安全事件周报

安全事件周报 (10.26-11.01)

360CERT
北京奇虎科技有限公司 | 2020-11-02

报告信息

报告名称	安全事件周报（10.26-11.01）		
报告类型	安全事件周报	报告编号	B6-2020-110202
报告版本	1.0	报告日期	2020-11-02
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	2020-11-02	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 32 项

话题集中在`数据泄露`、`勒索软件`方面，涉及的组织有：`Amazon`、`NVIDIA`、`Fragomen`、`QNAP`等。外网未加密数据库屡禁不止，各种漏洞扫描器肆虐互联网。

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**
Enel 集团今年遭受了第二次勒索软件攻击	★★★★★
KashmirBlack 僵尸网络攻击了 WordPress 等 CMS	★★★★
Sopra Steria 证实被 Ryuk 勒索软件攻击	★★★★
台湾政府遭到 Owlproxy 恶意软件攻击	★★★★
FBI,DHS,HHS 警告:医疗系统可能会发生重大的勒索软件攻击	★★★★
Earth Kitsune 行动：新增两个后门	★★★★
REvil 勒索软件团伙声称一年内利润超过 1 亿美元	★★★★
佛蒙特州医院最近遭遇勒索软件攻击	★★★★
Steelcase 家具巨头遭 Ryuk 勒索软件攻击	★★★
TrickBot Linux 变种在野活跃，尽管最近被攻陷	★★★
美国网络司令部曝光俄罗斯新恶意软件	★★★
数据安全	**等级**
芬兰心理治疗中心 Vastaamo 遭遇了严重的安全漏洞	★★★★
FBI：黑客通过 SonarQube 平台窃取政府源代码	★★★★
Lazada 证实了 110 万个账户在 RedMart 安全漏洞中受损	★★★★
数据泄露中间商正在出售 17 家公司的帐户数据库	★★★★
COVID-19 疫苗制造商遭遇数据泄露	★★★
律师事务所的谷歌员工个人信息数据遭泄露曝光	★★★
桑坦德银行表示无需担心 PagoFX 的黑客攻击行为	★★★
亚马逊通知客户：由于数据泄露，解雇掉了内部人员	★★★
网络攻击	**等级**
黑客在窃取 Harvest Finance2400 万美元后被确认身份	★★★★★

严重的 Oracle WebLogic 漏洞被在野利用	★★★★★
与俄罗斯有关的图拉 APT 黑客攻击了欧洲政府组织	★★★★
大学电子邮件劫持攻击推送钓鱼邮件与恶意软件	★★★★
InnerSloth 游戏玩家受到了严重的垃圾邮件攻击	★★★
Nando 的黑客大肆利用客户账户	★★★
特朗普的官方竞选网站遭到黑客的破坏	★★★
Xfinity, McAfee 品牌域名被攻击者滥用	★★★
其他事件	**等级**
100 多个灌溉系统在没有保护的情况下暴露在网上	★★★★
超 10 万台计算机仍然易受 SMBGhost 攻击	★★★★
研究人员用密码 MAGA2020 登录特朗普的推特	★★★
QNAP 警告可能会导致设备被接管的 QTS 漏洞	★★★
NVIDIA 修补了高性能服务器中的高危漏洞	★★★

三、 事件详情

(一) 恶意程序

Enel 集团今年遭受了第二次勒索软件攻击

日期: 2020-10-27

等级: 高

来源: SECURITYAFFAIRS

标签: ['Enel Group', 'Netwalker', 'Ransomware', 'Energy Company', 'Italian']

跨国能源公司埃奈尔集团(Enel Group)的系统被网络勒索软件感染，这是该集团在 2020 年遭受的第二次勒索软件攻击。网络勒索软件运营商要求支付 1400 万美元的赎金来换取解密密钥，黑客声称已经从该公司窃取了数 TB 的数据，并威胁说如果不支付赎金，就会泄露这些数据。 埃奈尔集团(Enel Group)是意大利的一家跨国能源公司，活跃于发电、配电以及天然气分销领域。 该公司在 40 个国家拥有 6100 多万客户，在《财富》全球 500 强中排名第 87 位，2019 年的收入为 900 亿美元。

详情

Enel Group suffered the second ransomware attack this year

https://securityaffairs.co/wordpress/110067/malware/enel-group-netwalker-ransomware.html

KashmirBlack 僵尸网络攻击了 WordPress 等 CMS

日期: 2020-10-26

等级: 高

来源: Catalin Cimpanu

标签: ['CMS', 'KashmirBlack', 'Botnet', 'Attack', 'Cryptocurrency']

一个高度复杂的僵尸网络通过攻击基础内容管理系统(CMS)平台，已经感染了数十万个网站。 `Imperva`的安全研究人员在 2020 年 10 月 22 日的一个两部分的系列文章中分析了僵尸网络，他们说僵尸网络的主要目的似乎是感染网站，然后使用他们的服务器进行加密货币挖掘，将一个网站的合法流量重定向到垃圾页面，并在较小的程度上显示网络损坏。 Imperva 说，僵尸网络开始的时候很小，但是经过几个月的持续增长，它已经发展成为一个复杂的庞然大物，能够每天攻击成千上万的网站。

详情

KashmirBlack botnet behind attacks on CMSs like WordPress, Joomla, Drupal, others

https://www.zdnet.com/article/kashmirblack-botnet-behind-attacks-on-cmss-like-wordpress-joomla-drupal-others/

