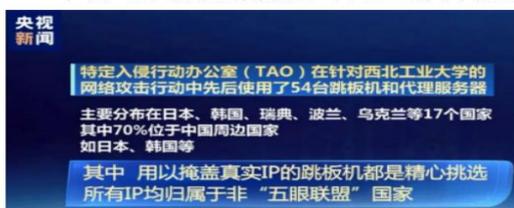


# 3Gweb-Shadow 影子防御系统简介

## 1、为什么需要影子防御？

- ◆ 生成式 AI 武器化的危险时代已到来！能根据攻击目标的漏洞、网络等状态每 24 小时自动生成攻击程序并实施攻击的 AI 武器已经列装 M 国网军。FBI 警告“使用 AI 发动网络攻击的黑客数量正在以惊人的速度增加”。黑客专用大模型 FraudGPT 能低门槛快速生成攻击代码和钓鱼邮件，哪怕是初级黑客。意味着互联网上每天都会新生海量的 AI 攻击，包括 AI+勒索、AI+APT 等。黑客机器人泛滥，网络空间防御变得异常困难，数字经济的拦路虎！
- ◆ 您的网站/Web 和 IT 系统直接接触和暴露在互联网，还带有大量漏洞。而攻击者都在隐身！
- ◆ 今天的互联网是高度动态变化、AI+网络战时代的互联网，是最大的攻击传染源！在这开放的网络空间里充斥着武器化的 AI 攻击、凶猛的勒索攻击、国家级高烈度网络攻击、堵不完的漏洞攻击（平均 480 种新漏洞/周，CNCERT）、每天超 38 万前所未有的恶意软件(卡巴斯基)等无数的**未知攻击**，还有 SQL 注入、命令注入、DDoS 等**已知攻击**。您面对的是结盟的西方网军、泛滥的攻击机器人、产业化的黑客团伙。WAF 等传统安全产品已不够用了。
- ◆ 您的 IT 系统存在两大安全短板：①不能防御“未知攻击”；②仍在用 Apache、IIS、nginx 等美国落后的二代 Web，没有实现自主可控替代！是互联网最大安全漏洞！在向网军和黑客提供着入侵通道：超过 75% 的互联网攻击、对云攻击是针对 Web 实施的！
- ◆ M 国国家力量对我国数据安全的威胁在加剧：

- 2021年5月，美国总统拜登一声令下，美国中情局从云上偷取了武汉病毒研究所的大量数据(美国CNN报道)；
- 2022年爆出了多个美国安局的监听窃密平台：“NOPE”木马、“电幕行动”、“量子攻击”、“酸狐狸”等；
- 2023年7月，武汉市地震检测中心系统遭美国入侵，植入后门程序，长期盗取地震敏感数据；
- 2022年9月5日，央视新闻报道：西北工业大学发现遭**美国国家安全局的TAO**的网络攻击窃密，……



- 先后使用了**41种**专用网络攻击武器装备，利用**多个**尚未被发现的漏洞；通过隐藏在**17个国家**里的**54台**计算机发起了攻击。渗透的攻击链路多达1100余条；
- **大约140GB的高价值科研数据被窃**

<https://mp.weixin.qq.com/s/TXS54RbkQgdYOv3hGEWgBQ>

美国早有警告：“在国家支持的网络安全攻击面前，传统网络安全工具根本就是螳臂挡车。”

