie 0day 进行了分析，分析详情见链接。

详情

Internet Explorer 0day 분석

https://enki.co.kr/blog/2021/02/04/ie_0day.html

Plex 媒体服务器可被用于放大 DDoS 威胁

日期: 2021-02-06

等级: 高

来源: Akshaya Asokan

标签: ['Plex', 'DDOS']

Plex Media 应用程序与 Windows、Linux 和 macOS 操作系统配合使用，通常允许用户与其他设备共享视频和其他媒体。NetScout 的研究人员认为，攻击者正在滥用 Plex 媒体服务器应用程序的某些版本来加强和放大各种 DDoS 攻击，大约 27000 台 Plex 媒体服务器容易受到 DDOS 攻击。

详情

Plex Media Server Used to Amplify DDoS Threats

https://www.databreachtoday.com/plex-media-server-used-to-amplify-ddos-threats-a-15941

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. 及时对系统及各个服务组件进行版本升级和补丁更新
3. 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
4. 如果允许，暂时关闭攻击影响的相关业务，积极对相关系统进行安全维护和更新，将损失降到最小

(三) 其他事件

Libgcrypt 开发人员发布紧急更新以解决严重的漏洞

日期: 2021-02-01

等级: 高

来源: Charlie Osborne

标签: ['Libgcrypt', 'vulnerability', 'GnuPG']

Libgcrypt 的开发人员发布了一个紧急更新，以解决该软件最新版本中的一个堆缓冲区溢出漏洞。Libgcrypt 是一个开源的加密库和 GNU 隐私保护（GnuPG）模块。该软件 1.9.0 版于 1 月 19 日发布。该漏洞 CVE 编号尚未分配。

详情

Libgcrypt developers release urgent update to tackle severe vulnerability

https://www.zdnet.com/article/libgcrypt-developers-release-urgent-update-to-tackle-severe-vulnerability/

Sudo 漏洞可能影响 macOS

日期: 2021-02-03

等级: 高

来源: Catalin Cimpanu

标签: ['macOS', 'Linux', 'CVE-2021-3156', 'Baron Samedit']

一位安全研究人员发现，Sudo 应用程序中最近的一个安全漏洞 CVE-2021-3156 也会影响 macOS 操作系统，只要稍作修改，这个安全漏洞也可以用来授予攻击者访问 macOS 根帐户的权限，而不是最初认为的 Linux 和 BSD。

详情

Recent root-giving Sudo bug also impacts macOS

https://www.zdnet.com/article/recent-root-giving-sudo-bug-also-impacts-macos/

SolarWinds 软件中发现 3 个新的严重安全漏洞

日期: 2021-02-03

等级: 高

来源: The Hacker News

标签: ['SolarWinds', 'Trustwave', 'Vulnerability']

网络安全研究人员披露了影响 SolarWinds 产品的三个严重安全漏洞，其中最严重的漏洞可能被用于提升权限实现远程代码执行。其中两个漏洞（CVE-2021-25274 和 CVE-2021-25275）是在 SolarWinds Orion 平台上发现的，而第三个单独的漏洞（CVE-2021-25276）是在该公司用于 Windows 的 Serv-U FTP 服务器上发现的。

详情

3 New Severe Security Vulnerabilities Found In SolarWinds Software

https://thehackernews.com/2021/02/3-new-severe-security-vulnerabilities.html?m=1

Cisco 小型企业 VPN 路由器存在远程代码执行漏洞

日期: 2021-02-05

等级: 高

来源: Liam Tung

标签: ['Cisco', 'Cisco Small Business Router', 'Remote Code Execution']

Cisco 小型企业 VPN 路由器存在远程代码执行漏洞，影响 Cisco Small Business RV160、RV160W、RV260、RV260P 和 RV260W VPN 路由器。路由器的 web 管理界面中存在多个漏洞，远程攻击者可以使用这些漏洞以根用户身份执行代码。Cisco 在固件版本 1.5.1.13 中修复了影响 RV320 和 RV325 双千兆 WAN VPN 路由器的错误。

详情

Cisco warns of critical remote code execution flaws in these small business VPN routers

https://www.zdnet.com/article/cisco-warns-of-critical-remote-code-execution-flaws-in-these-small-business-vpn-routers/

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 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