北京安域领创科技有限公司

安全通告

报告周期：2023 年 5 月第一周

(2023 年 5 月 5 日 2023 年 5 月 12 日)

目　录

1 本周漏洞通告

1.1 漏洞一：Textpattern CMS 任意文件上传漏洞

发布时间	2023-05-11
更新时间	2023-05-11
CNVD-ID	CNVD-2023-36289
漏洞危害级别	高
影响产品	Textpattern CMS Textpattern CMS v4.8.8
漏洞类型	通用型漏洞
漏洞描述	Textpattern CMS 是 Textpattern 团队的一个基于 Php 的内容管理系统。 Textpattern CMS v4.8.8 版本存在任意文件上传漏洞。该漏洞源于应用对上传的文件缺少有效的验证。攻击者利用该漏洞通过特制的 Zip 文件执行任意代码。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://textpattern.com/

1.2 漏洞二：北京宏景世纪软件股份有限公司人力资源信息管理系统存在 SQL 注入漏洞

发布时间	2023-05-06
更新时间	2023-05-06
CNVD-ID	CNVD-2023-08743
漏洞危害级别	高
影响产品	北京宏景世纪软件股份有限公司 人力资源信息管理系统
漏洞类型	通用型漏洞
漏洞描述	北京宏景世纪软件股份有限公司是国内专业的 e-HR 专业厂商。 北京宏景世纪软件股份有限公司人力资源信息管理系统存在 SQL 注入漏洞，攻击者可利用该漏洞获取数据库敏感信息。
漏洞解决方案	厂商已提供漏洞修复方案，请关注厂商主页更新： http://hjsoft.com.cn/

1.3 漏洞三：Apache Solr 命令执行漏洞

发布时间	2023-05-06
更新时间	2023-05-06
CNVD-ID	CNVD-2023-34111

漏洞危害级别	高
漏洞类型	通用型漏洞
影响产品	Apache Solr <=8.3.1
漏洞描述	Apache Solr 是一个开源的搜索服务，使用 Java 语言开发，主要基于 HTTP 和 Apache Lucene 实现的。 Apache Solr 存在命令执行漏洞，攻击者可利用该漏洞在目标系统上执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新： https solr apache org downloads html

1.4漏洞四：CLTPHP 输入验证错误漏洞

发布时间	2023-05-06
更新时间	2023-05-11
CNVD-ID	CNVD-2023-36309
漏洞危害级别	高
漏洞类型	通用型漏洞
影响产品	CNVD-2023-36309
漏洞描述	CLTPHP 是一款开源的高效建站的 PHP 内容管理系统。 CLTPHP 6.0 版本及之前版本存在输入验证错误漏洞，该漏洞源于 application/admin/controller/Template.php

	存在输入验证不正确。攻击者可利用该漏洞导致任意删除文件。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://gitee.com/chichu/cltopen/

1.5 漏洞五：OURPHP SQL 注入漏洞

发布时间	2023-05-06
更新时间	2023-05-11
CNVD-ID	CNVD-2023-36313
漏洞类型	通用型漏洞
漏洞危害级别	高
影响产品	OurPHP OurPHP <=7.2.0
漏洞描述	OURPHP 是 OURPHP 开源的一个开源、跨平台、企业级+电商+小程序+APP 多终端同步的 CMS 建站系统。 OURPHP 7.2.0 版本及之前版本存在 SQL 注入漏洞。该漏洞源于应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://www.ourphp.net/

2 本周病毒木马通告

2.1 本周流行病毒木马统计

2.1.1 如何使用 CTFR 并利用证书透明日志获取 HTTPS 网站子域名

病毒危险级别：★★★

关于 CTFR

CTFR 是一款功能强大的子域名枚举与爆破工具，在该工具的帮助下，广大研究人员可以轻松在几秒钟时间里获取一个 HTTPS 网站的所有子域名。值得一提的是，CTFR 即没有使用到字典攻击技术，也没有使用暴力破解工具，该工具使用的是证书透明度日志来实现其功能。