Sopra Steria 证实被 Ryuk 勒索软件攻击

日期: 2020-10-26

等级: 高

来源: Lawrence Abrams

标签: ['French', 'Sopra Steria', 'Ryuk', 'TrickBot', 'BazarLoader', 'Ransomware']

法国企业 IT 服务公司 Sopra Steria 2020 年 10 月 26 日证实，他们遭到了一次 Ryuk 勒索软件攻击。Sopra Steria 是一家欧洲信息技术公司，在全球 25 个国家拥有 46000 名员工。该公司提供广泛的 IT 服务，包括咨询、系统集成和软件开发。10 月 21 日，Sopra Steria 称他们受到网络攻击，但没有提供更多细节。该公司此前感染了`TrickBot`和`BazarLoader`，因此遭到了`Ryuk`勒索软件攻击。 这两种恶意软件感染都是由同一个黑客组织创建的，并提供远程访问`Ryuk`勒索软件背后的攻击者。这种访问允许攻击者进一步破坏网络，并最终在公司的设备中部署勒索软件。

详情

Sopra Steria confirms being hit by Ryuk ransomware attack

https://www.bleepingcomputer.com/news/security/sopra-steria-confirms-being-hit-by-ryuk-ransomware-attack/

台湾政府遭到 Owlproxy 恶意软件攻击

日期: 2020-10-28

等级: 高

来源: CYBERNEWS

标签: ['CyCraft', 'Taiwan Government', 'Owlproxy', 'Malware', 'Skeleton Keys']

2020 年 4 月，CyCraft 在多个台湾政府机构观察到高度恶意的网络活动。由于相似的技术、战术和程序，其中一些攻击被归因于同一个攻击者，其中最重要的是利用数字万能钥匙和 Owlproxy 恶意软件。 使用这种方法，就像一个物理万能钥匙可以打开房子里的任何一扇门一样，数字万能钥匙使其用户可以不受限制地访问远程访问服务。 `Owlproxy`是在 2020 年 4 月的几起事件中发现的主要恶意软件之一。为了在`internet`和`intranet`之间架起桥梁，攻击者使用这种带有后门功能的恶意软件来通过隧道进出网络。这个后门功能使攻击者可以启动任何命令直接进入目标系统。

详情

Taiwan government hit by Owlproxy Malware

https://cybernews.com/security/taiwan-government-targeted-by-multiple-cyberattacks-owlproxy-malware/

FBI,DHS,HHS 警告:医疗系统可能会发生重大的勒索软件攻击

日期: 2020-10-28

等级: 高

来源: The Hacker News

标签: ['FBI', 'TrickBot', 'Ransomware', 'Healthcare Systems', 'Data Theft']

美国联邦调查局(FBI)、国土安全部和卫生与公众服务部(HHS)2020 年 10 月 28 日发布联合警告，称针对医院和医疗服务提供商的勒索软件和其他网络攻击即将增加。 美国网络安全和基础设施安全局（NSA）在其咨询报告中表示:"恶意网络行为者正在使用`TrickBot`恶意软件攻击(医疗保健和公共卫生)领域，通常会导致数据盗窃以及医疗保健服务中断。" 臭名昭著的僵尸网络通常通过恶意垃圾邮件电子邮件传播给毫无戒心的收件人，并且可以窃取财务和个人数据并将其他软件（例如勒索软件）丢弃到受感染的系统上。

详情

FBI, DHS Warn Of Possible Major Ransomware Attacks On Healthcare Systems

https://thehackernews.com/2020/10/ransomware-attack-hospital.html

Earth Kitsune 行动：新增两个后门

日期: 2020-10-28

等级: 高

来源: TRENDMICRO

标签: ['SLUB', 'agfSpy', 'dneSpy', 'Malware', 'C&C']

Earth Kitsune 行动是一项旨在通过损害网站来窃取信息的"水坑行动"。除了大量使用恶意软件外，`trendmicro`团队还发现了两个新的间谍后门与这次行动有关:`agfSpy`和`dneSpy`，这是根据攻击者的三字母命名方案命名的。`trendmicro`团队之前对操作的研究发现，虽然 SLUB 主要用于窃取数据，但 agfSpy 和 dneSpy 用于同样的目的，而且还用于获取受影响系统的控制。这篇文章提供了更多关于这些恶意软件类型的细节，包括它们和它们的命令和控制(C&C)服务器之间的关系。

详情

Operation Earth Kitsune A Dance of Two New Backdoors

https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html

REvil 勒索软件团伙声称一年内利润超过 1 亿美元

日期: 2020-10-29

等级: 高

来源: ,Ionut Ilascu

标签: ['REvil', 'Ransomware']

REvil 勒索软件开发商说，他们通过从世界各地的各行业勒索大型企业，在一年内赚了超过 1 亿美元。他们受利润驱动，希望从勒索软件服务中赚取 20 亿美元，在追求财富时采用最有利可图的趋势。 一位在网络犯罪论坛上使用化名"UNKN"和"Unknown"的 REvil 代表接受了科技博客 Russian OSINT 的采访，提供了该组织活动的一些细节，并暗示了他们未来的打算。

详情

REvil ransomware gang claims over $100 million profit in a year

https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

佛蒙特州医院最近遭遇勒索软件攻击

日期: 2020-10-30

等级: 高

来源: PricillaWhite

标签: ['FBI', 'Ryuk', 'US', 'Attack', 'Vermont Hospitals', 'Ransomware']