——《网络空间战与未来网络安全》，美ZDNet, 2018年末

攻击者都在**隐身**，被攻击者却直接接触和暴露在互联网上……

## 2、3Gweb 影子防御系统的简单概念

### 3Gweb-Shadow 影子防御网站中心



颠覆“攻击者**隐身**，被攻击者却直接暴露在互联网上……”的传统互联网攻防模式。

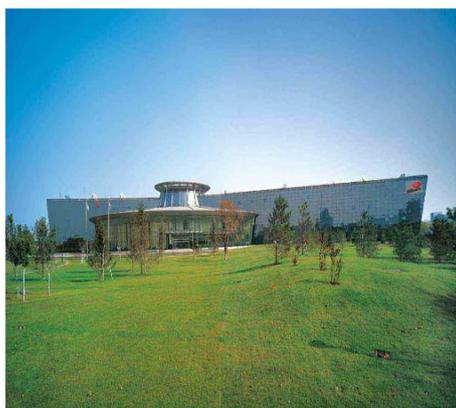
国家发明专利申请

让网民看得见您，让黑客找不到您！基于先进的国产互联网核心技术。



- 让您的网站从互联网上**隐身**！让攻击者看到的和攻击的只是您的影子！
- 让网站远离互联网-最危险的攻击传染源；减少互联网暴露点！
- 网络战级别的抗攻击能力：“隐身+隔离+生物自防御”；抗未知攻击；
- 快速构建网络空间纵深防御体系，与原安全产品兼容；补齐两大安全短板；
- 导入容易：每月付费即可享受最先进的影子防御服务！无论您的网站在哪里，无论在云上或不在云上……
- #1 影子网站中心：与联通合作 

## 全球首个影子网站中心:



- 五星级数据中心、TIER III+标准、世界一流水平的通信机房和IDC机房，园林化的办公环境；
- IDC大厦内有骨干传输节点，有充足的出局光纤，上联北京联通AS4808带宽1600G；
- 信息安全管理系统认证 ISO/IEC 27001；
- 提供流量清洗等抗DDoS攻击服务；
- 现有30余人组成的维护队伍，具有多年的通信行业维护经验，50%的运维人员具备高、中级技术职称；其中不乏拥有资深的网络专家。
- 7X24监控网络运行状况，进行网络配置管理、故障管理、网络性能管理、网络优化和网络运行分析。
- 动力环境监控系统可监控到高压市电停电、柴油发电机、UPS旁路柜、蓄电池、空调、输出配电柜、交流列头柜的运行情况烟感和FM-200，漏水检测声音报警都在监视报警范围内。
- #1 影子网站中心：与中国联通合作。 

全球首个影子网站: <https://www.bj3gweb.com> (已通过工信部ICP网站备案审查)

## 影子防御的核心技术二：第三代Web服务器

3Gweb®生物自防御Web服务器的主功能还是基于W3C国际http标准的Web服务器。但是其内部克隆了人体的生物自防御机制，实现了Web服务器里从表层到深层的多层防线，自己保护自己，成为不可篡改、不可挂马、防数据泄露不怕漏洞的新一代Web服务器。高可信&抗攻击，特别是抗“未知攻击”。是实现了弯道超车的国产互联网核心技术之一。

产品形态：机架式、超融合、双主板高性能计算机+4万预装文件；  
唯一的中国民族品牌的Web服务器，网络战时代的高端Web服务器；



3Gweb®生物自防御Web服务器  
(超融合高性能计算机，软硬件一体化)



用科学促进互联网的发展 用科学维护互联网的和平

30

## 3、3Gweb-Shadow 影子防御带给您什么？

基于更先进的国产互联网核心技术的 3Gweb-Shadow 影子防御系统将颠覆“攻击者隐身、被攻击者直接暴露在互联网上被动挨打”的传统互联网攻防模式，让您从互联网隐身！让攻击者攻击的只是您的影子，水中月镜中花！是网络战时代最前沿的防御技术。让野火般蔓延的AI攻击、国家级高烈度网络攻击、凶猛的勒索攻击、APT、SQL注入等各类目标定向攻击迷失真的攻击目标，并增加抗未知攻击能力。让您贵重的网站/Web系统，包括关键信息基础设施的、云平台上的SaaS服务、大数据平台，官网，OA等，可以更健壮、更长久、更经济地运行在网络战时代空前险恶的互联网环境里。任凭风吹雨打，我自闲庭信步。国家发明专利申请。

