安全事件周报

安全事件周报 (01.25-01.31)

360CERT
北京奇虎科技有限公司 | 2021-02-01

报告信息

报告名称	安全事件周报（01.25-01.31）		
报告类型	安全事件周报	报告编号	B6-2021-020101
报告版本	1.0	报告日期	2021-02-01
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	2021-02-01	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 12 项

话题集中在`恶意程序`、`数据泄露`方面，涉及的组织有：`Perl `、`Linux`、`Google`。恶意软件应对策略初见成效，顶级勒索厂商陆续被关停。

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**
世界上最危险的恶意软件 Emotet 被警方破坏	★★★★★
Perl.com 网站域名被盗，现在解析的 IP 地址指向恶意软件	★★★★★
美国指控 NetWalker 勒索软件附属公司并没收赎金	★★★★
针对云应用的加密劫持恶意软件获得了新的升级、蠕虫功能	★★★★
Fonix Crypter 勒索软件发布主解密密钥	★★★★
数据安全	**等级**
VIPGames 泄密案曝光 2300 万玩家记录	★★★★
网上有出售 1.76 亿巴基斯坦手机用户的数据库	★★★★
荷兰 COVID-19 患者数据在地下出售	★★★★
BuyUcoin 加密货币交易所的数据在网上泄露	★★★★
网络攻击	**等级**
朝鲜黑客通过社交媒体锁定安全研究人员	★★★★★
Volatile Cedar 黑客组织瞄准全球的电信、主机和 ISP	★★★★
其他事件	**等级**
Linux SUDO 漏洞允许本地用户获得 root 权限	★★★★

三、 事件详情

(一) 恶意程序

世界上最危险的恶意软件 Emotet 被警方破坏

日期: 2021-01-27

等级: 高

来源: Danny Palmer

标签: ['Europol', 'FBI', 'National Crime Agency', 'Emotet', 'Disrupted']

在进行了为期两年的全球执法行动之后，世界上最多产，最危险的恶意软件僵尸网络已被关闭。
欧洲刑警组织，联邦调查局，英国国家犯罪局等采取了协调一致的行动，调查人员控制了`Emotet`的基础设施。
Emotet 最初于 2014 年成为银行木马，但后来演变为网络犯罪分子使用的最强大的恶意软件之一。

详情

Emotet: The world's most dangerous malware botnet was just disrupted by a major police operation

https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/

Perl.com 网站域名被盗，现在解析的 IP 地址指向恶意软件

日期: 2021-01-29

等级: 高

来源: Lawrence Abrams

标签: ['Perl', 'Domain Stolen']

域名 perl.com 网站被盗，指向与恶意软件活动相关的 IP 地址。Perl.com 网站是 Perl 基金会拥有的一个网站，自 1997 年以来一直用于发布有关 Perl 编程语言的新闻和文章。1 月 27 日，Perl NOC 网站发布 perl.com 网站域被劫持的消息，正将用户指向另一个 IP 地址。这个 perl.com 网站该网站最初托管在 IP 地址 151.101.2.132，但由于被劫持，解析目标变成了谷歌云 IP 地址 35.186.238[.]101。

详情

Perl.com domain stolen, now using IP address tied to malware

https://www.bleepingcomputer.com/news/security/perlcom-domain-stolen-now-using-ip-address-tied-to-malware/

美国指控 NetWalker 勒索软件附属公司并没收赎金

日期: 2021-01-27

等级: 高

来源: Ionut Ilascu

标签: ['Netwalker', 'Canadian', 'U.S. Justice Department', 'Ransom', 'Dark Web']

美国司法部 2021 年 1 月 27 日宣布中断了`Netwalker`勒索软件的运作，并起诉了一名涉嫌参与文件加密勒索攻击的加拿大公民。
美国和保加利亚的执法部门在暗网上查获了`Netwalker`网站，这些网站上泄露了那些拒绝支付赎金的受害者的数据。
除了没收暗网网站以外，美国司法部表示，加蒂诺的加拿大公民塞巴斯蒂安·瓦肖恩·德斯贾尔丁斯丁(Sebastien Vachon-Desjardins)被指控与`Netwalker`勒索软件攻击有关。

详情

US charges NetWalker ransomware affiliate, seizes ransom payments
https://www.bleepingcomputer.com/news/security/us-charges-netwalker-ransomware-affiliate-seizes-ransom-payments/