佛蒙特大学健康网络现在正持续不断地遭受网络攻击。这次网络攻击的目标是佛蒙特州和纽约州的六所医院，这两所医院的目标主要是造成计算机网络问题。医院提到他们的"MyChart"和其他预约都因此受到影响。 FBI 拒绝评论这是否是勒索软件攻击。 但是，独

立安全专家怀疑这可能是 Ryuk 勒索软件的攻击结果，该勒索软件已经影响了至少五家美国医院，并可能进一步袭击数百家医院。

详情

Vermont Hospitals Now Latest Victim of Ransomware Attacks
https://gbhackers.com/vermont-health-network/

Steelcase 家具巨头遭 Ryuk 勒索软件攻击

日期: 2020-10-27

等级: 中

来源: Lawrence Abrams

标签: ['Steelcase', 'Ransomware', 'Ryuk', 'Cyberattack']

办公家具巨头 Steelcase 遭遇勒索软件攻击，迫使他们关闭网络以遏制攻击的蔓延。 Steelcase 是全球最大的办公家具制造商，在 2020 年拥有 13,000 名员工和 37 亿美元的资产。 在提交给美国证券交易委员会(SEC)的一份 8-K 表格中，Steelcase 公司透露，他们在 2020 年 10 月 22 日遭受了一次网络攻击。 目前，Steelcase 公司尚不清楚此次攻击导致其系统的任何数据丢失或任何其他资产损失。

详情

Steelcase furniture giant hit by Ryuk ransomware attack
https://www.bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomware-attack/

TrickBot Linux 变种在野活跃，尽管最近被攻陷

日期: 2020-10-28

等级: 中

来源: The Hacker News

标签: ['TrickBot', 'Netscout', 'Linux', 'Trojan', 'Ransomware']

`TrickBot`已经关闭了其大部分的主要基础设施，但`TrickBot`恶意软件背后的运营商并未处于闲置状态。 根据网络安全公司`Netscout`分享的新发现，`TrickBot`的作者已将其部分代码移至`Linux`，以扩大可能成为目标的受害者的范围。 TrickBot 是 2016 年首次检测到的金融木马，传统上是基于 Windows 的犯罪软件解决方案，它采用不同的模块在目标网络上执行各种恶意活动，包括凭证盗窃和永久勒索软件攻击。 但是在过去的几周里，由美国网络司令部和微软共同努力，已经消除了 94%的`TrickBot`使用中的命令和控制（C2）服务器以及犯罪分子试图将 TrickBot 引入网络的新基础架构 替换以前禁用的服务器。

详情

TrickBot Linux Variants Active in the Wild Despite Recent Takedown
https://thehackernews.com/2020/10/trickbot-linux-variants-active-in-wild.html

美国网络司令部曝光俄罗斯新恶意软件

日期: 2020-11-01

等级: 中

来源: Catalin Cimpanu

标签: ['US Cyber Command', 'Russian', 'ComRAT', 'Zebrocy', 'Turla']

美国网络司令部曝光了俄罗斯黑客在最近的攻击中开发和部署的 8 个新的恶意软件样本。这 8 个样本中有 6 个是 ComRAT 恶意软件（Turla hacking group 使用的），另外两个是 Zebrocy 恶意软件的样本（由 APT28 黑客组织使用）。 ComRAT 和 Zebrocy 都是恶意软件家族，已经被俄罗斯黑客组织使用了多年，而 ComRAT 从旧的 Agent.BTZ 恶意软件演变而来，在攻击中已经部署了十多年。 Turla 和 APT28 一直在更新这两种工具，以增加逃税技术，并保持他们的恶意软件不被发现。

详情

US Cyber Command exposes new Russian malware
https://www.zdnet.com/article/us-cyber-command-exposes-new-russian-malware/

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. 各主机安装 EDR 产品，及时检测威胁
3. 网段之间进行隔离，避免造成大规模感染
4. 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
5. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
6. 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
7. 及时对系统及各个服务组件进行版本升级和补丁更新

(二) 数据安全

芬兰心理治疗中心 Vastaamo 遭遇了严重的安全漏洞

日期: 2020-10-26
等级: 高
来源: SECURITYAFFAIRS
标签: ['Finnish', 'Vastaamo', 'Psychotherapy', 'Ransom']

芬兰内政部长 2020 年 10 月 25 日召开紧急会议，此前芬兰私人心理治疗中心`Vastaamo`遭遇安全漏洞，导致患者记录曝光。更糟糕的是，黑客现在要求赎金，威胁泄露被盗数据。 `Vastaamo`是芬兰公共卫生系统的一个分包商。黑客从近两年前开始的两次攻击中窃取了患者的敏感数据。目前尚不清楚被盗信息是否包括诊断、治疗记录或其他潜在的损害性信息。 国家调查局正在调查这起事件，并透露数据泄露可能影响了多达"数万"的 Vastaamo 客户。

详情

Finnish psychotherapy center Vastaamo suffered a shocking security breach
https://securityaffairs.co/wordpress/110002/cyber-crime/vastaamo-data-breach.html

FBI：黑客通过 SonarQube 平台窃取政府源代码

日期: 2020-10-27

等级: 高

来源: Sergiu Gatlan

标签: ['FBI', 'SonarQube', 'U.S Government', 'Vulnerability']

