X实验室

X实验室（XLab）是奇安信公司 致力于大网安全研究、威胁分析溯源和大规模多维度安全数据平台建设的团队。我们是2023年在奇安信成立的一个崭新的团队，同时也是一个积累深厚的团队，团队核心成员普遍在该领域深耕近 10年，是国内最早利用大规模数据进行安全研究、安全应用和威胁情报生产的团队， 我们建立了国内首个 PassiveDNS系统，以及多个业内领先的 Netflow、Whois、证书、IP 和恶意样本等基础数据系统。

在大网安全研究和威胁分析溯源方面，我们建设了业内领先的大规模多维度网络数据关联分析系统、僵尸网络发现和跟踪系统、全网高级蜜罐系统和知识图谱系统。特别是在大规模僵尸网络监控方面，我们披露了30多个具有全球影响力的僵尸网络，如Mirai、Bigpanzi等，发现了近年来几乎所有具有影响力的僵尸网络。

除了前沿技术研究，我们同时在积极探索商业化，努力将我们的研究成果应用到大网安全态势、威胁溯源分析、威胁情报等业务领域。

About XLab

XLab was founded within QAX which is one of the largest cybersecurity company in China. Dedicated to cyber security research, threat analysis and building large-scale multidimensional security data platforms. We are a brand new team, established within Qi'anxin in 2023. At the same time, we are also a team with substantial accumulated experience. Our core team members generally have around 10 years of experience in this field. We were one of the first teams in China to leverage big data for security research, security applications and threat

intelligence production. We built the first and largest PassiveDNS system in China, as well as several industry-leading Netflow, Whois, certificate, IP and malware sample foundational data systems.

In the areas of cyber security research and threat analysis, we built industry-leading large-scale multidimensional network data correlation analysis systems, botnet tracking systems, global network advanced honeypot systems and knowledge graph systems. We are especially renowned for our work in monitoring massive botnets and have exposed over 30 globally impactful botnets, such as Mirai and Bigpanzi. We have discovered almost every major botnet in recent years.

In addition to cutting-edge technology research, we are also actively exploring commercialization, striving to apply our research outcomes to business areas like cyber security situational awareness, threat attribution analysis, and threat intelligence.