



ISC 互联网安全大会



360 互联网安全中心



安全攻防的明天

于旻 腾讯安全玄武实验室

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
(原中国互联网安全大会)

自动化技术加持的攻击和防御

大数据加持的攻击和防御

区块链加持的攻击和防御

全面数字化过程中的攻击和防御

自动化技术加持的攻击和防御

对漏洞研究的影响：从辅助工具到生产力工具

对网络攻击的影响：从网络蠕虫到网络蝗虫

对网络防御的影响：基于规则和行为的技术在AI之下融合

大数据加持的攻击和防御

数据安全性，和防御方能力成正比，和攻击方能力成反比，
和数据存在时间成反比

大多数网站，在一段比较长的时间中，5 年或者 10 年，
都会至少一次被入侵并造成用户信息泄露

防御方的努力可以推迟这一天的到来，但无法绝对阻止

大数据加持的攻击和防御

我们可能是地球上最后一代曾有过隐私的人

未来在设计产品和业务的时候，需要假设用户此前的一切
基本信息已经掌握在网络犯罪者手上

区块链加持的攻击和防御

Code is law => God is flaw

大多数情况下，我们可以接受代码存在漏洞

而要将绝对裁判权交给代码，则需要保证代码绝对安全

区块链加持的攻击和防御

区块链技术扩大了网络安全的外延

性能优化也会成为漏洞：CVE-2017-9230 ASICBoost

仅能导致程序崩溃或者网络阻塞的漏洞，在区块链场景下
则可能直接用于获利：51%攻击”、“愈合攻击”

区块链加持的攻击和防御

任何匿名技术总会有利于攻击方

数字币让网络犯罪省去了最困难的洗钱这一步

如果木马用公链进行 C&C 通信，怎么拦截？怎么追踪？

全面数字化过程中的攻击和防御

数字化过程引入的风险远超过我们今天看到和想到的，远超过现在看到的数据泄露、动作控制等风险

更细微、更隐蔽、源自不当设计、难以解决的问题将逐渐暴露

零星出现的 TCP/IP 之外的“网络”安全问题将会长期困扰我们



ISC 互联网安全大会



360 互联网安全中心

谢谢!

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
(原中国互联网安全大会)