美国联邦调查局(FBI)发布了一个紧急警报，警告黑客通过网络暴露和不安全的`SonarQube`平台窃取美国政府机构和企业组织的数据。 SonarQube 是一个开源平台，用于自动化代码质量审计和静态分析，用于发现使用 27 种编程语言的项目中的 bug 和安全漏洞。 自 2020 年 4 月以来，攻击者一直在利用有漏洞的`SonarQube`服务器来访问政府和公司实体拥有的数据源代码存储库，随后对其进行公开泄漏。 FBI 表示，自攻击开始以来，他们已经发现了几起攻击者滥用`SonarQube`配置漏洞的事件。

详情

FBI: Hackers stole government source code via SonarQube instances

https://www.bleepingcomputer.com/news/security/fbi-hackers-stole-government-source-code-via-sonarqube-instances/

Lazada 证实了 110 万个账户在 RedMart 安全漏洞中受损

日期: 2020-10-30

等级: 高

来源: Eileen Yu

标签: ['RedMart', 'Data Breach', 'Singapore', 'Grocery Platform', 'Lazada']

新加坡在线杂货平台 RedMart 遭遇数据泄露，110 万个账户的个人数据受到破坏。个人信用卡中所包含的个人信用卡信息，包括个人信用卡和个人信用卡密码。 RedMart 的母公司 Lazada 在给客户的说明中说，该漏洞导致托管在第三方服务提供商上的"RedMart 专用数据库"可以被未经授权访问。Lazada 强调，该漏洞只影响 RedMart 的账户，而没有影响 Lazada 客户的数据。

详情

Lazada confirms 1.1M accounts compromised in RedMart security breach

https://www.zdnet.com/article/lazada-confirms-1-1m-accounts-compromised-in-redmart-security-breach/

数据泄露中间商正在出售 17 家公司的帐户数据库

日期: 2020-11-01

等级: 高

来源: Pierluigi Paganini

标签: ['BleepingComputer', 'Selling Account', 'Data Breach', 'Hacker Forum', 'Data Broker']

一名攻击者提供了一个出售账户的数据库，其中包含从 17 家公司窃取的总计 3400 万条用户记录。自 10 月 28 日以来，攻击者就在黑客论坛上发布被盗数据。 该攻击者表示，他只是一个中间商，并没有入侵这 17 家公司。 当时还不清楚攻击者是如何从据称被黑客攻击的公司收集这些记录的，很可能这些记录是在地下流传的，并被私下卖给了各种攻击者。

详情

A data breach broker is selling account databases of 17 companies

https://securityaffairs.co/wordpress/110259/data-breach/account-databases-stolen-17-companies.html

COVID-19 疫苗制造商遭遇数据泄露

日期: 2020-10-26

等级: 中

来源: SECURITYAFFAIRS

标签: ['Indian', 'Russia', 'Sputinik V', 'COVID-19', 'Dr. Reddy's Laboratories']

印度 COVID-19 疫苗生产商 Dr. Reddy s Laboratories 遭遇网络攻击，迫使其关闭了在巴西、印度、俄罗斯、英国和美国的工厂。 据《经济时报》报道，该公司遭受了数据泄露。为了应对安全漏洞，COVID-19 疫苗制造商隔离了所有数据中心服务。 首席信息官穆克什·拉提在一份媒体声明中表示:在检测到网络攻击之后，他们已经隔离了所有的数据中心服务，以采取必要的预防措施。他们预计所有服务将在 24 小时内恢复，并且预计此次事件不会对运营造成重大影响。

详情

COVID-19 vaccine manufacturer suffers a data breach

https://securityaffairs.co/wordpress/109994/hacking/covid-19-vaccine-manufacturer-hacked.html

律师事务所的谷歌员工个人信息数据遭泄露曝光

日期: 2020-10-26

等级: 中

来源: Lawrence Abrams

标签: ['Fragomen', 'Google', 'Data Breach', 'Law Firm']

移民律师事务所`Fragomen`，`Del Rey`，`Bernsen＆Loewy`，`LLP`披露了一项数据泄露事件，泄露了当前和以前`Google`员工的个人信息。 Fragomen 是美国最大的涵盖移民法的律师事务所之一，在全球 47 个地区拥有 582 位律师。 该律师事务所最近得知他们的网络被入侵，黑客访问了一个包含谷歌个人信息的文件。该文件包含了一些零散的谷歌员工(和前谷歌员工)的个人信息。

详情

Google employees personal info exposed in law firm data breach

https://www.bleepingcomputer.com/news/security/google-employees-personal-info-exposed-in-law-firm-data-breach/

桑坦德银行表示无需担心 PagoFX 的黑客攻击行为

日期: 2020-10-27

等级: 中

来源: Iain Thomson

标签: ['Santander', 'PagoFX', 'Underground Hacking Forum', 'Data Leak', 'Salesforce']

简言之，桑坦德银行（西班牙金融巨头）淡化了其国际转账初创公司 PagoFX 受到损害的说法。 2020 年 10 月 25 日，一位匿名消息人士联系了`The Register`平台，该消息人士称属于`PagoFX`的"数据库架构，基础架构文档，数字风险评估，客户安全检查和 Salesforce 培训材料"已被盗并在地下黑客论坛销售。 据称，这些文件（总共近 2GB）是从`PagoFX`使用的第三方软件开发人员那里窃取的。桑坦德银行的一位发言人告诉`The Register`，8 月份发现了一次泄露，不过他不愿透露任何细节，只是说其核心系统未受影响，"没有敏感的个人信息或支付数据"被窃取。从此次泄露的文件列表来看，大部分是示例源代码、用于内部程序和网络安全政策的 Word 文档等等。

