

基于网络APT攻击防护的网络安全预警技术

目前为企业网络、政府信息化系统、金融网络和互联网产业等网络攻击与日俱增，尤其对重点机构和部门的攻击，在使用0day，花了很多时间为一个长期目标进行深度攻击。这意味着测试手段是有很大的局限性，针对安全攻击事件我们的设备环境没办法高效的发现，所以一种能检测这样攻击的设备是非常重要的和必须的。这些对设备的攻击有：就一些网络攻击例如0day攻击，常规攻击和已知漏洞攻击提前预测发现，对这些攻击的能力的分析造成后果的评估功能。国家电网公司为保障信息化系统防护安全对体系结构建设的整体目标是基于网络安全预警技术其中包括保护应用系统环境被破坏、防止信息网络故障、防止企业信息资源外泄、防止有害不良信息快速传播、防止业务数据丢失损坏、防止恶意病毒攻击以及防止有害不良信息快速传播，保障业务流程安全运转，保障信息系统稳定安全高效的运行。

胡楠¹ 冉冉¹ 吕旭明² 杨壮观¹ 郑善奇¹ 刘为¹ 谭烨³/1.国网辽宁省电力有限公司信息通信分公司 2.国网辽宁省电力有限公司科技信通部 3.沈阳信普电子技术有限公司



胡楠/工程师

0 引言

APT (Advanced Persistent Threat) 即高级持续性威胁。相对于其他攻击方式，APT攻击的方式更加先进和高级，其攻击的高级型集中体现在攻击开始前针对攻对象的整体系统结构和相应的业务数据流程有效快速准确的搜索，以主动攻击方式，对系统漏洞进行快速的锁定，然后针对这些漏洞所在的网络进行大量长期有效0day漏洞攻击手段。

1 攻击特点

1.1 极强的隐蔽性

对于网络上的具体目标被APT低调

隐蔽攻击。在攻击前不会有太多活动，使其防御系统能预测攻击。此功能性理解为APT攻击已经融合搜索了业务系统环境和可信程序漏洞然后对对象进行攻击，在结构框架内部中，该融合很难被看到。比如，使用了MD5的碰撞漏洞使用最火的APT攻击“火焰(Flame)”，制作假的数字证书通过验证系统认为是正规的软件对网络欺骗性攻击。

1.2 潜伏期长，持续性强

单纯的破坏和追求短期利益并不是APT的目的，APT在于逐步的侵入来入侵整个系统的策略。APT攻击会长期潜伏在系统网络环境中，通过不断收集用户信息，实现整个系统业务数据的截取。以“被控主服务器”为跳板，持续搜索，已达到获取目标系统使用管理权限行为，如图1所示。这样的攻击方式，是“恶意的商业间谍威胁”，所以具备很长的潜伏期和持续性。



图1 APT攻击特点

1.3 目标性强

与常规病毒相比较而言，APT开发人员会凭借超高的网路攻击技术和系统漏洞的洞察能力。使用APT攻击需要的

关键词/Keywords

病毒攻击 ·
持续性威胁 ·
APT攻击 ·
网络安全 ·
0day漏洞 ·

技术和资源要求是要高于普通的网络攻击方式。这样的攻击方式不以普通的个人用户为主,其攻击的目标一般选定为价值比较高及相对比较重要的数据的特殊用户群体,其中工业控制系统和高密度机密数据为主题的网络运行环境为第一选择目标。

1.4 利用0day攻击

0day漏洞技术动态获取权限是被APT普遍使用的、这样的方式是已植入木马的形式远距离控制其目标系统或网络。同时使用N个0day漏洞攻击是APT的高级攻击方式,这样的多0day漏洞攻击方式是APT攻击的重要特点之一。

2 现有的检测技术

现阶段,传统企业是以多种网络安全防御体系结构来保障网络系统环境的安全性的,其中包括网络软硬件防火墙,IPS、VRV、IDS和日志管理等防御策略,但这样的网络体系结构无法针对APT攻击做到有效的防御和控制。

2.1 传统网络防火墙

初期的网络防火墙只针对企业局域网络访问加以控制和防御,以构建网络访问控制列表(ACLs)的方式,管理员来验证是否阻止一个源地址、一个访问地址及端口的访问请求。这种比较落后的防火墙是根本无法阻止APT攻击,传统防火墙是针对在网络层和会话层的攻击,但是APT攻击是攻击更高的协议层次,所以这样的攻击方式是无论防火墙是在外部和内部都无法发现其行踪的,防火墙做不到对这些流量和攻击的发现,智能以ACL列表的形式来对网络环境做简单的监视与控制是满足不了安全网络体系标准的。