“3Gweb 影子防御系统”提供前所未有的**网络战级别抗攻击能力**：

- “隐身+隔离+生物自防御+纵深防御”：

**隐身**：您的原网站将从空前险恶的互联网上隐身。让网军黑客找不到您原网站和 IP 地址，失去攻击目标；攻击者和访问者看到的仅仅是和您网站一模一样的影子！迷惑欺骗攻击者，抗御高烈度网络攻击的第一道防线；

**隔离**：原网站远离危险的攻击传染源——互联网！实现互联网与隐身网的物理隔离；从此您的原网站只面对安全的隐身网，不再直接接收来自互联网的访问请求，也不再直接承受来自互联网的攻击！不再直接接触最大的攻击传染源——互联网！

**生物自防御**：最前沿的生物自防御技术，未知攻击的克星：在计算机中实现了人体的生物自防御机制，内置“数字皮肤、免疫、自我痊愈、神经监测和排毒”五道主防线。世界第一。“隔离+生物自防御”是被验证过的可以抗御未知攻击的先进架构。

**纵深防御**：兼容您现有的安全防护系统，形成纵深防御体系。原有的安全防护强度只增不减，原来的安全投资不浪费。根据系统工程学的原理，科学地把 IT 系统被攻破的大概率事件变成小概率事件...

- 采用弯道超车的国产互联网核心技术之一的第三代 Web 服务器：3Gweb；中国美国发明专利、“Best of Interop Award”国际大奖、多家权威机构安全验证。20 年研究+10 年互联网实践检验，从未被黑。
  - ❖ **高可信**：①内容可信：被请求的 Web 内容在送出服务器时必经合法性和完整性高速检查。保证发布信息的真实性（二代 Web 不检查!）。②网站可信：支持 X.509 CA 认证，支持 SSL/TLS 证书；
  - ❖ **抗攻击**：①抗未知攻击：如：0 日攻击（新安全漏洞：200-700/周，CNCERT）、明天、今后出现的新型攻击（新恶意软件：38 万/日(卡巴斯基)）、超 100 国网军的秘密攻击武器等；②抗已知攻击：如：SQL 注入、一句话攻击、水坑攻击、网络蠕虫攻击、webshell，勒索攻击等等。极大地降低 Web 宕机几率。
- 不可篡改、不可挂马、不可暗链、0 秒恢复，防植入木马后门程序、防数据泄露、防数据篡改擦除被加密、不怕漏洞、防渗透，防监听.....
- 补齐原网站系统的两大安全短板：1)增加抗未知攻击的能力，2)封堵 Apache、IIS、Nginx 等美国二代 Web 带来的入侵通道和隐患。黑客机器人、勒索、APT、SQL 注入等攻击再也不能利用二代 Web 这一暗道入侵您的 Web 系统、数据库、云平台和网络了！
- 抗御勒索攻击(Ransomware)：让这唯一被美国定为“将利用国家力量的所有要素”消灭的黑客技术《(美国)2023 年国家网络安全战略》，还有 APT 攻击等定向攻击，迷失真的攻击目标！3Gweb 的“排毒功能”更让它们的木马程序不能驻留潜伏；
- 抗御 AI 攻击：隐身+抗未知攻击+抗 AI 攻击+纵深防御的架构，让暴增的 AI 攻击从互联网上找不到您！无法扫描发现您的网络漏洞；“排毒功能”更让 AI 攻击程序不能驻留潜伏；
- 抗 DDoS 攻击：当发生 DDoS 攻击时可以从 IP 城域网超核位置，从源头位置对 DDOS 攻击进行流量清洗过滤，保证用户正常业务的开展（联通）。
- 解除安全漏洞(已知漏洞、未知漏洞、秘密漏洞)的烦恼：现今 IT 系统平均每周新生 480 个安全漏洞（CNCERT）！0day 攻击暴增，为 AI 攻击提供新的攻击点。但频繁打补丁不但增加运维成本，还会增加系统的停机时间。更何况时间上已来不及每周打如此多的补丁！影子防御可以帮助您：让攻击者不能发现、接触和利用这些漏洞，再加上抗未知攻击！
- 超强抗渗透能力：您将独享一台 3Gweb 服务器：特殊结构的超融合高性能计算机，内部实现物理隔离，软硬件一体化；
- 数字皮肤里的“Smart WAF”，可以同时过滤 http 和加密的 https 通信协议。补齐云 WAF 不能过滤加密的 https 通信包、不能拦截未知攻击等短板。

