蓝队视角下的防御体系突破

奇安信安服团队

奇安信行业安全研究中心

2020.12

前　言

网络实战攻防演习，是新形势下关键信息系统网络安全保护工作的重要组成部分。演习通常是以实际运行的信息系统为保护目标，通过有监督的攻防对抗，尽可能地模拟真实的网络攻击，以此来检验信息系统的实际安全性和运维保障的实际有效性。

2016 年以来，在国家监管机构的有力推动下，网络实战攻防演习日益得到重视，演习范围越来越广，演习周期越来越长，演习规模越来越大。国家有关部门组织的全国性网络实战攻防演习从 2016 年仅有几家参演单位，到 2020 年已扩展到上百家参演单位；同时各省、各市、各行业的监管机构，也都在积极地筹备和组织各自管辖范围内的实战演习。一时间，网络实战攻防演习遍地开花。

在演习规模不断扩大的同时，攻防双方的技术水平和对抗能力也在博弈中不断升级。

2016 年，网络实战攻防演习尚处于起步阶段，攻防重点大多集中于互联网入口或内网边界。

2017 年，实战攻防演习开始与重大活动的网络安全保障工作紧密结合。就演习成果来看，从互联网侧发起的直接攻击仍然普遍十分有效；而系统的外层防护一旦被突破，横向移动、跨域攻击，往往都比较容易实现。

2018 年，网络实战攻防演习开始向行业和地方深入。伴随着演习经验的不断丰富和大数据安全技术的广泛应用，防守方对攻击行为的监测、发现和溯源能力大幅增强，与之相应的，攻击队开始更多地转向精准攻击和供应链攻击等新型作战策略。

2019 年以来．网络实战攻防演习工作受到了监管部门、政企

机构和安全企业的空前重视。流量分析、EDR、蜜罐、白名单等专业监测与防护技术被防守队广泛采用。攻击难度的加大也迫使攻击队全面升级，诸如 0Day 漏洞攻击、1Day 漏洞攻击、团队社工、身份仿冒、钓鱼 WiFi、鱼叉邮件、水坑攻击等高级攻击手法，在实战攻防演练中均已不再罕见，攻防演习与网络实战的水平更加接近。

如何更好地参与网络实战攻防演习？如何更好地借助实战攻防演习提升自身的安防能力？这已经成为大型政企机构运营者所关心的重要问题。

作为国内前沿的网络安全企业，奇安信集团已成为全国各类网络实战攻防演习的主力军。奇安信集团安服团队结合 220 余次实战攻防演习经验，总结编撰了这套实战攻防演习系列丛书，分别从红队视角、蓝队视角和紫队视角，来解读网络实战攻防演习的要领，以及如何结合演习提升政企机构的安防能力。

需要说明的是，实战攻防演习中的红方与蓝方对抗实际上是沿用了军事演习的概念和方法，一般来说，红蓝双方分别代表攻击方与防守方。不过，红方和蓝方的名词定义尚无严格的规定，在实际的攻防演习中，有将红队作为攻击队的、也有将蓝队作为攻击队的。在本系列丛书中，我们依据国内最新的相关工作实践要求，统一将攻击队命名为蓝队，将防守队命名为红队，而紫队则代表组织演习的机构。

《蓝队视角下的防御体系突破》是本系列丛书的第一册。本册希望通过归纳总结蓝队常用的攻击策略和攻击战术，帮助政企机构理解攻方思维，以便提升演习水平，构筑更有效的安全防御体系。正所谓“知己知彼，百战不殆”。

《红队视角下的防御体系构建》是本系列丛书的第二册。本

册希望通过归纳总结红队防御的四个阶段、应对攻击的常用策略，以及建立实战化的安全体系的基本方法，帮助政企机构查找薄弱环节，更好地提升演习水平，构筑更有效的安全防御体系。

《紫队视角下的实战攻防演习组织》是本系列丛书的第三册。本册重点介绍实战环境下的紫队工作，提出如何组织一场有效的实战攻防演习、如何组织演习过程中的应急演练、如何组织对无法开展实战演习的关基设施的沙盘推演。

目　　录

第一章　什么是蓝队 1

第二章　蓝队演变趋势 3

第三章　蓝队四板斧——攻击的四个阶段 5

一、　第一阶段：准备收集 5

二、　第二阶段：情报收集 6

三、　第三阶段：建立据点 6

四、　第四阶段：横向移动 7

第四章　蓝队也套路——常用的攻击战术 9

一、　利用弱口令获得权限 9

二、　利用互联网边界渗透内网 10

三、　利用通用产品组件漏洞 10

四、　利用安全产品 ODAY 漏洞 11

五、　利用人心弱点社工钓鱼 11

六、　利用供应链隐蔽攻击 12

七、　利用下属单位迂回攻击 12

八、　秘密渗透 13

九、　多点潜伏 14

第五章　蓝队三十六计——经典攻击实例..... 15

一、　正面突破——跨网段控制工控设备..... 15

二、　百折不饶——社工钓鱼突破边界 16

三、　迂回曲折——供应链定点攻击 18

四、　浑水摸鱼——社工钓鱼突破系统 20

五、　声东击西——混淆流量躲避侦察 22

六、　李代桃僵——旁路攻击搞定目标 23

七、　顺手牵羊——巧妙种马实施控制 25

八、　暗渡陈仓——迂回渗透取得突破 26

第六章　蓝队眼中的防守弱点..... 28

一、　资产混乱、隔离策略不严格 28

二、　通用中间件未修复漏洞较多 28

三、　边界设备成为进入内网的缺口 28

四、　内网管理设备成扩大战果突破点 29

五、　安全设备自身安全成为新的风险点..... 29

附录 奇安信蓝队能力及攻防实践..... 30

奇安信
新一代网络安全领军者

蓝队视角下的防御体系突破

奇安信安服团队

奇安信行业安全研究中心

2020.12

第一章 什么是蓝队

蓝队，一般是指网络实战攻防演习中的攻击一方。

蓝队一般会采用针对目标单位的从业人员，以及目标系统所在网络内的软件、硬件设备同时执行多角度、全方位、对抗性的混合式模拟攻击手段；通过技术手段实现系统提权、控制业务、获取数据等渗透目标，来发现系统、技术、人员、管理和基础架构等方面存在的网络安全隐患或薄弱环节。