关于证书透明度

谷歌的证书透明度项目修复了 SSL 证书系统中的几个结构缺陷，SSL 证书系统是所有 HTTPS 连接的主要加密系统。这些缺陷削弱了加密互联网连接的可靠性和有效性，并可能危及关键的 TLS/SSL 机制，包括域验证、端到端加密和证书颁发机构建立的信任链。如果不加以控制，这些缺陷可能会引发广泛的安全攻击，如网站欺骗、服务器冒充和中间人攻击等。

工具要求

```
Python 3+

pip3
```

工具安装

由于该工具基于 Python 3+环境，因此我们首选需要在本地设备上安装并配置好 Python 3+环境。接下来，运行下列命令安装 pip3 工具：

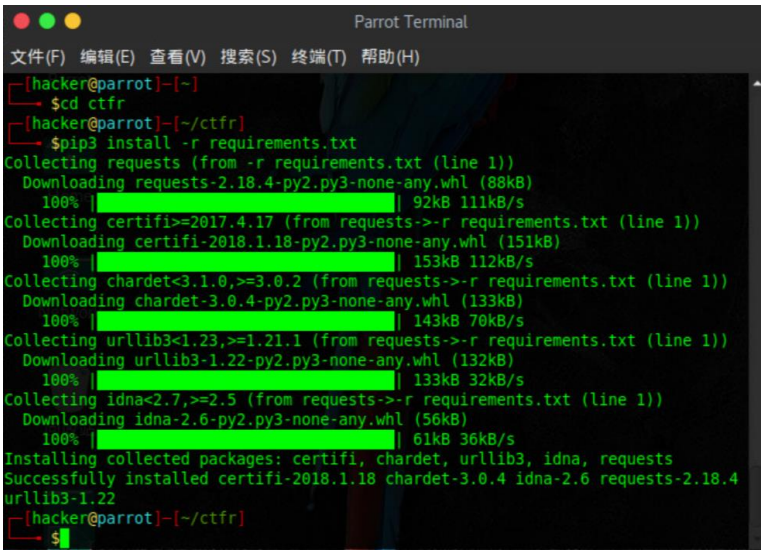
```
sudo apt-get install python3-pip
```

然后使用下列命令将该项目源码克隆至本地：

```
git clone https://github.com/UnaPibaGeek/ctfr.git
```

切换到项目目录中，使用 pip3 命令和项目提供的 requirements.txt 安装该工具所需的其他依赖组件：

```
cd ctfr

pip3 install -r requirements.txt
```



工具运行

```
python3 ctfr.py --help
```

Docker 使用

```
docker pull unapibageek/ctfr

docker container run --rm unapibageek/ctfr -d starbucks.com
```