详情

Santander downplays 'hack' of PagoFX cash transfer biz, says nothing to worry about
https://www.theregister.com/2020/10/27/in_brief_security/

亚马逊通知客户：由于数据泄露，解雇掉了内部人员

日期: 2020-10-27

等级: 中

来源: Ax Sharma

标签: ['Amazon', 'Data Leak', 'Twitter']

亚马逊(Amazon)最近解雇了一些员工，因为他们违反公司政策，将客户数据(包括电子邮件地址)泄露给了一家非关联的第三方。 事件发生后，该公司向受影响的客户发送了一封电子邮件通知。尽管邮件通知将事件归咎于"亚马逊员工"，但一份公司声明暗示，可能有多名内部人士应对此负责。

详情

Amazon sacks insiders over data leak, alerts customers
https://www.bleepingcomputer.com/news/security/amazon-sacks-insiders-over-data-leak-alerts-customers/

相关安全建议

1. 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
2. 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
3. 严格控制数据访问权限
4. 管控内部员工数据使用规范，谨防数据泄露并及时做相关处理
5. 注重内部员工安全培训
6. 建议加大口令强度，对内部计算机、网络服务、个人账号都使用强口令
7. 登陆入口增加验证码功能。
8. 发生数据泄漏事件后，及时进行密码更改等相关安全措施

(三) 网络攻击

黑客在窃取 Harvest Finance2400 万美元后被确认身份

日期: 2020-10-27

等级: 高

来源: SECURITYAFFAIRS

标签: ['Harvest Finance', 'Cryptocurrency', 'Web Portal ', 'Attack']

黑客已经从分布式金融服务`Harvest Finance`窃取了价值约 2400 万美元的加密货币资产，该网站是一个门户网站，让用户发现农业机会，使他们的产量(APY)回报最大化。 攻击者最初在`Harvest Finance`公司的服务中投资了大量加密货币资产，然后利用加密技术窃取平台的资金，并将其转移到`Harvest Finance`公司控制的钱包中。 专家们注意到，攻击发生后不久，黑客返还了大约 250 万美元给`Harvest Finance`，但他们并没有说出原因。

详情

Hacker was identified after the theft of $24 million from Harvest Finance

https://securityaffairs.co/wordpress/110043/cyber-crime/harvest-finance-cyber-heist.html

严重的 Oracle WebLogic 漏洞被在野利用

日期: 2020-10-29

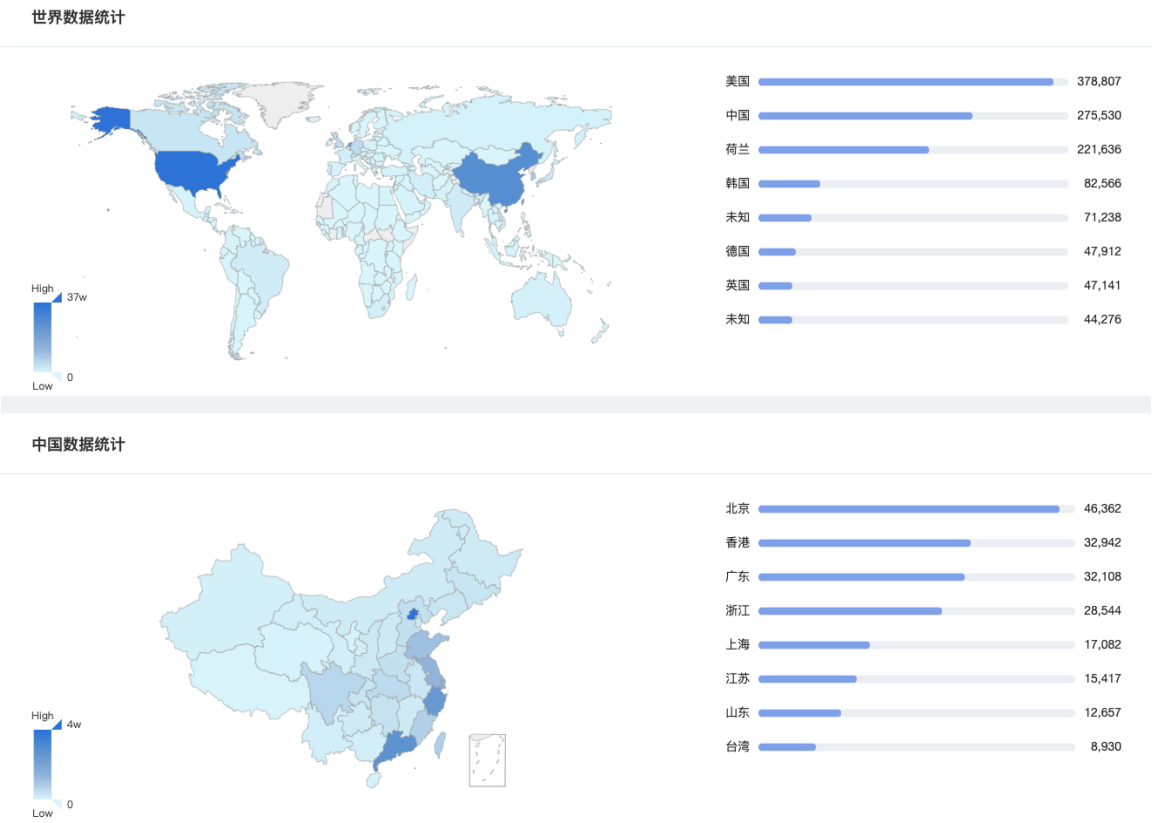
等级: 高

来源: Ionut Ilascu

标签: ['Oracle Weblogic', 'HTTP', 'Vulnerability', 'CVE-2020-14882', 'No Authentication']