蓝队人员并不是一般意义上的电脑黑客。因为黑客往往以攻破系统，获取利益为目标；而蓝队则是以发现系统薄弱环节，提升系统安全性为目标。此外，对于一般的黑客来说，只要发现某一种攻击方法可以有效地达成目标，通常就没有必要再去尝试其他的攻击方法和途径；但蓝队的目标则是要尽可能地找出系统中存在的所有安全问题，因此往往会穷尽已知的“所有”方法来完成攻击。换句话说，蓝队人员需要的是全面的攻防能力，而不仅仅是一两招很牛的黑客技术。

蓝队的工作也与业界熟知的渗透测试有所区别。渗透测试通常是按照规范技术流程对目标系统进行的安全性测试；而蓝队攻击一般只限定攻击范围和攻击时段，对具体的攻击方法则没有太多限制。渗透测试过程一般只要验证漏洞的存在即可，而蓝队攻击则要求实际获取系统权限或系统数据。此外，渗透测试一般都会明确要求禁止使用社工手段（通过对人的诱导、欺骗等方法完成攻击），而蓝队则可以在一定范围内使用社工手段。

还有一点必须说明：虽然实战攻防演习过程中通常不会严格限定蓝队的攻击手法，但所有技术的使用，目标的达成，也必须严格遵守国家相关的法律和法规。

在演习实践中，蓝队通常会以 3 人为一个战斗小组，1 人为组长。组长通常是蓝队中综合能力最强的人，需要较强的组织意识、应变能力和丰富的实战经验。而 2 名组员则往往需要各有所长，具备边界突破、横向移动（利用一台受控设备攻击其他相邻设备）、情报收集或武器研制等某一方面或几个方面的专长。

蓝队工作对其成员的能力要求往往是综合性的、全面性的。蓝队成员不仅要会熟练使用各种黑客工具、分析工具，还要熟知目标系统及其安全配置，并具备一定的代码开发能力，以便应对特殊问题。

第二章 蓝队演变趋势

“魔高一尺道高一丈”！防守能力提升的同时，攻击能力也在与时俱进。目前，蓝队的工作已经变得非常体系化、职业化和工具化，主要变现如下。

1） 体系化

从漏洞准备、工具准备，到情报收集、内网渗透等，每个人都有明确的分工，有组织地形成团队作战能力，已经很少有一个人干全套的情况了。

2） 职业化

蓝队人员都来自各组织专职实战演习团队，有明确分工和职责，具备协同配合的职业操守，平时开展专业化训练。

3） 工具化

工具化程序持续提升，除了使用常用渗透工具，基于开源代码的定制化工具应用增多，自动化攻击被大规模应用，如采用多IP出口的自动化攻击平台进行作业。

从实战对抗的手法来看，现如今的蓝队还呈现出社工化、强对抗和迂回攻击的特点。

1） 社工化

利用“人”的弱点实施社会工程学攻击，是黑产团伙和高级威胁组织的常用手段，如今也被大量引入实战攻防演习当中。

除了钓鱼、水坑等传统社工攻击手段外，如今的蓝队还会经常通过在线客服、私信好友等多种交互平台进行社工攻击，以便更加高效地获取业务信息。社工手段的多变性往往会让防守方防

不胜防。

2） 强对抗

利用 0Day 漏洞、NDay 漏洞、免杀技术等方式与防守方进行高强度的技术对抗，也是近 1-2 年来蓝队在实战攻防演习中表现出的明显特点。特别的，蓝队人员大多出自安全机构，经过专业训练，因此往往会比民间黑客更加了解安全软件的防护机制和安全系统的运行原理，其使用的对抗技术也往往更具针对性。

3） 迂回攻击

对于防护严密，有效监控的目标系统来说，正面攻击往往难以奏效。这就迫使蓝队越来越多的采用“曲线救国”的攻击方式，将战线拉长：从目标系统的同级单位和下级单位入手，从供应链及业务合作方下手，在防护相对薄弱的关联机构中寻找突破点，通过迂回攻击的方式攻破目标系统。

第三章 蓝队四板斧——攻击的四个阶段

蓝队的攻击并非是天马行空的撞大运，而是一个有章可循、科学合理的作战过程。一般来说，蓝队的工作可分为四个阶段：站前准备、情报收集、建立据点和横向移动。我们也常将这个四个阶段称为蓝队工作的“四板斧”。

一、 第一阶段：准备收集

在一场实战攻防演习作战开始前，蓝队人员主要会从以下几个方面进行准备。

1） 漏洞挖掘

漏洞一直是第一攻击力。前期的漏洞挖掘对于打开突破口显得非常重要，在实战中，漏洞挖掘工作一般会聚焦于互联网边界应用、网络设备、办公应用、运维系统、移动办公、集权管控等方面。此外，只是找到漏洞还不够，好的漏洞利用方式也是十分重要的。想要在不通环境下达到稳定、深度的漏洞利用，这对漏洞挖掘人员来说是一个不小的挑战。

2） 工具储备

工具的目的是为了提升工作效率，好的工具往往能事半功倍，在实战中，蓝队通常需要准备信息收集、钓鱼、远控、WebShell管理、隧道、扫描器、漏洞利用等多种工具。

3） 战法策略

团队作战考虑的是配合，因此，攻击队成员的分工角色就显得尤为重要，小的战役靠个人，大的战役一定是靠机制、流程以及团队合作。好的战法策略，对于一场大的战役来讲至关重要。

4） 以赛代练

日常的任务中，需要挑选出一些具有代表性的任务来对蓝队进行有针对性的训练，有利于蓝队队员提高自身的技能。参加各类安全大赛将非常有助于蓝队队员的技术能力提升。

二、 第二阶段：情报收集

当蓝队专家接到目标任务后，并不会像渗透测试那样在简单收集数据后直接去尝试各种常见漏洞，而是先去做情报侦察和信息收集工作。收集的内容包括目标系统的组织架构、IT 资产、敏感信息泄露、供应商信息等各个方面。

组织架构包括单位部门划分、人员信息、工作职能、下属单位等；IT 资产包括域名、IP 地址、C 段、开放端口、运行服务、Web 中间件、Web 应用、移动应用、网络架构等；敏感信息泄露包括代码泄露、文档信息泄露、邮箱信息泄露、历史漏洞泄露信息等方面；供应商信息包括相关合同、系统、软件、硬件、代码、服务、人员等相关信息。