针对云应用的加密劫持恶意软件获得了新的升级、蠕虫功能

日期: 2021-01-28

等级: 高

来源: Derek B. Johnson

标签: ['Monero', 'Rocke Group', 'Cloud', 'Pro-Ocean']

Pro-Ocean 在 2018 年和 2019 年一直被用于从受感染的 Linux 机器上非法开采 Monero 币。Pro-Ocean 由四个模块组成，每个模块的设计都是为了进一步实现不同的目标：隐藏恶意软件、挖掘 Monero、感染更多的应用程序以及搜索和禁用消耗 CPU 的其他进程，以便恶意软件能够更有效地挖掘。它利用 apache activemq、oracle weblogic、Redis 和其他云应用程序中已知的、存在多年的漏洞，在云环境中部署一个隐藏的 XMRig miner。该软件还可以更新和定制，以攻击其他云应用程序。近几年被研究人员曝光后，该软件进行了更新，最新版本的恶意软件还使用了一些新的模糊层进行隐藏。

详情

Cryptojacking malware targeting cloud apps gets new upgrades, worming capability
https://www.scmagazine.com/home/security-news/malware/cryptojacking-malware-targeting-cloud-apps-gets-new-upgrades-worming-capability/

Fonix Crypter 勒索软件发布主解密密钥

日期: 2021-01-30

等级: 高

来源: Catalin Cimpanu

标签: ['FonixCrypter', 'Twitter']

FonixCrypter 勒索软件背后的网络犯罪组织在 Twitter 上宣布，他们已经删除了勒索软件的源代码，并计划停止他们的勒索运营。FonixCrypter 团伙还发布了一个包含解密工具、操作说明和勒索软件主解密密钥的软件包。以前受感染的用户可以使用这些文件免费解密和恢复他们的文件，而无需支付解密密钥的费用。

详情

FonixCrypter ransomware gang releases master decryption key

https://www.zdnet.com/article/fonixcrypter-ransomware-gang-releases-master-decryption-key/

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. 各主机安装 EDR 产品，及时检测威胁
3. 不盲目信任云端文件及链接
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

(二) 数据安全

VIPGames 泄密案曝光 2300 万玩家记录

日期: 2021-01-26

等级: 高

来源: Becky Bracken

标签: ['VIPGames', 'Leak', 'Cloud Misconfiguration', 'Personal Data']

VIPGames.com 是一个免费平台，共有 56 款经典棋牌游戏，暴露了成千上万用户的个人数据。
`WizCase`的一份最新报告显示，由于云计算配置不当，总共有超过 66000 名用户的 2300 万条数据被曝光。
该网站未受保护的服务器泄露的数据超过 30GB 的数据，包括用户名、电子邮件、IP 地址、散列密码、Facebook、Twitter 和谷歌 ID、赌注，甚至是被禁止进入该平台的玩家的数据。

详情

23M Gamer Records Exposed in VIPGames Leak
https://threatpost.com/gamer-records-exposed-vipgames-leak/163352/

网上有出售 1.76 亿巴基斯坦手机用户的数据库

日期: 2021-01-27

等级: 高

来源: Waqas

标签: ['Pakistani', ' Mobile Phone Users', 'Database', 'Sold Online']

一名网络犯罪分子正在出售一个据称包含超过 1.76 亿巴基斯坦公民个人信息的数据库。
显然，该数据库是一个属于该国不同电信公司的数据汇总，一同出售。
目前，巴基斯坦的一些主要电信公司包括 Zong，Warid，Ufone，Telenor 和 Jazz（以前称为 Mobilink＆Warid）。

该数据库不是从任何特定的电信公司窃取的。这可能是非法数据回收技术的结果，也可能是政府官员/电信部门内部人士出售的。

详情

Database of 176 million Pakistani mobile phone users sold online
https://www.hackread.com/pakistani-mobile-phone-users-database-sold-online/

荷兰 COVID-19 患者数据在地下出售

日期: 2021-01-25

等级: 高

来源: Catalin Cimpanu

标签: ['Dutch', 'Data Sold', 'Criminal Underground', 'Dutch Health Ministry']

荷兰警方 2021 年 1 月 22 日逮捕了两名犯罪人员，原因是他们涉嫌向地下犯罪团伙出售荷兰卫生部的 COVID-19 系统的数据。
据称，这些数据已经在网上销售了数月，价格从每人 30 欧元到 50 欧元不等。
买家会收到详细的数据信息，例如家庭住址，电子邮件，电话号码，出生日期和 BSN 标识符（荷兰社会保险号）。