攻击者已经开始寻找运行`Oracle WebLogic`实例的服务器，这些服务器容易受到一个严重漏洞的攻击，这个漏洞允许不需要认证就能控制系统。 攻击中利用的漏洞是 CVE-2020-14882，其严重性评级为 9.8(满分 10 分)，允许通过一个简单的 HTTP GET 请求危及系统。Oracle 在 2020 年 10 月发布的高危补丁更新(CPU)中修复了该漏洞，并将其归功于`Chaitin`安全研究实验室的安全研究员`Voidfyoo`的发现和报告。

目前 Weblogic 的具体分布如下图，数据来自于 360 QUAKE



详情

Critical Oracle WebLogic vulnerability exploited in the wild

https://www.bleepingcomputer.com/news/security/critical-oracle-weblogic-vulnerability-exploited-in-the-wild/

与俄罗斯有关的图拉 APT 黑客攻击了欧洲政府组织

日期: 2020-10-29

等级: 高

来源: Pierluigi Paganini

标签: ['European', 'Accenture', 'APT Turla ', 'Russia', 'Attack']

埃森哲网络威胁情报公司(ACTI)发布的一份报告称，与俄罗斯有关的网络间谍组织图拉(Turla)侵入了一个秘密欧洲政府组织的系统。 Turla APT 组织（又名 Snake，Uroburos，Waterbug，Venomous Bear 和 KRYPTON）自 2007 年以来一直活跃，其目标客户是中东，亚洲，欧洲，北美和南美以及前苏联集团的外交和政府组织以及私营企业。

详情

Russia-linked Turla APT hacked European government organization

https://securityaffairs.co/wordpress/110127/apt/turla-target-eu-gov-org.html

大学电子邮件劫持攻击推送钓鱼邮件与恶意软件

日期: 2020-10-29

等级: 高

来源: THREATPOST

标签: ['University', 'Email Hijacking', 'Phishing', 'Malware']

网络犯罪分子劫持了包括普渡大学、英国牛津大学和斯坦福大学在内的十多所大学的合法电子邮件账户，并利用这些账户绕过检测，诱骗受害者交出他们的电子邮件证书或安装恶意软件。 INKY 的首席执行官和联合创始人 Dave Bagget 告诉网站 Threatpost，目前还没有迹象表明这些账户是如何被入侵的，但他推测，受害者落入了一种获取证书的圈套。 Bagget 还说，这个月研究人员继续看到来自真实大学账户的钓鱼邮件，所以一些账户似乎仍然受到威胁。

详情

University Email Hijacking Attacks Push Phishing, Malware

https://threatpost.com/university-email-hijacking-phishing-malwarephishing-malware/160735/

InnerSloth 游戏玩家受到了严重的垃圾邮件攻击

日期: 2020-10-26

等级: 中

来源: WELIVESECURITY

标签: ['InnerSloth', 'Eris Loris', 'YouTube', 'Spam Attack']

InnerSloth 是一款人气颇高的推理推理类社交游戏的开发商，但它不得不在玩家在线比赛期间抵御一场影响其玩家的网络攻击。这一事件始于 2020 年 10 月 22 日，以垃圾邮件的形式轰炸玩家的游戏内聊天。 游戏参与者在聊天时被灌输大量的垃圾信息，包含一个`Eris Loris`句柄，促使玩家订阅其`YouTube`频道。 一些消息甚至威胁玩家，警告玩家除非订阅他们的设备，否则它们将被黑客入侵。

详情

'Among Us' players hit by major spam attack

https://www.welivesecurity.com/2020/10/26/among-us-players-hit-major-spam-attack/

Nando 的黑客大肆利用客户账户

日期: 2020-10-26

等级: 中

来源: THREATPOST

标签: ['Nando', 'Chicken Dinner', 'Credential Stuffing Attack', 'Brute Force']

一家颇受欢迎的鸡肉晚餐连锁店的食客们发现，在网络攻击者能够获取他们的餐厅点餐凭证后，他们的银行账户中被抽走了数百美元。但问题是，支付卡信息并没有存储在 Nando 的账户中，黑客入侵究竟是如何发生的。 Nando 的 Peri-Peri 鸡肉餐厅连锁店在英国和欧洲城市中存在很多店铺，在美国也有数十个地点。 它证实了 2020 年 10 月 23 日的凭证填充攻击。 凭证填充是由黑客完成的，他们利用那些经常在多个在线帐户中重复使用相同密码的用户。 这些网络攻击者利用先前数据泄露中窃取的密码和用户名，对账户进行大规模暴力攻击，一旦发现匹配，他们就可以接管受害者的账户。