掌握了目标企业相关人员信息和组织架构，可以快速定位关键人物以便实施鱼叉攻击，或确定内网横纵向渗透路径；而收集了 IT 资产信息，可以为漏洞发现和利用提供数据支撑；掌握企业与供应商合作相关信息，可为有针对性开展供应链攻击提供素材。而究竟是要社工钓鱼，还是直接利用漏洞攻击，抑或是从供应链下手，一般取决于安全防护的薄弱环节究竟在哪里，以及蓝队对攻击路径的选择。

三、 第三阶段：建立据点

在找到薄弱环节后，蓝队专家会尝试利用漏洞或社工等方法去获取外网系统控制权限，一般称之为“打点”或撕口子。在这个过程中，蓝队专家会尝试绕过 WAF、IPS、杀毒软件等防护设备或软件，用最少的流量、最小的动作去实现漏洞利用。

通过撕开的口子，寻找和内网联通的通道，再进一步进行深入渗透，这个由外到内的过程一般称之为纵向渗透。如果没有找到内外联通的 DMZ 区（Demilitarized Zone，隔离区），蓝队专家会继续撕口子，直到找到接入内网的点为止。

当蓝队专家找到合适的口子后，便可以把这个点作为从外网进入内网的根据地。通过 frp、ewsocks、reGeorg 等工具在这个点上建立隧道，形成从外网到内网的跳板，将它作为实施内网渗透的坚实据点。

若权限不足以建立跳板，蓝队专家通常会利用系统、程序或服务漏洞进行提权操作，以获得更高权限；若据点是非稳定的 PC 机，则会进行持久化操作，保证 PC 机重启后，据点依然可以在线。

四、 第四阶段：横向移动

进入内网后，蓝队专家一般会在本机以及内部网络开展进一步信息收集和情报刺探工作。包括收集当前计算机的网络连接、进程列表、命令执行历史记录、数据库信息、当前用户信息、管理员登录信息、总结密码规律、补丁更新频率等信息；同时对内网的其他计算机或服务器的 IP、主机名、开放端口、开放服务、开放应用等情况进行情报刺探。再利用内网计算机、服务器不及时修复漏洞、不做安全防护、同口令等弱点来进行横向渗透扩大战果。

对于含有域的内网，蓝队专家会在扩大战果的同时去寻找域管理员登录的蛛丝马迹。一旦发现某台服务器有域管理员登录，就可以利用 Mimikatz 等工具去尝试获得登录账号密码明文，或者用 Hashdump 工具去导出 NTLM 哈希，继而实现对域控服务器的渗透控制。

在内网漫游过程中，蓝队专家会重点关注邮件服务器权限、OA 系统权限、版本控制服务器权限、集中运维管理平台权限、统一认证系统权限、域控权限等位置，尝试突破核心系统权限、控制核心业务、获取核心数据，最终完成目标突破工作。

第四章 蓝队也套路——常用的攻击战术

在蓝队的实战过程中，蓝队专家们逐渐摸出了一些套路、总结了一些经验：有后台或登录入口的，会尽量尝试通过弱口令等方式进入系统；找不到系统漏洞时，会尝试社工钓鱼，从人开展突破；有安全防护设备的，会尽量少用或不用扫描器，使用 EXP 力求一击即中；针对防守严密的系统，会尝试从子公司或供应链来开展工作；建立据点过程中，会用多种手段多点潜伏，防患于未然。

下面介绍九种蓝队最常用的攻击战术。

一、 利用弱口令获得权限

弱密码、默认密码、通用密码和已泄露密码通常是蓝队专家们关注的重点。实际工作中，通过弱口令获得权限的情况占据 90%以上。

很多企业员工用类似 zhangsan、zhangsan001、zhangsan123、zhangsan888 这种账号拼音或其简单变形，或者 123456、888888、生日、身份证后 6 位、手机号后 6 位等做密码。导致通过信息收集后，生成简单的密码字典进行枚举即可攻陷邮箱、OA 等账号。

还有很多员工喜欢在多个不同网站上设置同一套密码，其密码早已经被泄露并录入到了黑产交易的社工库中；或者针对未启用 SSO 验证的内网业务系统，均习惯使用同一套账户密码。这导致从某一途径获取了其账户密码后，通过凭证复用的方式可以轻而易举地登录到此员工所使用的其他业务系统中，为打开新的攻击面提供了便捷。

很多通用系统在安装后会设置默认管理密码，然而有些管理员从来没有修改过密码，如 admin/admin、test/123456、

admin/admin888 等密码广泛存在于内外网系统后台，一旦进入后台系统，便有很大可能性获得服务器控制权限；同样，有很多管理员为了管理方便，用同一套密码管理不同服务器。当一台服务器被攻陷并窃取到密码后，进而可以扩展至多台服务器甚至造成域控制器沦陷的风险。

二、 利用互联网边界渗透内网

大部分企业都会有开放于互联网边界的设备或系统，如：VPN 系统、虚拟化桌面系统、邮件服务系统、官方网站等。正是由于这些设备或系统可以从互联网一侧直接访问，因此也往往会成为蓝队首先尝试的，突破边界的切入点。

此类设备或系统通常都会访问内网的重要业务，为了避免影响到员工使用，很多企业都没有在其传输通道上增加更多的防护手段；再加上此类系统多会集成统一登录，一旦获得了某个员工的账号密码，就可以通过这些系统突破边界直接进入内网中来。

譬如，开放在内网边界的邮件服务如果缺乏审计，也未采用多因子认证；员工平时又经常通过邮件传送大量内网的敏感信息。如服务器账户密码、重点人员通讯录等。那么，当掌握相关员工的邮箱账号密码后，在邮件中所获得的信息，会被蓝队下一步工作提供很多方便。

三、 利用通用产品组件漏洞

信息化的应用提高了工作效率，但其存在的安全漏洞也是蓝队人员喜欢的。历年实战攻防演习中，经常被利用的通用产品漏洞包括：邮件系统漏洞、OA 系统漏洞、中间件软件漏洞、数据库漏洞等。这些漏洞被利用后，可以使攻击方快速获取大量账户权限，进而控制目标系统。而作为防守方，漏洞往往很难被发现，相关活动常常被当作正常业务访问而被忽略。

四、 利用安全产品 0Day 漏洞

安全产品自身也无法避免 0Day 攻击！安全产品也是一行行代码构成，也是包含了操作系统、数据库、各类组件等组合而成的产品。历年攻防实战演习中，被发现和利用的各类安全产品的 0Day 漏洞，主要涉及安全网关、身份与访问管理、安全管理、终端安全等类型安全产品。这些安全产品的漏洞一旦被利用，可以使攻击者突破网络边界，获取控制权限进入网络；获取用户账户信息，并快速拿下相关设备和网络的控制权限。