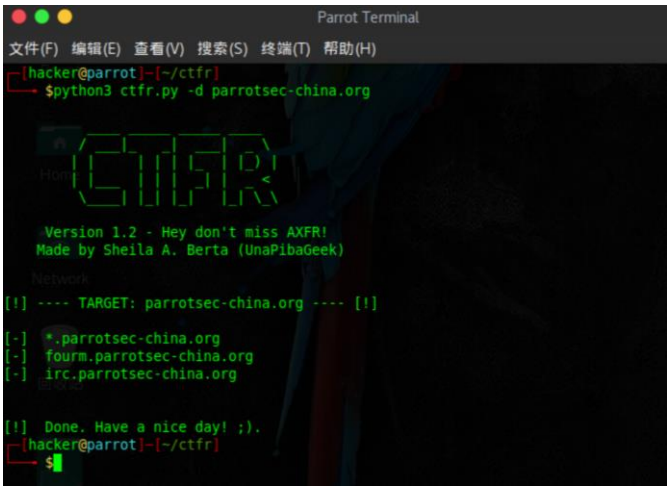
工具参数

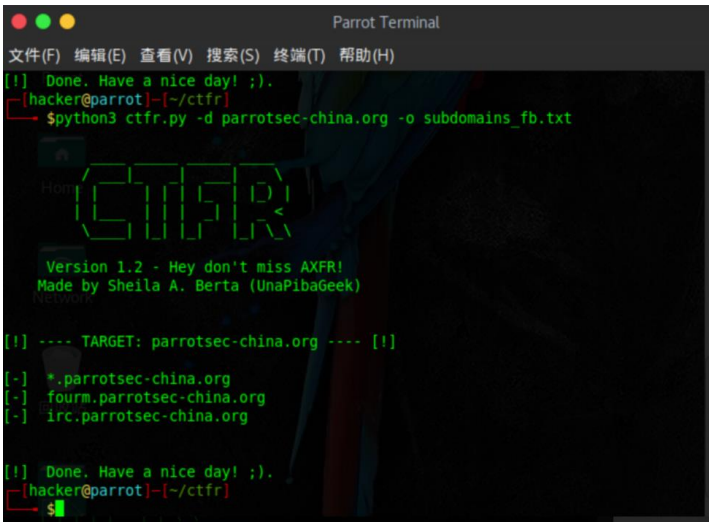
```
-d --domain [目标域名] (必须)

-o --output [输出文件] (可选)
```

工具使用样例

```
python3 ctfr.py -d starbucks.com

python3 ctfr.py -d facebook.com -o /home/shei/subdomains_fb.txt
```

工具运行截图





3 安全事件通告

3.1 本周国内外安全事件通告

3.1.1 针对 VMware ESXi 的勒索软件爆发！因源码泄露，近一年涌现出 9 个变种

多个恶意黑客团伙利用 2021 年 9 月 Babuk（又名 Babk 或 Babyk）勒索软件泄露的源代码，构建了多达 9 个针对 VMware ESXi 系统的不同勒索软件家族。美国安全厂商 SentinelOne 公司的研究员 Alex Delamotte 表示，“这些变体在 2022 年下半年至 2023 年上半年开始出现，表明对 Babuk 源代码的利用呈现出上升趋势。”“在泄露源代码的帮助下，即使恶意黑客缺乏构建攻击程序的专业知识，也能对 Linux 系统构成威胁。”许多大大小小的网络犯罪团伙都将目光投向 ESXi 管理程序。自今年年初以来，已经出现至少三种不同的勒索软件变种——Cylance、Rorschach（又名 BabLock）和 RTM Locker 等，它们都以泄露的 Babuk 源代码为基础。

图：Babuk 默认展示的赎金消息

SentinelOne 最新分析表明，如今这种现象已经愈发普遍，Conti 和 REvil（又名 REvix）等黑客团伙也开始利用 Babuk 源代码开发更多 ESXi 勒索软件。其他将 Babuk 功能移植进自身代码的勒索软件家族还包括 LOCK4、DATAF、Mario、Play 和 Babuk 2023（又名 XVGV）等。尽管出现了明显的趋势，但 SentinelOne 公司表示，它没有观察到 Babuk 同 ALPHV、Black Basta、Hive 及 LockBit 的 ESXi 勒索软件间存在相似之处。该公司还发现，ESXiArgs 和 Babuk 之间同样“几乎没有相似之处”，表明之前的归因可能有误。Delamotte 解释道，“随着越来越多 ESXi 勒索软件采用 Babuk 源代码，恶意黑客们有可能会转向该组织基于 Go 语言开发的 NAS 勒索软件。在黑客群体之间，Go 语言目前仍是个小众选项，但其接受程度正在不断增加。”这一趋势始于 Royal 勒索软件的幕后团伙（疑似前 Conti 成员）扩展攻击工具库，他们曾将针对 Linux 和 ESXi 环境的 ELF 变体纳入自己的武器储备。Palo Alto Networks 旗下安全部门 Unit 42 发布文章也指出，“ELF 变体与 Windows 变体非常相似，样本没有使用任何混淆技术。包括 RSA 公钥和赎金记录在内的所有字符串，均以明文形式存储。” Royakl 勒索软件攻击会从各种初始访问向量（如回调钓鱼、BATLOADER 感染或窃取凭证等）起步，随后投放 Cobalt Strike Beacon 以预备执行

勒索软件。自 2022 年 9 月出现以来，Royal 勒索软件已在其泄露网站上宣称对 157 家组织的事件负责，其中大多数攻击针对美国、加拿大和德国的制造、零售、法律服务、教育、建筑及医疗服务组织。