详情

Nando's Hackers Feast on Customer Accounts
https://threatpost.com/nandos-hackers-customer-accounts/160527/

特朗普的官方竞选网站遭到黑客的破坏

日期: 2020-10-28

等级: 中

来源: Chris Williams

标签: ['Donald Trump', 'Campaign Website', 'Vandalized', 'Uncle Sam', 'Attack']

唐纳德·特朗普(Donald Trump)的总统竞选网站 2020 年 10 月 28 日晚遭到了短暂的黑客攻击和损毁。 这个名为`donaldjtrump.com`的网站被篡改，取而代之的是一条模仿山姆大叔特工们通常宣布的、针对犯罪分子的域名查封。上面和美国政府的封条一起声称，“这个网站被查封了”，因为”世界已经受够了唐纳德·J·特朗普总统每天散播的假新闻”。

详情

Trump's official campaign website vandalized by hackers who 'had enough of the President's fake news'
https://www.theregister.com/2020/10/28/trump_website_hacked/

Xfinity, McAfee 品牌域名被攻击者滥用

日期: 2020-10-29

等级: 中

来源: Tara Seals

标签: ['Emotet', 'Comcast', 'Domain Parking', 'Emotet', 'McAfee']

`停驻域名`可作为别名并重定向到其他网站，可以将访问者重定向到恶意或不需要的登录页面——最近的`Emotet`勒索软件运营商的运动，滥用`Comcast`和`McAfee`品牌的单独行动以及一次以选举为主题的攻击就证明了这一点。 帕洛阿尔托网络公司(Palo Alto Networks)的研究人员在 2020 年 10 月 28 日的一份分析报告中指出，`domain-parking`通常发生在为广告服务的领域。如果有人搜索`BreadDepot`(虚构的例子)，这个人可能会在`Bread Depot.net`而不是官方的`BreadDepot.com`上搜索，因为它会出现在搜索结果中。如果`BreadDepot.net`是一个寄望于人们犯这个错误而创建的域名，它可以将访问者重定向到一个满是广告的页面，以提高印象。

详情

Xfinity, McAfee Brands Abused by Parked Domains in Active Campaigns
https://threatpost.com/xfinity-mcafee-brands-abused-parked-domains/160698/

相关安全建议

1. 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
2. 积极开展外网渗透测试工作，提前发现系统问题
3. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等

4. 建议加大口令强度，对内部计算机、网络服务、个人账号都使用强口令
5. 减少外网资源和不相关的业务，降低被攻击的风险
6. 条件允许的情况下，设置主机访问白名单

(四) 其他事件

100 多个灌溉系统在没有保护的情况下暴露在网上

日期: 2020-10-27

等级: 高

来源: SECURITYAFFAIRS

标签: ['Israeli', 'Security Joes', 'Motorola', 'ICC PRO', 'Irrigation Systems', 'Shodan']

以色列安全公司 Security Joes 的安全专家发现，运行`ICC PRO`的 100 多个灌溉系统在没有保护的情况下暴露在网上。`ICC PRO`是由摩托罗拉公司设计的顶级智能灌溉系统。 ICC PRO 系统是使用默认出厂设置进行部署的，这些默认设置没有给默认用户帐户设置密码。更糟糕的是，专家指出，使用 Shodan 等物联网搜索引擎来搜索互联网上公开的这些设备非常简单。 一旦攻击者获得了访问设备的权限，它可以从控制面板执行多种操作，包括控制发送到水泵的水的数量和压力，删除用户，或更改设置等。

详情

Over 100 irrigation systems left exposed online without protection

https://securityaffairs.co/wordpress/110032/iot/irrigation-systems-exposed-online.html

超 10 万台计算机仍然易受 SMBGhost 攻击

日期: 2020-11-01

等级: 高

来源: Pierluigi Paganini

标签: ['Microsoft', 'SMBGhost', 'CVE-2020-0796']

在微软发布了严重 SMBGhost 漏洞的补丁 8 个月后，超过 10 万个在线暴露的系统仍然容易受到此攻击。2020 年 3 月，微软已经解决了服务器消息块（SMB）协议中的严重 SMBGhost 漏洞（CVE-2020-0796）。 远程代码执行漏洞存在于 Microsoft Server Message Block 3.1.1 (SMBv3)协议处理某些请求的方式中。成功利用该漏洞的攻击者可以在目标服务器或客户机上执行代码。

详情

103,000 machines are still vulnerable to SMBGhost attacks

https://securityaffairs.co/wordpress/110247/hacking/smbghost-vulnerable-machines-dangers.html

研究人员用密码 MAGA2020 登录特朗普的推特

日期: 2020-10-28

等级: 中

来源: HACKREAD

标签: ['Dutch', 'Victor Gevers', 'Trump', 'Twitter', 'Password']

荷兰网络安全研究员维克多·盖弗斯透露，他在猜到美国特朗普的总统账号密码`MAGA2020`后，成功登录了该账号。MAGA 代表"让美国再次伟大"，而这恰好是特朗普总统在他成功的 2016 年总统大选中使用的竞选口号。 研究人员还透露，特朗普没有对该帐户启用两步验证，这意味着任何可以猜出该密码的人都可以登录该帐户，进行更改并鸣叫他们想要的任何内容。 这个拥有 8700 万粉丝的推特账户是特朗普总统的个人账户，自 2017 年 1 月当选总统以来一直非常活跃。