安全产品的 0Day 漏洞常常是蓝队最好的攻击利器。

五、 利用人心弱点社工钓鱼

利用人的安全意识不足或安全能力不足，实施社会工程学攻击，通过钓鱼邮件或社交平台进行诱骗，是蓝队专家经常使用的社工手段。在很多情况下，“搞人”要比“搞系统”容易得多。

钓鱼邮件是最经常被使用的攻击手段之一。蓝队专家常常会首先通过社工钓鱼或漏洞利用等手段盗取某些安全意识不足的员工邮箱账号；再通过盗取的邮箱，向该单位的其他员工或系统管理员发送钓鱼邮件，骗取账号密码或投放木马程序。由于钓鱼邮件来自内部邮箱，“可信度”极高，所以，即便是安全意识较强的 IT 人员或管理员，也很容易被诱骗点开邮件中的钓鱼链接或木马附件，进而导致关键终端被控，甚至整个网络沦陷。

冒充客户进行虚假投诉，也是一种常用的社工手法，攻击方会通过单人或多人配合的方式，通过在线客服平台、社交软件平台等，向客户人员进行虚假的问题反馈或投诉，设局诱使或迫使客服人员接受经过精心设计的带毒文件或带毒压缩包。一旦客户人员的心理防线被突破，打开了带毒文件或压缩包，客服人员的电脑就会成为攻击队打入内网的一个“立足点”。

除了客服人员外，很多非技术类岗位的工作人员也很容易成为社工攻击的“外围目标”。例如，如给法务人员发律师函，给人力资源人员发简历，给销售人员发送采购需求等，都是比较常用的社工方法。而且往往“百试百灵”。

六、 利用供应链隐蔽攻击

供应链攻击是迂回攻击的典型方式。攻击方会从 IT（设备及软件）服务商、安全服务商、办公及生产服务商等供应链入手，寻找软件、设备及系统漏洞，发现人员及管理薄弱点并实施攻击。常见的系统突破口包括：邮件系统、OA 系统、安全设备、社交软件等；常见的突破方式包括软件漏洞，管理员弱口令等。

利用供应链攻击，可以实现第三方软件系统的恶意更新，第三方服务后台的秘密操控，以及物理边界的防御突破（如，受控的供应商驻场人员设备被接入内网）等多种复杂的攻击目标。

七、 利用下属单位迂回攻击

在有红队防守的实战攻防演习中，有时总部的系统防守会较为严密，蓝队很难正面突破，很难直接撬开进入内网的大门。此时，尝试绕过正面防御，通过攻击防守相对薄弱的下属单位，再迂回攻入总部的目标系统，就是一种很“明智”的策略。

蓝队大量实战中发现：绝大部分企业机构，其下属单位之间的内部网络，下属单位与集团总部之间的内部网络，均未进行有效隔离。很多部委单位、大型央企均习惯于使用单独架设一条专用网络，来打通各地区之间的内网连接，但同时又普遍忽视了不通区域网络之间必要的隔离管控措施，缺乏足够有效的网络访问控制。

这就导致蓝队一旦突破了子公司或分公司的防线，便可以通

过内网横向渗透，直接攻击到集团总部，或是漫游整个企业内网，进而攻击任意系统。

例如 A 子公司位于深圳，B 子公司位于广州，而总部位于北京。当 A 子公司或 B 子公司被突破后，就可以毫无阻拦地进入到总部网络中来。事实上，A 子公司与 B 子公司可能仅需要访问北京总部的部分业务系统；同时，A 与 B 则可能完全不需要有任何业务上的往来。那么，从安全角度看，就应该严格限制 A 与 B 之间的网络访问。但实际情况常常是：一条专线内网通往全国各地，一处沦陷，处处沦陷。

八、 秘密渗透

不同于民间黑客或黑产团队，蓝队工作一般不会大规模使用漏洞扫描器，因为扫描器活动特征明显，很容易暴露自己。例如，目前主流的 WAF、IPS 等防护设备都有识别漏洞扫描器的能力，一旦发现后，可能第一时间触发报警或阻断 IP。

因此，信息收集和情报刺探是蓝队工作的基础。在数据积累的基础上，针对性地根据特定系统、特定平台、特定应用、特定版本，去寻找与之对应的漏洞，编写可以绕过防护设备的 EXP 来实施攻击操作，可以达到隐蔽攻一击即中的目的。

如果目标系统的防御纵深不够，或使用安全设备的能力不足，当面对这种有针对性攻击时，往往就很难及时发现和阻止攻击行为。在攻防演习的实战中，常常使用蓝队获取到目标资料或数据后，被攻击单位尚未感知到入侵行为。

如果参与演习的安全人员本身的技术能力也比较薄弱，无法实现对攻击行为的发现、识别，无法给出有效的攻击阻断、漏洞溯源及系统修复策略，则在攻击发生的很长一段时间内，防守一方可能都不会对蓝队的隐蔽攻击采取有效的应对措施。

九、 多点潜伏

蓝队专家在工作中，通常不会仅仅站在一个据点上去去开展渗透工作，而是会采取不同的 Webshell，使用不同的后门程序，利用不同的协议来建立不同特征的据点。

事实上，大部分应急响应过程并没有溯源攻击源头，也未必能分析完整攻击路径。在防护设备告警时，很多防守方队员会仅仅只处理告警设备中对应告警 IP 的服务器，而忽略了对攻击链的梳理，从而导致尽管处理了告警，但仍未能将蓝队排除在内网之外。而蓝队则可以通过多个潜伏据点，实现快速“死灰复燃”。

如果某些防守方成员专业程度不高，安全意识不足，还有可能在蓝队的“伏击”之下暴露更多敏感信息。例如，在针对 Windows 服务器应急运维的过程中，有防守方队员会直接将自己的磁盘通过远程桌面共享挂载到被告警的服务器上。这样反而可以给秘密潜伏的蓝队进一步攻击防守方成员的机会。

第五章　蓝队三十六计——经典攻击实例

古人带兵打仗讲三十六计。而蓝队实战亦是一个攻防对抗的过程，同样是人与人之间的较量，需要出谋划策、斗智斗勇。在这个过程中，有着“勾心斗角”、“尔虞我诈”，也有着勇往直前、正面硬刚。为此，我们精选了几个小案例，以三十六计为题向大家更加具体的展现蓝队的常见攻击手法。

