安全事件周报

安全事件周报 (03.01-03.07)

360CERT
北京奇虎科技有限公司 | 2021-03-08

报告信息

报告名称	安全事件周报（03.01-03.07）		
报告类型	安全事件周报	报告编号	B6-2021-030801
报告版本	1.0	报告日期	2021-03-08
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	2021-03-08	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`恶意软件`、`数据安全`方面，涉及的组织有：`马来西亚航空公司`、`Microsoft`、`Polecat`等。供应链攻击袭击航空业，多家航空公司客户数据泄露。

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**
Ursnif 特洛伊木马攻击 100 多家意大利银行	★★★★
黑客利用搜索引擎优化来传递恶意软件	★★★★
微软发现三个 SolarWinds 攻击者使用的新恶意软件	★★★★
俄罗斯黑客部署新的勒索软件变种	★★★★
D-Link、物联网设备受到基于 Tor 的 Gafgyt 变体的攻击	★★★★
数据安全	**等级**
马航披露长达 9 年的数据泄露事件	★★★★★
数据分析公司 Polecat 暴露了 30TB 的数据	★★★★
SITA 数据泄露影响了数百万来自主要航空公司的旅客	★★★★
网络攻击	**等级**
加密僵尸网络使用比特币钱包来绕过安全检测	★★★★
其他事件	**等级**
Microsoft 的紧急安全更新修复了 Exchange 漏洞	★★★★★

三、 事件详情

(一) 恶意程序

Ursnif 特洛伊木马攻击 100 多家意大利银行

日期: 2021-03-03

等级: 高

来源: Charlie Osborne

标签: ['Trojan', 'Ursnif', 'Bank', 'Italy']

Ursnif 特洛伊木马最早于 2007 年被发现，其被追踪到针对意大利至少 100 家银行的攻击。据 Avast 称，这些恶意软件的运营商对意大利的目标非常感兴趣，针对这些银行机构的攻击导致了凭证和财务数据的丢失。根据研究人员收集的信息，至少有 100 家银行成为攻击目标。仅在一个案例中，一个不知名的支付处理器就有 1700 多套凭证被盗，包括用户名、密码、信用卡、银行和支付信息。

详情

Ursnif Trojan has targeted over 100 Italian banks

https://www.zdnet.com/article/ursnif-trojan-has-targeted-over-100-italian-banks/

黑客利用搜索引擎优化来传递恶意软件

日期: 2021-03-02

等级: 高

来源: Akshaya Asokan

标签: ['Trojans', 'Sophos', 'Gootloader', 'Search Engine Optimization']

安全公司 Sophos 报道称，一种新的恶意软件加载程序名为"Gootloader"，它利用搜索引擎优化技术传播勒索软件、特洛伊木马和其他恶意软件。
Sophos 的研究人员表示，该活动在北美、韩国、德国和法国都很活跃。
为了诱骗受害者访问受感染的网站，"Gootloader 使用恶意的搜索引擎优化技术来扰乱谷歌搜索结果，"Sophos 指出。"这些技术可以有效地避开网络上的检测，直到恶意活动越过行为检测规则。

详情

Hackers Use Search Engine Optimization to Deliver Malware

https://www.databreachtoday.com/hackers-use-search-engine-optimization-to-deliver-malware-a-16092

微软发现三个 SolarWinds 攻击者使用的新恶意软件

日期: 2021-03-05

等级: 高

来源: Liam Tung

标签: ['Microsoft', 'SolarWinds', 'Backdoor']

微软目前已经披露了 SolarWinds 黑客使用的三个新的恶意软件组件：GoldMax、GoldFinder 和 Sibot。GoldMax 被微软视为一个充当指挥与控制（C2）的后门，是用系统编程语言 Go 编写的。GoldFinder 也是用 Go 编写的，被认为是一个定制的 HTTP 跟踪工具，它记录数据包到达 C2 服务器的路由或跳数。Sibot 是一种多用途的恶意软件，由微软的 visualbasic 脚本（VBScript）构建。

详情

Microsoft: We've found three more pieces of malware used by the SolarWinds attackers

https://www.zdnet.com/article/microsoft-weve-found-three-more-pieces-of-malware-used-by-the-solarwinds-attackers/

俄罗斯黑客部署新的勒索软件变种

日期: 2021-03-05

等级: 高

来源: Akshaya Asokan

标签: ['RTM', 'Quoter', 'Kaspersky']

据安全公司卡巴斯基称，俄罗斯黑客组织 RTM 正在部署一个名为"Quoter"的新型勒索软件变种以及一个银行特洛伊木马，作为勒索活动的一部分。据报道，该组织最新的活动始于 2020 年 12 月，迄今已针对俄罗斯的 10 个组织发起攻击。攻击者首先发送恶意电子邮件，在邮件内部填充与业务操作相关的消息，并附上附件。如果受害者打开附件，则会下载特洛伊木马。

详情

Russian Hackers Deploy New Ransomware Variant

https://www.databreachtoday.com/russian-hackers-deploy-new-ransomware-variant-a-16124