3.1.2 推特终于推出了加密的直接信息，仅限验证的用户

在埃隆-马斯克（Elon Musk）于 2022 年 11 月确认该功能的计划后五个多月，Twitter 正式开始在该平台上推出加密直接信息（DMs）的功能。

这一功能的 “第一阶段 “将作为单独对话出现在用户收件箱的旁边。加密的聊天记录会有一个锁定的图标，以便在视觉上加以区分。

选择加入功能目前仅限于经过验证的用户或经过验证的组织及附属机构。此外，发送方和接收方都必须使用 Android、iOS 和客户端最新版本的 Twitter 应用程序。

发送和接收加密信息的另一个标准是，收件人必须关注发件人，过去曾向发件人发送过信息，或者在某个时候接受过发件人的直接信息请求。

虽然 Twitter 没有透露它用来加密对话的确切方法，但该公司表示，它采用了 “强大的加密方案组合 “来加密用户的信息、链接。

Twitter 进一步强调，加密的聊天内容储存在其基础设施上时仍然是加密的，只有在接收方的一端才会解密。该实施方案预计将在今年晚些时候开放源代码。

也就是说，目前该项目正在进一步开发中，现在并不支持加密的小组对话，也不允许交换媒体和其他文件附件。其他一些值得注意的限制如下：

- 用户最多只能注册 10 台设备来发送和接收加密信息。
- 新设备（重新安装 Twitter 应用程序）不能参与现有的加密对话
- 从 Twitter 注销将调用所有信息，包括加密的 DMs，从当前设备上删除

Twitter 还表示，当前的架构不能“提供针对中间人攻击的保护”，并且不保证前向保密，这是一项关键的安全措施，可确保单个会话密钥的泄露不会影响其他会话中共享的数据。

“如果注册设备的私钥被泄露，攻击者将能够解密该设备发送和接收的所有加密消息”。Twitter 表示，并补充说它不打算修复限制，而是考虑更好的用户体验。

3.1.3 西班牙警方捣毁大规模网络犯罪团伙，逮捕 40 名嫌疑人

西班牙国家警察局逮捕了 40 名 Trinitarians 网络犯罪团伙的成员。据悉，这群人中包括两名通过网络钓鱼等技术手段实施银行诈骗的黑客，以及 15 名犯有银行诈骗、伪造文件、身份盗窃和洗钱等多项罪行的犯罪分子。

对于此次抓捕行动，西班牙政府方面表示 Trinitarians 犯罪组织利用黑客工具实施计算机诈骗，据信总共诈骗了 30 多万受害者，造成了 70 多万欧元的损失。

犯罪分子通过发送短信实施诈骗

根据西班牙警方透露的消息，为发动网络攻击活动，网络攻击者通过短信发送虚假链接，一旦用户点击进去，便立刻被重定向到伪装成合法金融机构的网络钓鱼页面。这时候，网络攻击者就会窃取用户的凭据，滥用其申请贷款的权限，并将卡链接到其控制的加密货币钱包上。

值得一提的是，网络攻击者还会在发送的短信中“诱导”用户进入紧张的情绪中（一直以解决银行账户所谓的安全问题为由，催促受害者点击附带链接），从而增加诈骗成功的概率。

被网络犯罪分子盗取的卡一般都被用来购买数字资产，随后被套现，用以资助 Trinitarians 日常运营，例如支付法律费用、向监狱成员汇款，以及购买毒品和武器

等。一些非法所得也会转移到外国银行账户，集团成员用这些钱在多米尼加共和国购买房产。

此卡，西班牙国家警察局指出 Trinitarians 组织还有一个内部网络体系，用来从银行转账中收款，并通过自动取款机提取。

西班牙当局表示，通过侦察和分析线索，警方在马德里、塞维利亚和瓜达拉哈拉省进行了 13 次房屋搜查，最终查收 Trinitarians 组织大量的计算机设备、挂锁、5000 欧元现金、开锁工具包和其它包含该团伙组织结构信息的文件。