一、 正面突破——跨网段控制工控设备

某企业为国内某大型制造业企业，内部生产网大量使用双网卡技术实现网络隔离。在本次实战攻防演习活动中，攻击队的目标是：获取该企业工控设备控制权限。

经过前期的情报收集与分析，攻击队制定了首先突破办公网，再通过办公网渗透进入工控网的战略部署。

1）　突破办公网

攻击队首先选择该企业的门户网站作为突破口，并利用一个 0Day 漏洞获取了该门户网站应用与操作系统的管理员权限，从而获取到该企业办公内网的接入权限。

在横向移动过程中，攻击队又探测到该企业内网中的多个服务系统和多台服务器。使用已经获得门户网站管理员账号和密码进行撞库攻击，成功登录并控制了该企业内网中的绝大多数服务器。这表明，该企业内网中的大量系统服务器都使用了相同的管理账号和密码。

至此，攻击队突破办公网的第一阶段目标顺利完成，并取得了巨大的战果。接下来的目标就是找到工控网络的突破口。

2）　定位运维人员

对已经被攻破的服务器系统进行全面排查，攻击队发现，有多台服务器中存储了用 Excel 明文记录的密码本，密码本中包含所有系统用户的账户和密码。同时，服务器上还明文存储了大量机构内部敏感文件，包括企业 IT 部门的组织架构等信息。结合组织架构及密码本信息，攻击队成功定位到了一位工控系统的运维人员，并对其联网行为开展了长时间的监控。

3） 突破工控网

经过一段时间的监控，攻击队发现该运维人员自己的办公终端上有嵌套使用远程桌面的情况，即：首先通过远程桌面登录一台主机 A；继而，操作人又用主机 A 继续通过远程桌面，登录另一网段的主机 B。通过于密码本进行对比时，发现主机 A 和 B 都是该企业工控系统中的主机设备，但各自处于网络拓扑结构中不同的层次。其中，B 主机之下连有关键的工控设备。

进一步分析发现，主机 A 使用了双网卡，两个网卡分别对应不同网段，但是两个网卡之间没有采取任何隔离措施。同时，主机 B 也是一台双网卡主机，其上部署了隔离卡软件进行双网卡切换。

最终，攻击队发现了 B 主机上隔离卡软件的一个重大设计缺陷，并利用该缺陷成功绕过双网卡的隔离机制，成功拿到了工控设备的操作权限，可以随意停止、启动、复位相应的工控设备，某些操作可对设备的生产过程造成直接严重的伤害。

同时，攻击队的另一组人马继续摸排受控主机的用途和存储文件。功夫不负有心人，攻击队最终又发现一台“生产住操作室”的主机设备，其上存储有生产专用的文件，内容包括一些涉密文件，一旦被窃取，后果难以想象。

二、 百折不饶——社工钓鱼突破边界

某企业为某大型特种设备制造商，同时具有比较成熟的互联网服务经验。在本次实战攻防演习活动中，攻击队的目标是：获取该企业一个核心业务管控平台的控制权限。

攻击队在前期的情报收集工作中发现，该企业内部的网络防御体系比较健全，正面突破比较困难。经过头脑风暴，大家达成共识——要通过社工方法进行迂回入侵。

1） 寻找社工突破口

攻击队首先想到的社工方法也是最常见的邮件钓鱼。但考虑到该企业相对完善的网络防御体系，猜测其内网中很可能已经部署了邮件检测类的防御手段，简单的使用邮件钓鱼，很可能会被发现。

进一步的情报搜集发现：该企业使用了微信客服平台，而且微信客服平台可以进行实时聊天并发送文件。考虑到客服人员一般没有很强的技术功底，安全意识往往相对薄弱，攻击队最终商定：将社工对象确定为微信客服人员，并以投诉为话题尝试对客服进行钓鱼。

2） 冒充客服反馈问题

于是，一名攻击队队员开始冒充客户，在该企业的微信客服平台上进行留言投诉，并要求客服人员接收名为“证据视频录像”的压缩文件包。该压缩包实际上是攻击队精心伪装的，带有木马程序的文件包。让攻击队意想不到的是，该客户人员以安全为由，果断地拒绝接收不明来源的文件。显然，攻击队可能低估了该企业客服人员的安全意识素养。

3） 社工升级攻破心理防线

不过，攻击队并没有放弃，而是进一步采用多人协作的方式，

对当班客服人员进行了轮番轰炸，要求客服人员报上工号，并威胁将要对其客服质量进行投诉。经过 1 个小时的拉锯战，客服人员的心理防线最终被攻破，最终接受了带毒压缩包，并打开了木马文件。该客服人员的终端设备最终被控制。

以受控终端为据点，攻击队成功打入该企业的内网，后又利用一个未能及时修复的系统漏洞获取到关键设备控制权限，再结合内网的信息收集，最终成功获取到管控平台的权限。

三、 迂回曲折——供应链定点攻击

某超大型企业为一个国家级关键信息基础设施运营管理方，一旦发生安全事故，将直接危害国家安全及人民生命财产安全。在本次实战攻防演习活动中，攻击队的目标是：获取该企业内部系统的安全管控权限。

根据攻击队前期的情报收集摸排，该企业的办公网络及核心工业控制系统得到了非常严密的安全防护，对互联网暴露的业务系统较少，而且业务系统做了安全加固及多层防护，同时也拥有较强的日常网络安全运维保障能力。想要正面突破，非常困难。

前期情报分析还显示，该企业虽然规模大、人员多，但并不具备独立的 IT 系统研发和运维能力，其核心 IT 系统的建设和运维，实际上大多来自外部采购或外包服务。于是，攻击队根据这一特点，制定了从供应链入手的整体攻击策略。

1） 寻找目标供应商

攻击队首先通过检索“喜报”、“中标”、“签约”、“合作”、“验收”等关键字，在全网范围内，对该企业的供应商及商业合作伙伴进行地毯式摸排，最终选定将该企业的专用即时通信软件系统开发商 A 公司作为主要的攻击目标。

情报显示，A 公司为该企业开发的专用即时通信系统刚刚完成开发，推测该项目目前尚处于测试阶段，A 公司应该有交付和运维人员长期驻场为该企业提供运维全服务。如果能拿下驻场人员的终端设备，则可以成功进入该公司内网系统。