防火墙技术得到重大的进步是以状态检测防火墙使用了状态检测包过滤技术。这种技术室基于网络层以检查引擎来截取数据包的方式来抽离出于应用层有关状态的信息数据,然后用截取的状态信息及数据包与上一时刻的状态信息及数据包相对比,以对比结果为依据,对是否接受连接做出判断。为了提高网络安全性为目的,要对网络通信的各个层都要检测,与包的过滤技术相同,是以IP地址、端口号和TCP标记,检测通过

的过滤的数据包。但是,对应用层的攻击很多是没办法通过状态防火墙进行过滤检测出来的,一个隐藏攻击如果存在合法的数据包中,它是可以顺利通过防火墙的检测过滤从而到达应用服务器中。

2.2 入侵检测系统(IDS)

IDS对网络传输过程作实时监控检测的比较标准的网络搜索设备。它无须网络流量流经也不需要跨接在任何链路上都可以工作的。在报文的收集上,IDS能够利用内置的数据知识库分离取出相应的流量统计数据值来,IDS设置挂接在所流经的链路上对所经过的流量给予关注,通过自身数据库与流经的数据流量特这进行智能匹配比较,再通过预设的阈值,比较耦合度较高的报文流量被检测出为恶意攻击,IDS会根据相关配置参数对其进行报警、限制和隔离等操作。

智能识别技术记录并报警存在的安全隐患和漏洞是入侵检测系统的重要特点。现在普遍安全系统都智能针对已知漏洞进行检测,不可以对未知系统安全漏洞做出预警。现阶段很多攻击数据库都是通过网络层攻击的,以TCP碎片攻击,通过加密的方式还有很多方式是可以避开入侵检测系统的检测,从而攻击网络及服务器。

2.3 防病毒网关

防病毒网关是以保护网络内进出数据的安全为目的网络设备。其重要功能包括查杀病毒,过滤关键敏感词汇,阻止垃圾邮件接收发送等,同时还具备部分防火墙功能。支持HTTPS地址加密,针对恶意代码植入检测功能,并要求对URL地址过滤和控制应用,还可以对互联网行为形成跟踪统计等功能。

现阶段,病毒不在成为威胁网络安全的唯一来源了,同时还要同时伴随恶意代码的植入、垃圾邮件及黑客恶意攻击同时多样化攻击和威胁。所以怎么样保护国内企业网络安全,更加完善地构建安全体系是更重要目标,但是首先要针对病毒通过电子邮件与附件的形式来侵入的网络要给予强有力的手段阻止入侵网关,网关就象是一扇大门,来链接网络,如果网关敞开那么企业的整个网络安全将不受任何保护。

从安全的角度来关注对网关的防护,就能使

网关发挥出“一夫当关，万夫莫开”的作用。但如果不能有效地设置网关，那么恶意代码就可以顺利的植入企业的内部系统中，病毒就能通过网关流入到企业内网中肆意破坏企业网络环境，为企业带来灾难性的损失。对于以上安全策略的考虑，企业逐渐认识网关在网络环境中的重要性，分别部署了防病毒网关，用来阻挡病毒进入网络。

进出网络内部的数据能够被这种网关防病毒产品检测，可以对POP3、SMTP、IMAP、HTTP和FTP等协议的数据进行病毒搜索和检测，如果发现病毒根据预设的策略对病毒进行隔离和查杀等措施，在网络安全防护方面起到重要的作用，但是对于利用0day进行的APT攻击是无法防御的，这是因为病毒网关的检测都是根据文件类型，而且只能通过数据库对已知病毒进行防御，对未知病毒是束手无策的。

3 安全需求

现阶段，就企业网络、政府信息化系统、金融网络和互联网产业的攻击与日俱增，尤其对重点机构和部门的攻击，在使用0day，花了很多时间为一个长期目标进行深度攻击。同时因为技术和硬件方面诸多因素的限制，针对这样的攻击方式检测方法有限，没有办法高效的对这类的攻击做到有效的防范和控制。因此就要有一套用来检测这类攻击方法的设备，这类设备应该具备的功能包括：0day攻击，常规攻击，已知漏洞攻击提前预测发现，对这些攻击的能力的分析造成后果的评估。

4 网络安全预警技术

网络安全预警技术是通过解析关键网络协议，对网络数据快速截取数据包进行统计分析。利用多种方式来对APT攻击进行分析、追踪和定位。其重要手段有检测恶意流量攻击检测已知威胁安全漏洞检测0day漏洞、检测主动攻击和综合预警策略。通过分析综合关联策略准确得出APT攻击路径和攻击的行为，如图2所示。

4.1 APT攻击检测流程

检测文件攻击、0day攻击、邮件攻击和Web应



图2 APT攻击的行为和攻击路径

用攻击，流量行为分析是网络安全预警技术重要功能。

4.2 Web应用攻击检测

网络安全预警平台还能进行网络URL翻译、Cookie安全、限制请求和URL参数定义。网络安全预警技术能检测恶意主动被动攻击方式，不管它是未知还是已知的。都能够阻止，例如缓冲区攻击、脚本攻击、SQL注入和恶意访问等攻击方式。