3.1.4 瑞士跨国科技公司 ABB 遭 Black Basta 勒索软件攻击，严重影响其业务运营

瑞士跨国公司 ABB 是一家行业领先的电气化和自动化技术提供商。据报道，该公司近日遭遇了 Black Basta 勒索软件攻击，影响到了其业务运营。

ABB 总部位于瑞士苏黎世，拥有约 105,000 名员工，2022 年的收入为 294 亿美元。作为其服务的一部分，该公司为制造业和能源供应商开发工业控制系统(ICS)和 SCADA 系统。该公司与很多客户和地方政府合作，包括沃尔沃、日立、DS Smith、纳什维尔市和萨拉戈萨市。

ABB 在美国运营着 40 多家工程、制造、研究和服务设施，并拥有良好的业绩记录，为多种联邦机构提供服务，包括国防部，如美国陆军工程兵团，以及联邦民用机构，如内政部、交通部、能源部、美国海岸警卫队以及美国邮政服务。

5 月 7 日，Black Basta 勒索软件对 ABB 发起了攻击。有多名员工称，勒索软件攻击影响到了该公司的 Windows Active Directory，并波及到了数百台设备。

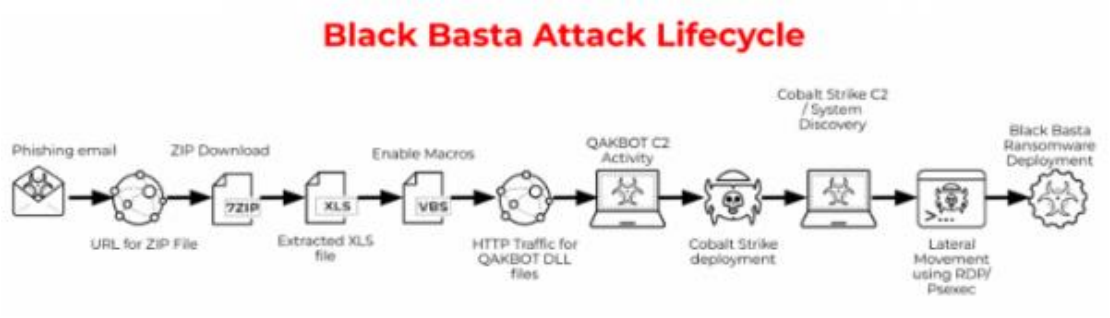
遭到攻击后，ABB 中断了与客户的 VPN 连接，以防止勒索软件传播到其他网

络。这次袭击导致该公司的不少项目被推迟，扰乱了该公司的运营及工厂生产周期。

Black Basta 勒索团伙究竟是谁?

2022 年 4 月，Black Basta 勒索软件团伙启动了勒索软件即服务(RaaS)行动，并迅速开始在双重勒索攻击中积累企业受害者。

2022 年 6 月，Black Basta 与 QBot 恶意软件操作(QakBot)合作，在受感染的设备上投放了 Cobalt Strike。不仅如此，Black Basta 还会利用 Cobalt Strike 获得公司网络的初始访问权限，并横向传播到其他设备上。



黑巴斯塔攻击流

来源:Palo Alto Networks Unit 42

与其他针对企业的勒索软件操作一样，Black Basta 创建了一个 Linux 加密器来攻击运行在 Linux 服务器上的 VMware ESXi 虚拟机。

研究人员认为，这个勒索软件团伙可能和 FIN7 黑客组织有所关联。FIN7 黑客组织是一个专门以经济作为攻击动机的网络犯罪团伙，也被称为 Carbanak。

自该勒索软件“面世”以来，威胁行为者发起了一系列攻击，攻击的对象包括美国牙科协会，索比斯，可耐福和加拿大黄页等。

最近，该勒索软件又攻击了英国最大的外包公司 Capita，并在网上泄露其盗取来的数据。

3.1.5 长达两年调查：朝鲜黑客入侵韩国最大医院致 831,000 人信息泄露

韩国国家警察厅（KNPA）警告说，朝鲜黑客入侵了该国最大的医院之一首尔国立大学医院（SNUH）的网络，以窃取敏感的医疗信息和个人详细信息。该事件发生在 2021 年 5 月至 6 月之间，警方在过去两年中进行了分析调查，以确定肇事者。