2） 盗取管理员账号

分析发现，A 公司开发的即时通信软件也在其公司内部进行使用。而该软件的网络服务管理后台，存在一个已知的系统安全漏洞。攻击队利用该漏洞获取了服务器的控制权，并通过访问服务器的数据库系统，获取了后台管理员的账号和密码。

3） 定位驻场人员

攻击队使用管理员的账号和密码登录服务器后，发现该系统的聊天记录在服务器上是准明文（低强度加密或转换）存储的，而且管理员可以不受限制的翻阅其公司内部的历史聊天记录。

攻击队对聊天记录进行关键字检索后发现：A 公司有三名员工的聊天记录中，多次出现目标企业名、OA、运维等字眼；并且这三名员工的登录 IP 经常落在目标企业的专属网段上。因此，攻击队判断，这三名员工就是 A 公司在目标企业的驻场人员。

4） 定向恶意升级包

攻击队最初的设想是，通过被控的即时通信软件服务器，向三名驻场人员定向发送恶意升级包。但这种攻击方法需要修改服务器系统配置，稍有不慎，就可能扩大攻击面，给演习工作造成不必要的损失，同时也有可能暴露自身攻击活动。

为实现对三名驻场人员更加隐蔽的定向攻击，攻击队对 A 公司的即使通信软件进行了更加深入的安全分析，发现其客户端软件对服务器的身份安全验证、对升级包的合法性校验机制都存在

设计缺陷。

于是，攻击队利用上述缺陷，通过中间人攻击，对服务器推送给三名驻场人员的客户端软件升级包进行了劫持和篡改。最终三名驻场人员都在完全没有任何感知情况下，在各自的 PC 机上安装了攻击队伪装设计的恶意升级包。

5） 横向移动

攻击队以驻场人员的运维机作为跳板机进入内网后，开始进行横向移动。

攻击队首先找到了该企业的一台域控服务器，并利用一个近期最新爆出的域控系统安全漏洞，获取了该主域的域账号密码哈希信息。但防守对很快地发现了此次攻击，并将该域控服务器进行了隔离。

不过，攻击队并没有放弃，又在内网中找到了一套终端安全管理系统。攻击队经过现场挖掘，找到了该系统的一个新的 0Day 漏洞，并利用该漏洞成功地获取了管理员权限。在成功登录系统后台后，攻击方可实现任意命令的下发和执行，能够控制该安全管理系统所辖范围内的所有终端设备。

四、 浑水摸鱼——社工钓鱼突破系统

社会工程学（简称社工）在蓝队工作中占据着半壁江山，而钓鱼攻击则是社工中的最常使用的套路。钓鱼攻击通常具备一定的隐蔽性和欺骗性，不具备网络技术能力的人通常无法分辨内容的真伪；而针对特定目标及群体精心构造的鱼叉钓鱼攻击则可令具备一定网络技术能力的人防不胜防，可谓之渗透利器。

小 D 团队便接到这样一个工作目标：某企业的财务系统。通过前期踩点和信息收集发现，目标企业外网开放系统非常少，也

没啥可利用的漏洞，很难通过打点的方式进入到内网。

不过还是让他们通过网上搜索以及一些开源社工库中收集到一批目标企业的工作人员邮箱列表。掌握这批邮箱列表后，小 D 便根据已泄露的密码规则、123456、888888 等常见弱口令、用户名密码相同，或用户名 123 这种弱口令等生成了一份弱口令字典。利用 hydra 等工具进行爆破，成功破解一名员工的邮箱密码。

小 D 对该名员工来往邮件分析发现，邮箱使用者为 IT 技术部员工。查看该邮箱发件箱，看到他历史发过的一封邮件如下：

标题：关于员工关掉 445 端口以及 3389 端口的操作过程

附件：操作流程.zip

小 D 决定浑水摸鱼，在此邮件的基础上进行改造伪装，构造钓鱼邮件如下。其中，zip 文件为带有木马的压缩文件。

标题：关于员工关掉 445 端口以及 3389 端口的操作补充

附件：操作流程补充.zip

为提高攻击成功率，通过对目标企业员工的分析，小 D 决定对财务部门以及几个跟财务相关的部门进行邮件群发。

小 D 发送了一批邮件，有好几个企业员工都被骗上线，打开了附件。控制了更多的主机，继而便控制了更多的邮箱。在钓鱼邮件的制作过程中，小 D 灵活根据目标的角色和特点来构造。譬如在查看邮件过程中，发现如下邮件：

尊敬的各位领导和同事，发现钓鱼邮件事件，内部定义为 19626 事件，请大家注意邮件附件后缀后.exe、.bat 等… …

小 D 同样采用浑水摸鱼的策略，利用以上邮件为母本，以假乱真构造以下邮件继续钓鱼：

尊敬的各位领导和同事，近期发现大量钓鱼邮件，以下为检

测程序… …

附件：检测程序.zip

通过不断地获取更多的邮箱权限、系统权限，根据目标角色针对性设计钓鱼邮件，小 D 最终成功拿下目标！

五、 声东击西——混淆流量躲避侦察

在有红队（防守方）参与的实战攻防工作中，尤其是有红队排名或通报机制的工作中，蓝队与红队通常会产生对抗。IP 封堵与绕过、WAF 拦截与绕过、Webshell 查杀与免杀，红蓝之间通常会开展一场没有硝烟的战争。

小 Y 和所带领的团队就遭遇了这么一次：刚刚创建的跳板几个小时内就被阻断了；刚刚上传的 Webshell 过不了几个小时就被查杀了。蓝队打到哪儿，红队就根据流量威胁审计跟到哪，不厌其烦，团队始终在目标的外围打转。

没有一个可以维持的据点，就没办法进一步开展内网突破。小 Y 和团队开展了一次头脑风暴，归纳分析了流量威胁审计的天然弱点，以及红队有可能出现的人员数量及技术能力不足等情况，制定了一套声东击西的攻击方案。

具体方法就是：同时寻找多个具有直接获取权限漏洞的系统，正面大流量进攻某个系统，吸引火力，侧面尽量减少流量直接拿权限并快速突破内网。

为此，小 Y 团队先通过信息搜集发现目标企业的某个外网 WEB 应用，并通过代码审计开展漏洞挖掘工作，成功发现多个严重的漏洞。另外发现该企业的一个营销网站，通过开展黑盒测试，发现存在文件上传漏洞。