网络安全预警技术是针对应用网络环境和Web流量监控进行深度分析检测，使入侵防御能力得到全面提高。在没有攻击到达Web服务器之前进行提前检测，并实时攻击提供预警功能。网络安全预警技术能够解析所有访问的请求。根据规则策略验证合法性；只能以正确格式或者RFC遵从的请求可以通过。恶意请求会被阻断，对恶意脚本的注入也会被阻止。

4.3 流量分析检测

APT都会同时伴随着人工渗透攻击，人工渗透攻击中通常会使用病毒扩散以及高频率的扫描方式。实施这些方式的过程中，会产生很多的恶意流量。再通过恶意流量特征，准确地判断检测攻击方式。

现阶段，检测通过以下维度，如：

- 通过端口的检测；
- 通过IP的检测；
- 通过日期时间的检测；
- 通过协议的检测。

4.4 0day攻击检测

诸多0day攻击的特点是在大量的运行维护工作中，通过现场运维人员归纳总结出来的。网络流量分析过程中，通过目标文件以快速检测算速进行检测，搜索发现网络流量0day攻击样本。

有效检测0day攻击行为是结合动态分析技术

(下转第350页)

提出更高的要求,在本文中对智能变电站的各个使用环节及其现状进行了详细分析,并提出了相应的技术要求。在既能够体现智能变电站的技术特征又要屏蔽底层复杂的技术细节的基础上,提出了面向使用的智能变电站综合一体化系统软件的实现方案,从需求、功能和模式等几个方面进行了阐述,方案可操作性强,具有较强的推广价值。

参考文献

- [1] 叶翔,刘辉,周永忠.智能变电站图模一体化设计软件实现方案[J].江苏电机工程,2014,33(3):41-44.
- [2] 龚晖,吴玉硕,李新梅,等.智能变电站二次系统测试方案研究[J].甘肃电力技术,2014:1-4.
- [3] 张阳.智能化变电站二次系统调试技术[J].农村电气化,2014,1:40-42.

- [4] 赵勇,石光,杨经超,等.智能变电站的运维调试研究,信息通信[J].2014,1:275-277.
- [5] Q/GDW383-2009 智能变电站技术导则[S].
- [6] Q/GDW431-2010 智能变电站自动化系统现场调试导则[S].
- [7] Q/GDW431-2010智能变电站自动化系统现场调试导则[S].
- [8] 梅德冬,黄国方,孙军陵.智能变电站二次设备自动检测系统设计[J].低压电器,2011(4):43-36

(收稿日期:2015-03-30) EA

作者简介

张庆伟(1981-),男,硕士,高级工程师,主要研究方向为电力系统继电保护和自动化技术。

王力(1983-),男,硕士,工程师,主要研究方向为电力系统继电保护和自动化技术。

(上接第342页)

通过检测目标文件中的以脚本类文件中的攻击特征和shellcode来实现的。

4.5 深度协议解析

现阶段能解析五种协议,包括POP3、SMTP、IMAP、HTTP和FTP等。

网络安全预警技术是对网络流量数据深度解析的过程中,快速全面地检测流量中的恶意攻击并实时的预警功能,能够在网络APT攻击前做到提前发现,并实时预警。Oday攻击及恶意攻击可以各种检测手段暴露出来。

网络安全预警技术能预警及检测APT攻击等,不管它是未知还是已知的,都能得到有效的控制和处理,其常见的攻击模式包括:网络恶意攻击、恶意脚本注入恶意攻击和上传文件恶意攻击等。

4.6 邮件攻击检测

网络安全预警技术对首先对深度解析邮件协议,分析并记录邮件信息,还要对其附件文件进行更为行之有效的检测,对其中安全漏洞和问题进行预警。

扫描动态分析以是可以发现邮件附件的未知攻击漏洞,同时对攻击特征的分析测试出已知攻

击特征,从而发现恶意攻击。

5 结束语

网络安全预警技术研究,应用与实施可以能够深层解析网络攻击。使国家利益、社会利益和企业利益得到有效的控制和减少,同时降低风险。

参考文献

- [1] 卜娜. APT攻击: 阴险潜伏, 一心窃取企业机密[J]. 中国计算机学报, 2012.
- [2] 高春燕. 动静结合应对APT攻击[J]. 中国计算机学报, 2012.

(收稿日期:2015-03-30) EA

作者简介

胡楠(1982-),博士,工程师,主要研究方向为故障抢修运检技术、数据库应用集成、应用系统集成与优化实施工作。

冉冉(1980-),女,硕士,工程师,主要研究方向为数据库应用集成、应用系统集成与优化实施工作。