根据执法机构的新闻稿，根据以下信息将此次攻击归因于朝鲜黑客：

在攻击中观察到的入侵技术

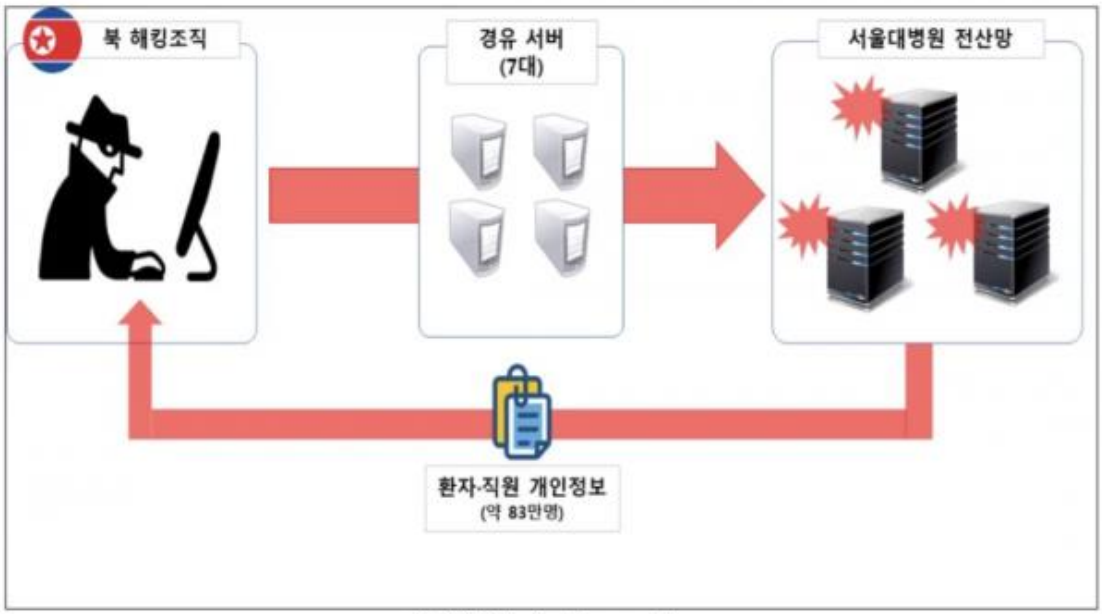
与朝鲜威胁行为者独立关联的 IP 地址

网站注册详情

特定语言和朝鲜语词汇的使用

韩国当地媒体将这次袭击与 Kimsuky 黑客组织联系起来，但警方的报告并未明确提及具体的威胁组织。

攻击者使用韩国等国的七台服务器对医院内部网络发起攻击。



攻击概要 *(police.go.kr)*

警方表示，该事件导致 831,000 人的数据泄露，其中大多数是患者。此外，受影响的人中有 17,000 人是现任和前任医院员工。

KNPA 新闻警告说，朝鲜黑客可能会试图渗透各个行业的信息和通信网络。它强调需要加强安全措施和程序，例如实施安全补丁、管理系统访问和加密敏感数据。

KNPA 警告说：“我们计划调动我们所有的安全能力，积极应对国家政府支持的有组织网络攻击，并通过信息共享和与相关机构的合作来防止进一步的损害，从而坚定地保护韩国的网络安全。”

毛伊岛和安达利尔

据悉，朝鲜黑客此前与医院网络入侵有关，旨在窃取敏感数据并向医疗机构勒索赎金。

美国政府曾强调了 Maui 勒索软件威胁本身，警告医疗保健部门他们需要加强对朝鲜行动的防御。

发出此警告后不久，卡巴斯基的安全研究人员将 Maui 勒索软件操作与名为“Andariel”（又名“Stonefly”）的特定活动集群联系起来，该活动被认为是 Lazarus 的一个子组。

自 2021 年 4 月以来， Lazarus 以使用勒索软件攻击韩国实体而闻名 。