小 Y 将团队兵分两路，除自己外的所有其他成员主攻营销网

站，准备了许多分属不同 A 段的跳板，不在乎是否被发现，也不在乎是否封堵，甚至连漏洞扫描器都上了，力求对流量威胁分析系统开启一场规模浩大的“分布式拒绝服务”，让红队的防守人员忙于分析和应对；而自己则悄无声息地用不同的 IP 和浏览器指纹特征对 WEB 应用网站开展渗透，力求用最少的流量拿下服务器，让威胁数据淹没在营销网站的攻击洪水当中。

通过这样的攻击方案，小 Y 团队同时拿下营销网站和 WEB 应用网站，但在营销网站的动作更多，包括关闭杀软、提权、安置后门程序、批量进行内网扫描等众多敏感操作；同时在 WEB 应用网站利用营销网站上获得的内网信息，直接建立据点，开展内网渗透操作。

很快营销网站就被蓝方下线了，红队开始根据流量开展分析、溯源和加固工作；而此时小 Y 已经在 WEB 应用网站上搭建了 frp socks 代理，内网横向渗透拿下多台服务器，使用了多种协议木马，备份多个通道稳固权限，以防被防守方发现或直接踢出局。接续的几天服务器权限再未丢失，继续后渗透拿下域管理员、域控制器，最终拿下目标权限，工控设备权限等核心目标系统。

在渗透收尾的后期，小 Y 团队通过目标企业安全信息中心的员工邮件看到，红队此时依旧在对营销网站产生的数据报警做分析和上报防守战果等工作，然而此时该企业的目标系统其实早已经被蓝队拿下了。

六、 李代桃僵——旁路攻击搞定目标

其实在蓝队工作过程当中，也碰到过很多奇葩的事情：譬如有红队将整个网站的首页替换成了一张截图；有的将所有数据传输接口全部关闭了，然后采用 excel 表格的方式实现数据导入；有的将内网目标系统的 IP 做了限定，仅允许某个管理员 IP 访问

等。

小 H 带领的蓝队就遇到类似的一次：目标企业把外网系统能关的都关了，甚至连邮件系统都做了策略，基本上没有办法实现打点和进入内网。

为此，小 H 团队通过充分信息收集后，决定采取“李代桃僵”的策略：既然母公司不让搞，那么就去搞子公司。然而工作过程中发现，子公司也做好了防护，而且基本上也关个遍。一不做，二不休，子公司不让搞，那么就搞子公司的子公司，搞它的孙公司。

于是，小 H 团队从孙公司下手，利用 sql 注入+命令执行漏洞成功进入(孙公司 A) DMZ 区。继续后渗透、内网横向移动控制了孙公司域控、DMZ 服务器。在(孙公司 A)稳固权限后，尝试搜集最终目标内网信息、子公司信息，未发现目标系统信息。但发现(孙公司 A)可以连通(子公司 B)。

小 H 决定利用(孙公司 A)内网对(子公司 B)展开攻击。利用 tomcat 弱口令+上传漏洞进入(子公司 B)内网域，利用该服务器导出的密码在内网中横向渗透，继而拿下(子公司 B)多台域服务器，并在杀毒服务器获取到域管理员账号密码，最终获取(子公司 B)域控制器权限。

在(子公司 B)内做信息收集发现：(目标系统 x) 托管在 (子公司 C)，(子公司 C) 单独负责运营维护，而(子公司 B)内有 7 名员工与 (目标系统 x) 存在业务往来，7 名员工大部分时间在 (子公司 C) 办公，但办公电脑资产属于(子公司 B)，加入(子公司 B)的域，且办公电脑经常带回(子公司 B)。

根据收集到的情报信息，小 H 团队以(子公司 B)内的 7 名员工作为入口点，在其接入(子公司 B)内网时，利用域权限在其电

脑种植木马后门。待其接入（子公司 C）内网时，继续通过员工计算机实施内网渗透，并获取（子公司 C）域控制权限。根据日志分析，锁定了（目标系统 x）管理员电脑，继而获取（目标系统 x）管理员登录账号，最终获取（目标系统 x）控制权限。

七、 顺手牵羊——巧妙种马实施控制

蓝队永远不会像渗透测试那样，根据一个工作流程或者漏洞测试手册，按照规范去做就能完成任务。蓝队的工作永远是具有随机性、挑战性、对抗性的。在工作过程中，总会有各种出其不意的情况出现，只有能够随机应变，充分利用出现的各种机遇，才能最终突破目标完成任务，小 P 这次做的目标就是如此。

小 P 团队通过挖掘目标企业 OA 系统的 0Day 漏洞，继而获得了 Webshell 权限。然而脚跟还没站稳，红队的管理员便发现了 OA 系统存在异常，对 OA 系统应用及数据库进行了服务器迁移，同时修复了漏洞。

本来是个很悲伤的事情，然而小 P 测试发现：红队虽然对 OA 系统进行了迁移并修复了漏洞，但是居然没有删除全部 Webshell 后门脚本。部分后门脚本仍然混杂在 OA 程序中，并被重新部署在新的服务器。攻击队依然可以连接之前植入的 Webshell，顺利提权，拿到了服务器权限。

拿到服务器权限后，小 P 团队发现红队的管理员居然连接到 OA 服务器进行管理操作，并将终端 PC 主机的磁盘全部挂载到 OA 服务器中。“既来之，则安之”，小 P 发现这是一个顺手牵羊的好机会。

小 P 团队小心翼翼地对管理员身份及远程终端磁盘文件进行确认，并向该管理员的终端磁盘写入了自启动后门程序。经过了一天的等待，红队管理员果然重启了终端主机，后门程序上线。

在获取到管理员的终端权限后，小 P 很快发现，该管理员为单位运维人员，主要负责内部网络部署、服务器运维管理等工作。该管理员使用 MyBase 工具对重要服务器信息进行加密存储，攻击队通过键盘记录器，获取了 MyBase 主密钥，继而对 MyBase 数据文件进行了解密，最终获取了包括 VPN、堡垒机、虚拟化管理平台等关键系统的账号及口令。