- 保护用户的隐私和数字资产：原网站系统上的 web 应用程序和数据库等都留在原处，不被触及。从此不再暴露在互联网上；
- 支持国际标准的 CA 证书、https 通信，ssl 加密功能，用户的密码、信用卡号、银行卡号身份证等敏感信息，以及各种重要数据都将被自动加解密，不会发生互联网通信道泄密，防止中途窃听监听和中间人攻击；
- 解决作为互联网辅助技术的传统安全产品解决不了的诸多问题：不抗未知攻击、WAF 不能过滤 https 通信协议、来不及更新特征库、互联网战略安全等等；
- 适用范围广、兼容性强：无论是云平台上的网站还是传统主机上的网站，无论是消费互联网还是工业互联网，电子政府、电子金融、新闻媒体、医院、教育科学、交通能源、关键信息基础设施等等各行各业的网站/web 系统；适用各种 OS：Unix、Windows 等，适用各种架构计算机，X86、ARM.....。适合各类拥有贵重数字资产的用户。
- 容易导入：只需按月付费，即可享受最先进的 3Gweb 影子防御服务。原网站/Web 系统无需部署设备、无需安装软件、无需改动应用系统和数据库；通过 DNS 解析快速接入。无论您的网站在哪里。无论是在公有云、私有云还是没有布置在云上；无论在哪个省份.....
- 省事、省钱、省心、省时：
  - ❖ 不必再为每周修补 200-700 个漏洞安全补丁、每日更新 38 万-70 万次攻击特征库、为每天处理海量的安全警报而伤脑筋了！
  - ❖ 有效解决政企客户安全能力不足、安全支出成本居高不下的难题；减低原网站的运维成本和 IT 成本；
  - ❖ 提供漂亮的网站访问统计图表和攻击统计图表；轻松掌握网站系统的运行情况。
  - ❖ 提高系统的稳定性减少网站中断，减少因为打补丁造成的系统重启次数、不必在敏感期间拔网线了！提高网站的服务质量和生产力；
  - ❖ 避免网站和数据库被黑带来的巨大的政治损失、经济损失、罚款损失甚至刑事损失。避免水涨船高的巨额勒索赎金。
- 政策合规、自主可控：
  - ❖ 符合国务院办公厅〔2017〕47 号文的要求；满足公安部安全等保 2.0 关于 Web 安全的要求；符合《关键信息基础设施安全保护要求》（GB/T 39204-2022）国家标准要求：“收敛暴露面，减少互联网出口数量。”
  - ❖ 中国人原创发明；发明专利申请，从理论到技术到系统。境外网军和黑客尚不清楚的先进防御体系。

## 4、结束语

习总书记指出：“互联网核心技术是我们最大的命门，核心技术受制于人是我们最大隐患”。让我们一起使用更先进的**国产互联网核心技术**：第三代 Web，助力我国建成网络强国，防护我国关键信息基础设施，筑牢我国数字经济发展的坚固底座。

无数的数据泄露和网络犯罪事实告诉我们：没有互联网安全就没有数据安全，使用美国落后的二代 Web 就没有中国互联网的安全！

全球首个影子网站：<https://www.bj3gweb.com> 欢迎体验、渗透测试和指导；

欢迎：指导、询问、技术交流、合作！

业务：13911821399

技术：19833166729

東方博盾(北京)科技有限公司

专注 AI+ 网络战时代的互联网核心技术

<https://www.bj3gweb.com>

2024.1.25. 北京

影子防御 3Gweb-Shadow  
高可信 & 抗攻击