详情

Researcher logs into Trump's Twitter with password MAGA2020
https://www.hackread.com/researcher-logs-trump-twitter-password-maga2020/

QNAP 警告可能会导致设备被接管的 QTS 漏洞

日期: 2020-10-28

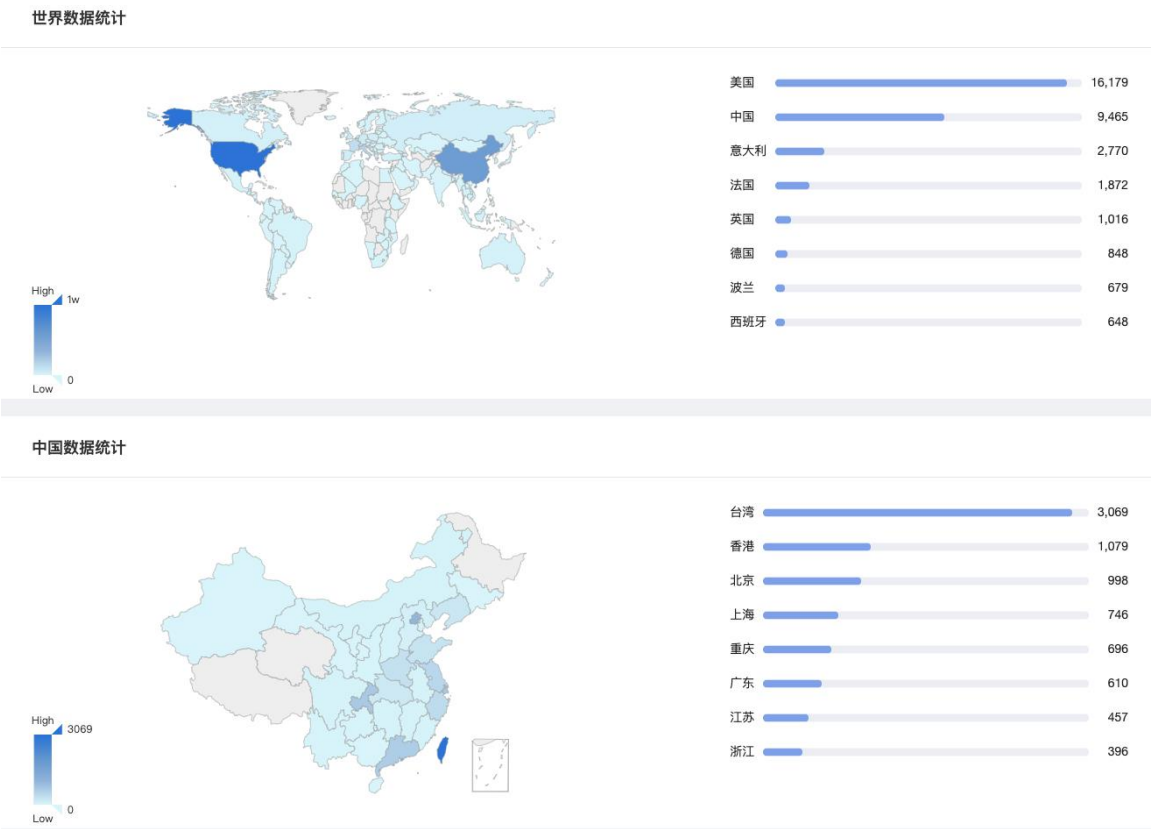
等级: 中

来源: Ionut Ilascu

标签: ['QNAP', 'QTS', 'Vulnerability', 'Command Injection']

`QNAP` 2020 年 10 月 28 日公布了两个影响 QTS 的漏洞，QTS 是支持其网络存储设备的操作系统，可能允许运行任意命令。 这些漏洞可以被远程利用，并且已经在 2020 年 9 月 8 日之前发布的版本中被报告。 `QNAP`表示，这两个漏洞的编号为 CVE-2020-2490 和 CVE-2020-2492，为命令注入漏洞。

目前 QTS 的具体分布如下图，数据来自于 360 QUAKE



详情

QNAP warns of new QTS bugs that allow take over of devices
https://www.bleepingcomputer.com/news/security/qnap-warns-of-new-qts-bugs-that-allow-take-over-of-devices/

NVIDIA 修补了高性能服务器中的高危漏洞

日期: 2020-10-29

等级: 中

来源: Tom Spring

标签: ['NVIDIA', 'Vulnerability', 'AI', 'Patches']

NVIDIA 针对其高性能 DGX 服务器产品线中的高危漏洞发布了补丁，该漏洞可能会为远程攻击者打开大门，使他们可以控制和访问通常由政府和财富 100 强公司运营的系统上的敏感数据。 NVIDIA 共发布了 9 个补丁，每个补丁都修复了 DGX 高性能计算（HPC）系统使用的固件中的漏洞，这些漏洞用于处理器密集型人工智能（AI）任务，机器学习和数据建模。 所有这些漏洞都与在 DGX AMI 基板管理控制器（BMC）上运行的自己的固件有关，该固件是远程监控服务服务器背后的大脑。

详情

NVIDIA Patches Critical Bug in High-Performance Servers
https://threatpost.com/nvidia-critical-bug-hpc/160762/

相关安全建议

1. 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
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. 建议加大口令强度，对内部计算机、网络服务、个人账号都使用强口令

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