详情

Dutch COVID-19 patient data sold on the criminal underground
https://www.zdnet.com/article/dutch-covid-19-patient-data-sold-on-the-criminal-underground/

BuyUcoin 加密货币交易所的数据在网上泄露

日期: 2021-01-25

等级: 高

来源: Charlie Osborne

标签: ['BuyUcoin', 'ShinyHunters', 'Cryptocurrency', 'Leaked']

据报道，BuyUcoin 加密货币交易所的数据泄露导致用户信息在地下被泄露。
据称，用户的姓名、电子邮件地址、电话号码、加密货币交易记录和银行详细信息可能已被泄露，多达 32 万名用户受到影响，
据称该数据是`ShinyHunters`泄露的，`ShinyHunters`以出售失窃的公司数据库为名。

详情

Data of BuyUcoin cryptocurrency exchange traders allegedly leaked online
https://www.zdnet.com/article/cyberattack-allegedly-leaks-data-of-indian-cryptocurrency-exchange-buyucoin-users/

相关安全建议

1. 及时备份数据并确保数据安全
2. 条件允许的情况下，设置主机访问白名单
3. 合理设置服务器端各种文件的访问权限

(三) 网络攻击

朝鲜黑客通过社交媒体锁定安全研究人员

日期: 2021-01-26

等级: 高

来源: Catalin Cimpanu

标签: ['Google', 'North Korean', 'Social Media', 'Security Researchers', 'Visual Studio']

Google 在 2021 年 1 月 26 日表示，一个朝鲜政府黑客组织已将从事漏洞研究的网络安全社区作为攻击目标。
在 2021 年 1 月 26 日发布的一份报告中，Google 表示，朝鲜黑客利用 Twitter、LinkedIn、Telegram、Discord 和 Keybase 等社交网络上的多个个人资料，利用虚假的角色接触安全研究人员。
在建立初步沟通后，参与者询问目标研究人员是否想一起进行漏洞研究，然后向研究人员提供`Visual Studio`项目。
`Visual Studio`项目包含将恶意软件安装在目标研究人员的操作系统上的恶意代码。
该恶意软件充当后门，与远程命令和控制服务器联系并等待命令。

详情

Google: North Korean hackers have targeted security researchers via social media
https://www.zdnet.com/article/google-north-korean-hackers-have-targeted-security-researchers-via-social-media/

Volatile Cedar 黑客组织瞄准全球的电信、主机和 ISP

日期: 2021-01-29

等级: 高

来源: The Hacker News

标签: ['Hezbollah', 'Telecoms', 'ISP', 'APT']

一个 APT 组织用新版远程访问木马（RAT）对其恶意软件库进行了重组，以打入全球公司并提取有价值的信息。以色列网络安全公司 ClearSky 研究小组发表的一份新报告说，自 2020 年初以来，该公司发现至少 250 个面向公众的网络服务器遭到黑客攻击。这些黑客袭击了位于美国、英国、埃及、约旦、黎巴嫩、沙特阿拉伯、以色列和巴勒斯坦权力机构的众多公司，其中大多数代表电信运营商的受害者（Etisalat, Mobily, Vodafone）、互联网服务提供商（SAUNID、TE 数据），以及托管和基础设施服务提供商（Secured Servers LLC，iomart）。

详情

Hezbollah Hacker Group Targeted Telecoms, Hosting, ISPs Worldwide
https://thehackernews.com/2021/01/hezbollah-hacker-group-targeted.html

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. 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

(四) 其他事件

Linux SUDO 漏洞允许本地用户获得 root 权限

日期: 2021-01-26

等级: 高

来源: Sergiu Gatlan

标签: ['Sudo', 'CVE-2021-3156', 'Buffer Overflow']

Sudo 是一个 Unix 程序，它使系统管理员能够向 sudoers 文件中列出的普通用户提供有限的 root 权限，同时保留他们的活动日志。
在 sudo 解析命令行参数的方式中发现了基于堆的缓冲区溢出。
任何本地用户（普通用户和系统用户，sudoer 和非 sudoers）都可以利用此漏洞，而无需进行身份验证，攻击者不需要知道用户的密码。
成功利用此漏洞可以获得 root 权限。

详情

New Linux SUDO flaw lets local users gain root privileges

https://www.bleepingcomputer.com/news/security/new-linux-sudo-flaw-lets-local-users-gain-root-privileges/

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