D-Link、物联网设备受到基于 Tor 的 Gafgyt 变体的攻击

日期: 2021-03-05

等级: 高

来源: Lindsey O'Donnell

标签: ['Gafgyt', 'Tor', 'IoT']

研究人员发现了他们所说的 Gafgyt 僵尸网络家族的第一个变种，与其他 Gafgyt 变体相比，Gafgyt 的最大变化是 C2 通信基于 tor，这增加了检测和阻断的难度。僵尸网络主要通过弱 Telnet 密码（物联网设备上的常见问题）和三个漏洞进行传播。这些漏洞包括 D-Link 设备中的远程代码执行漏洞（CVE-2019-16920）；Liferay enterprise portal 软件中的远程代码执行漏洞（没有可用的 CVE）；Citrix Application Delivery Controller 中的漏洞（CVE-2019-19781）。

详情

D-Link, IoT Devices Under Attack By Tor-Based Gafgyt Variant

https://threatpost.com/d-link-iot-tor-gafgyt-variant/164529/

相关安全建议

1. 条件允许的情况下，设置主机访问白名单
2. 注重内部员工安全培训
3. 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
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. 各主机安装 EDR 产品，及时检测威胁

(二) 数据安全

马航披露长达 9 年的数据泄露事件

日期: 2021-03-02

等级: 高

来源: Lawrence Abrams

标签: ['Malaysia Airlines', 'Data Breach', 'Personal Information']

马来西亚航空公司（Malaysia Airlines）遭遇了长达 9 年的数据泄露事件，该事件暴露了其 Enrich 常客计划中成员的个人信息。
据马来西亚航空公司称，该漏洞发生在一家第三方 IT 服务提供商处，该提供商通知马航，会员数据在 2010 年 3 月至 2019 年 6 月期间被曝光。
数据泄露期间曝光的会员信息包括会员姓名、联系方式、出生日期、性别、常客号码。

详情

Malaysia Airlines discloses a nine-year-long data breach

https://www.bleepingcomputer.com/news/security/malaysia-airlines-discloses-a-nine-year-long-data-breach/

数据分析公司 Polecat 暴露了 30TB 的数据

日期: 2021-03-05

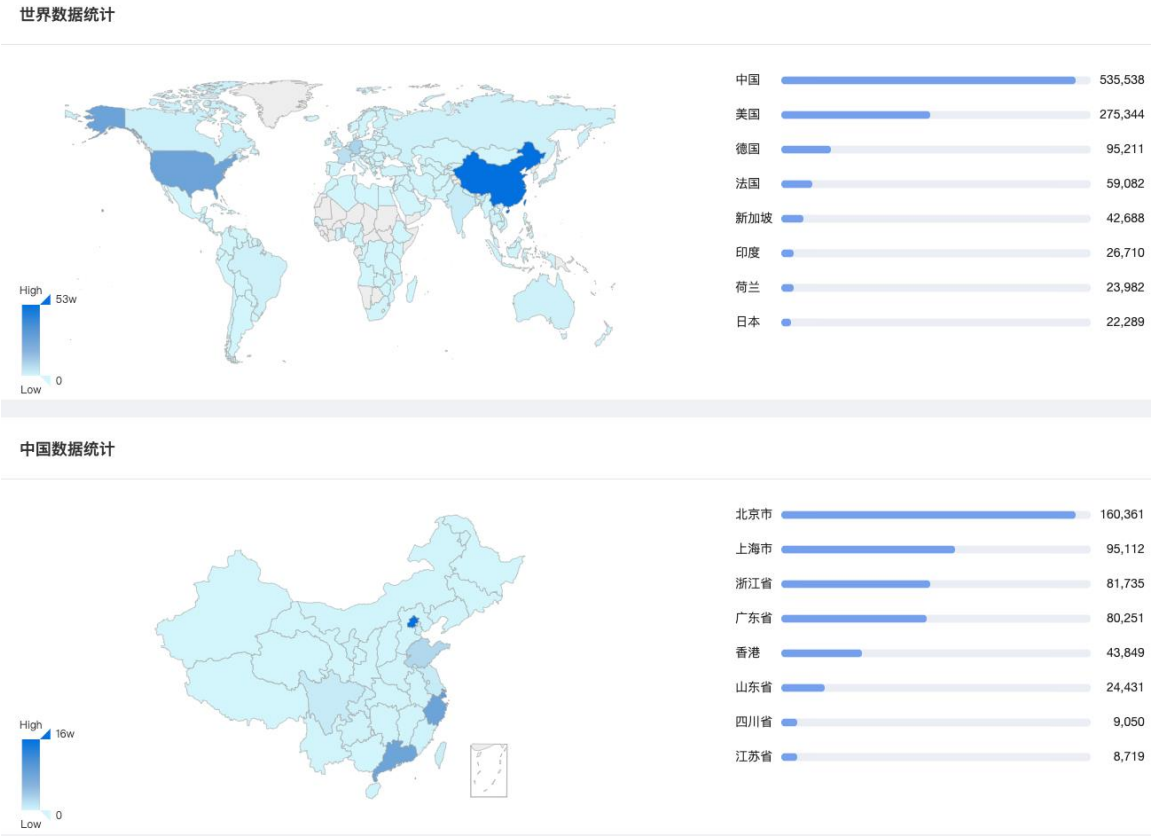
等级: 高

来源: Prajeet Nair

标签: ['Polecat', 'ElasticSearch']