最终，小 P 团队利用获取到的账号口令登录到虚拟化平台中，定位到演习目标系统的虚拟主机，并顺利获取了管理员权限。至此，工作正式完成！

八、 暗渡陈仓——迂回渗透取得突破

在有明确重点目标的实战攻防演习中，通常红队都会严防死守、严阵以待，时时刻刻盯着从外网进来的所有流量，不管你攻还是不攻，他们始终坚守在那里。发现有可疑 IP 立即成段地封堵，一点机会都不留。此时，从正面硬刚显然不划算，蓝队一般会采取暗度陈仓的方式，绕过红队的防守线，从其他没有防守的地方去开展迂回攻击，小 M 这回遇到的就是这样一个硬骨头。

小 M 团队在确定攻击目标后，对目标企业的域名、ip 段、端口、业务等信息进行收集，并对可能存在漏洞目标进行尝试性攻击。结果发现大多数目标要么是都已关闭，要么是使用高强度的防护设备。在没有 0day 且时间有限情况下，小 M 决定放弃正面突破，采取暗度陈仓策略。

通过天眼查网站，小 M 了解到整个公司的子公司及附属业务分布情况，目标业务覆盖了香港、台湾、韩国、法国等地，其中香港包涵业务相对较多，极大可能有互相传送数据及办公协同的内网，故决定选择从香港作为切入点。

经过对香港业务进行一系列的踩点刺探，小 M 团队在目标企

业的香港酒店业务网站找到一个 SA 权限的注入点，成功登录后台并利用任意文件上传成功 getshell。通过数据库 SA 权限获取数据库服务器 system 权限，发现数据库服务器在域内且域管在登录状态。因服务器装有赛门铁克，因此采取添加证书的方式，成功绕过杀软并抓到域管密码，同时导出了域 hash 及域结构。

在导出的域结构中发现了国内域的机器，于是小 M 团队开始尝试从香港域向目标所在的国内域开展横向渗透。在国内域的 IP 段内找到一台服务器并 getshell，提权后抓取此服务器密码。利用抓取到的密码尝试登录其他服务器，成功登录到一台杀毒服务器，并在杀毒服务器上成功抓到国内域的域管密码。使用域管账号成功控制堡垒机、运维管理、vpn 等多个重要系统。

通过大量的信息收集，小 M 团队最终获得了渗透目标的 IP 地址，利用前期收集到的账号密码，成功登录目标系统，并利用任意文件上传漏洞拿到服务器权限。

至此，整个渗透工作结束。

第六章　蓝队眼中的防守弱点

奇安信通过对政府、央企、银行、证券、民生、运营商、互联网等行业的蓝队实战工作，发现各行业安全防护具备如下特点。

一、 资产混乱、隔离策略不严格

除了大型银行之外，很多行业对自身资产情况比较混乱，没有严格的访问控制（ACL）策略，且办公网和互联网之间大部分相通，可以直接使远程控制程序上线。

除了大型银行与互联网行业外，其他很多行业在 DMZ 区和办公网之间不做或很少做隔离，网络区域划分也不严格，给了蓝队很多可乘之机。

此外，几乎所有行业的下级单位和上级单位的业务网都可以互通。而除了大型银行之外，其他很多行业的办公网也大部分完全相通，缺少必要的分区隔离。所以，蓝队往往可以轻易地实现实施从子公司入侵母公司，从一个部门入侵其他部门的策略。

二、 通用中间件未修复漏洞较多

通过中间件来看，Weblogic、Websphere、Tomcat、Apache、Nginx、IIS 都有使用。Weblogic 应用比较广泛，因存在反序列化漏洞，所以常常会被作为打点和内网渗透的突破点。所有行业基本上都有对外开放的邮件系统，可以针对邮件系统漏洞，譬如跨站漏洞、XXE 漏洞等来针对性开展攻击，也可以通过钓鱼邮件和鱼叉邮件攻击来开展社工工作，均是比较好的突破点。

三、 边界设备成为进入内网的缺口

从边界设备来看，大部分行业都会搭建 VPN 设备，可以利用 VPN 设备的一些 SQL 注入、加账号、远程命令执行等漏洞开展攻

击，亦可以采取钓鱼、爆破、弱口令等方式来取得账号权限，最终绕过外网打点环节，直接接入内网实施横向渗透。

四、 内网管理设备成扩大战果突破点

从内网系统和防护设备来看，大部分行业都有堡垒机、自动化运维、虚拟化、邮件系统和域环境，虽然这些是安全防护的集中管理设备，但往往由于缺乏定期的维护升级，反而都可以作为开展权限扩大的突破点。

五、 安全设备自身安全成为新的风险点

“锁”出问题了给防守工作带来极大挑战。每年攻防演习都会爆出某某安全设备自身存在某某漏洞利用、被控制，反映出安全设备厂商自身安全开发和检测能力没有做到位，而作为用户又缺乏必要的安全检测流程及工作的开展，给蓝队人员留下了“后门”，最终形成新的风险点。

附录 奇安信蓝队能力及攻防实践

自 2016 年奇安信集团协助相关部委首次承办网络实战攻防演习以来，这种新的网络安全检验模式已经有了长足的发展。

仅 2020 年全年，奇安信就参与了全国范围内 244 多场实战攻防演习的蓝队活动，攻破了 1900 余个目标系统。累计派出蓝队 306 支次、投入蓝队专家 918 人次、投入工作量 6685 人天。项目涵盖党政机关、公安、政企单位、民生、医疗、教育、金融、交通、电力、银行、保险、能源、传媒、生态、水利、旅游等各个行业。在实战演习过程中，奇安信集团派遣最优秀的蓝队高手全力参与工作，并在所有行业化的实战攻防演习排名中名列前茅，其中排名第一的次数高达 66.7%。

在协助国家主管机关的工作中，针对等级保护重要信息系统以及国家关键基础设施，深入开展实战攻防工作，使得国家相关重点信息系统的整体安全性有了显著提高和可靠保障；在协助央、国企单位工作中，对企业本级以及下级单位的重点网络信息系统、敏感系统、工控系统，进行全面的蓝队渗透攻击，极大地提升了各级单位应对网络安全突发事件能力，大幅度提高了相关网络及系统的防护水平。

如今，奇安信集团已组建起 10 余支技术高强、能力突出的网络蓝队，聘请具备 APT 高级渗透实战经验的专职攻防专家 100 余人，是目前国内规模最大、人数最多的蓝队队伍之一。

实战攻防是个对抗的过程，无论对抗中的攻还是防，其目的都是为了提升网络的安全防护能力，加强安全应急的响应处置能力。奇安信集团将肩负“让网络更安全、让世界更美好”的使命，以攻促防，为提升网络安全水平贡献力量。