

# 奇安信「X 实验室」

Global Cybersecurity Threat Analysis and Hunt



Botnet

**CatDDoS-Related Gangs Have Seen a Recent Surge in Activity**

Overview XLab's CTIA(Cyber Threat Insight Analysis) System continuously tracks and monitors the active mainstream DDoS botnets. Recently, our system has observed that CatDDoS-related gang...

2024年5月22日 · 8 min read



Botnet

## CatDDoS系团伙近期活动激增分析

概述 XLab大网威胁感知系统会对当前活跃的主流DDoS僵尸网络家族进行持续跟踪和监控，最近3个月，这套系统观察到CatDDoS系团伙持续活跃，利用的漏洞数量达80+，攻击目标数量最大峰值...

2024年5月22日 · 10 min read



Backdoor

## Playing Possum: What's the Wpeeper Backdoor Up To?

Summary On April 18, 2024, XLab's threat hunting system detected an ELF file with zero detections on VirusTotal being distributed through two different domains. One of the domains was marked as...

2024年4月29日 · 11 min read



Backdoor

## 假死疑云：Wpeeper木马所图为何？

简介 2024年4月18日，XLab的未知威胁狩猎系统发现一个VT 0检测的ELF文件正通过2个不同的域名传播，其中一个域名已被3家安全产商标注为恶意，另一个域名为近期注册且无任何检测，这个异常...

2024年4月29日 · 15 min read

Botnet

## Mirai Nomi: A Botnet Leveraging DGA

Overview The Mirai family, as the evergreen tree of botnet, exists numerous variants, but rarely appear Mirai variants using DGA(Domain Generation Algorithm), according to our observation, the last Mirai variant using DGA appeared in 2016. in March 2024, we captured new suspicious ELF...

2024年3月18日 · 6 min read

Botnet

## 使用DGA的僵尸网络Mirai Nomi

概述 Mirai家族作为botnet的常青树，存在众多变种，但极少出现使用DGA的Mirai变种，据我们观测，上一个使用DGA (Domain Generation Algorithm) 的Mirai变种出现于2016年。2024年3月，我们捕获到了新的可疑ELF样本，通过分析得知是另一个使用DGA的Mirai变种，分析关联的历史样本，我们不...

2024年3月18日 · 7 min read



DDoS

## Smargaft Harnesses EtherHiding for Stealthy C2 Hosting

Background At XLab, we see a lot of botnets every day, mainly tweaks of old Mirai and Gafgyt codes. These are pretty common and usually don't grab our attention. But today, we found...

2024年2月2日 · 16 min read



DDoS

## 币安智能合约正在被Smargaft僵尸网络滥用

背景 在XLab的日常工作中，我们的僵尸网络监控系统每天都能检测到大量基于Mirai, Gafgyt代码魔改而来的变体的僵尸网络。这些变体已经司空见惯，无法引起我们的兴趣。然而，今天的主角是一个异...

2024年2月2日 · 22 min read



DNS

## Deep Dive into NXDOMAIN Data in China

The Domain Name System (DNS) is an essential protocol in the architecture of today's Internet. It routinely translates domain names into IP addresses and also often handles a multitude of invalid...

2024年1月29日 · 32 min read



DNS

## 中国全网DNS错误数据分析

在电影《流浪地球2》中，重启全球互联网的情节让观众印象深刻，影片中重启根服务器象征着全球 DNS (Domain Name System) 解析服务的重新启动。在现实世界中，DNS不仅承担着将域名转换为...

2024年1月29日 · 43 min read



Botnet

## Bigpanzi Exposed: The Hidden Cyber Threat Behind Your Set-Top Box

Background Some time ago, we intercepted a dubious ELF sample exhibiting zero detection on VirusTotal. This sample, named pandoraspear and employing a modified UPX shell, has an MD5...

2024年1月15日 · 33 min read



Botnet

## 笼罩在机顶盒上空的阴影：揭开隐蔽8年黑灰产团伙Bigpanzi的神秘面纱

背景 一段时间之前，我们捕获了一个VT 0 检测，使用变形UPX加壳，名为pandoraspear，MD5为9a1a6d484297a4e5d6249253f216ed69的可疑ELF样本。在分析过程中，我们发现它硬编码了9个...

2024年1月15日 · 40 min read

Botnet

## Rimasuta New Variant Switches to ChaCha20 Encryption Algorithm

In June 2021, 360netlab discovered a completely new variant of the Mirai malware. It was named Mirai\_ptea based on the use of the TEA algorithm. However, the author of the malware expressed dissatisfaction in subsequent samples after the variant was publicly disclosed to the community: ...

2024年1月10日 · 12 min read

Botnet

## Rimasuta新变种出现，改用ChaCha20加密

时间回到两年前，2021年6月360netlab捕获到一个全新的mirai变种，根据使用的TEA算法给它取名为mirai\_ptea，没想到在向社区公布了该变种之后，作者在随后更新的样本里吐槽了360netlab的命名：“-\_- you guys didnt pick up on the name? really??? its RI-MA-SU-TA. not MIRAI\_PTEA this is dum...”

2024年1月10日 · 13 min read

# Mirai.TBOT Uncovered: Over 100 Groups and 30,000+ Infected Hosts in a big IoT Botnet

Overview As we all know Mirai was first discovered in 2016 and it infects IoT devices by exploiting their weak passwords and vulnerabilities. Once the devices are infected, they become part of a botnet controlled by attackers for large-scale distributed denial-of-service attacks. Mirai botnets...

2024年1月3日 · 13 min read

## 一个新的超大规模分组的Mirai变种僵尸网络TBOT

概述 众所周知Mirai于2016年首次被发现，它通过利用物联网设备的弱密码和漏洞来感染它们。一旦设备感染，它们将成为网络的一部分，由攻击者控制，用于大规模的分布式拒绝服务攻击。Mirai僵尸网络通常根据感染方式或者被感染设备不同将Bot分为不同的组，以便攻击者更有效地管理和控制庞大...

2024年1月2日 · 16 min read