英国数据分析公司 Polecat 的一台未加密服务器暴露了大约 30 TB 的数据，其中包括 120 亿条与社交媒体相关的记录。包括超过 65 亿条 tweets，近 50 亿条标记为"社交"的记录（似乎都是 tweets），以及超过 10 亿条不同博客和网站的帖子。曝光的数据包括推文内容、推文 ID、作者用户名、浏览/跟帖人数、帖子内容、URL、收获时间、发布者、地区和帖子标题。在服务器暴露的第二天，研究人员发现 Meow 攻击已经开始扫描该数据库，并删除了接近一半的数据，攻击者留下了一张赎金纸条，要求 0.04 比特币（当时大约 550 美元）才能取回数据。

目前 ElasticSearch 的具体分布如下图，数据来自于 360 QUAKE



详情

Data Analytics Firm Polecat Exposed 30TB of Data

https://www.databreachtoday.com/data-analytics-firm-polecat-exposed-30tb-data-a-16114

SITA 数据泄露影响了数百万来自主要航空公司的旅客

日期: 2021-03-05

等级: 高

来源: Ionut Ilascu

标签: ['SITA', 'Airline', 'Passenger Service System']

黑客入侵全球信息技术公司 SITA 的服务器后，全球多家航空公司的乘客数据遭到泄露。近十几家航空公司已经通知乘客，由于黑客侵入了 SITA 的乘客服务系统（PSS），乘客的一些数据已经被侵入者窃取。乘客服务系统负责处理从机票预订到登机的交易数据和业务。受影响的旅客总数仍不清楚，但至少超过 210 万。

详情

SITA data breach affects millions of travelers from major airlines

https://www.bleepingcomputer.com/news/security/sita-data-breach-affects-millions-of-travelers-from-major-airlines/

相关安全建议

1. 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
2. 对于托管的云服务器(VPS)或者云数据库，务必做好防火墙策略以及身份认证等相关设置
3. 数据库数据，尤其是密码等敏感信息需进行加密存储
4. 及时备份数据并确保数据安全
5. 及时检查并删除外泄敏感数据

(三) 网络攻击

加密僵尸网络使用比特币钱包来绕过安全检测

日期: 2021-03-01

等级: 高

来源: Prajeet Nair

标签: ['Akamai', 'Cryptomining Botnet', 'Blockchain', 'Remote Code Execution']

根据安全公司`Akamai`的说法，一个加密采矿僵尸网络活动正在使用比特币区块链交易来隐藏命令和控制服务器地址。
最初的感染始于利用 Hadoop Yarn，Elasticsearch（CVE-2015-1427）和 ThinkPHP（CVE-2019-9082）中的远程代码执行漏洞。传递的有效负载使易受攻击的计算机下载并执行恶意的 Shell 脚本。
目前，攻击者在过去三年中从不知情的主机中挖出了 30,000 美元的门罗币。

详情

Cryptomining Botnet Uses Bitcoin Wallet to Avoid Detection
https://www.databreachtoday.com/cryptomining-botnet-uses-bitcoin-wallet-to-avoid-detection-a-16085

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) 其他事件

Microsoft 的紧急安全更新修复了 Exchange 漏洞

日期: 2021-03-02

等级: 高

来源: Lawrence Abrams

标签: ['Microsoft', 'Microsoft Exchange', 'Security Update', 'SSRF']

`Microsoft`发布了针对 Microsoft Exchange 的紧急带外安全更新，修复了四个在被积极利用的 0day 漏洞。
这四个 0day 漏洞被组合在一起利用，以获得对 Microsoft Exchange 服务器的访问、窃取电子邮件，并植入更多恶意软件以增加对网络的访问。
CVE-2021-26855 是服务端请求伪造漏洞，利用此漏洞的攻击者能够发送任意 HTTP 请求并通过 Exchange Server 进行身份验证。
CVE-2021-26857 是序列化漏洞，该漏洞需要管理员权限，利用此漏洞的攻击者可以在 Exchange 服务器上以 SYSTEM 身份运行代码。
CVE-2021-26858/CVE-2021-27065 是任意文件写入漏洞，攻击者通过 Exchange 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径。该漏洞可以配合 CVE-2021-26855 SSRF 漏洞进行组合攻击。

详情

Microsoft fixes actively exploited Exchange zero-day bugs, patch now

https://www.bleepingcomputer.com/news/security/microsoft-fixes-actively-exploited-exchange-zero-day-bugs-patch-now/

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