江西省网络与信息安全情况通报

江西省网络与信息安全信息通报中心　　2017年5月27日

关于应对“影子经纪人”公布的系列漏洞威胁的预警通报

2017年4月14日，黑客组织影子经纪人Shadow Brokers公布了NSA泄露的“网络军火库”。5月12日，新型“蠕虫”勒索病毒WannaCry在全球大规模爆发，此次勒索病毒正是利用披露的军火库中的一款漏洞工具。省网络与信息安全信息通报中心对本次泄露的18种应用较为广泛的网络攻击工具进行了认真分析研判，从攻击工具名称、影响系统版本、利用端口号、处置措施等方面进行了认真梳理（详见附件）。请各成员单位高度关注，迅速组织开展紧急排查、漏洞修复及其他处置措施，一旦发现攻击情况请及时上报。

附：常用网络攻击工具及处置建议

省网络与信息安全信息通报中心

2017年5月27日

报：心社、刘奇同志
建业、力平、为文同志
国家通报中心、公安部十一局
省信息通报机制成员单位主管厅（局）领导

送：厅直有关单位
省信息通报机制成员单位
各设区市公安局网络安全保卫支队

（共印 200 份，存档 3 份）

审批：琚忠秋　　核稿：叶文锋　　编校：徐钒婕

附件：

常用网络攻击工具及处置建议

攻击工具名称	影响系统或应用名称	利用端口号	处置建议
Easybee	WorldClient 9.5, 9.6, 10.0, 10.1	1000/3000	升级最新版本 17.0.1 下载地址：http://www.altn.com/Downloads/MDaemon-Mail-Server-Free-Trial/
Easypi	IBM Lotus Notes（Windows NT, 2000 ,XP, 2003）	3264	升级到 9.0.1 以上版本并安装最新补丁 地址 1：http://www-03.ibm.com/software/products/en/ibmnotes 地址 2：https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=Collaboration%20Solutions&product=ibm/Lotus/Lotus+Notes&release=9.0.1.8&platform=Windows&function=all
Eclipsedwing	Windows 2000, XP, 2003	139/445	补丁版本号：KB958644 下载地址：https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
Educatedscholar	Windows vista, 2008	445	补丁版本号：KB975517 下载地址：https://technet.microsoft.com/en-us/library/security/ms09-050.aspx
Emeraldthread	Windows XP，Vista，7，Windows Server 2003,2008	139/445	补丁版本号：KB2347290 下载地址：https://technet.microsoft.com/en-us/library/security/ms10-061.aspx
Emphasismine	IBM Lotus Domino 6.5.4, 6.5.5, 7.0, 8.0, 8.5	143	升级到 9.0.1 以上版本并安装最新补丁 下载地址 1：http://www-03.ibm.com/software/products/en/ibmdomino 下载地址 2：https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=Collaboration%20Solutions&product=ibm/Lotus/Lotus+Domino&release=9.0.1.8&platform=Windows&function=all
Englishmansdentist	Outlook Exchange	25	升级到 2010 以上版本 下载地址：https://products.office.com/zh-cn/exchange/email

Erraticgopher	Windows XP SP3, Windows 2003	445	建议升级到 vista 以上版本，由于微软停止服务，暂无补丁，可禁用 SMB 服务，防火墙禁用 445 端口。
Eskimoroll	Windows 2000, 2003, 2003 R2, 2008, 2008 R2	88	补丁版本号：KB3011780 下载地址：https://technet.microsoft.com/en-us/library/security/ms14-068.aspx
Esteemaudit	Windows XP, Windows Server 2003	3389	建议升级到 win7 以上系统，由于微软停止服务，暂无补丁，可禁用远程桌面服务，关闭 3389 端口防护。
Eternalromance	Windows XP, Vista, 7, Windows Server 2003, 2008, 2008 R2	139/445	补丁版本号：KB4013389 下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx
Eternalsynergy	Windows 8, Windows Server 2012	139/445	补丁版本号：KB4013389 下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx
Ewokfrenzy	IBM Lotus Domino 6.5.4, 7.0.2	143	升级到 9.0.1 以上版本并安装最新补丁下载地址 1：:http://www-03.ibm.com/software/products/en/ibmnotes 下载地址 2：https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=Collaboration%20Solutions&product=ibm/Lotus/Lotus+Domino&release=9.0.1.8&platform=Windows&function=all
Explodingcan	Windows Server 2003 WEBDAC	80	微软停止服务，暂无补丁，微软建议升级 WIN7 防护。
Zippybeer	Windows Domain	445	建议升级系统，由于微软停止服务，暂无补丁，可禁用 SMB 服务，防火墙禁用 445 端口。

Eternalblue	Windows XP(32),Windows Server 2008 R2(32/64),Windows 7(32/64)	139/445	补丁版本号：KB4013389 下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx
Doublepulsar	Windows Vista, 7, Windows Server 2003, 2008, 2008 R2	139/445	补丁版本号：KB4013389 下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx
Eternalchampion	Windows XP, Vista, 7, 10,Windows Server 2003, 2008, 2008 R2, 2012, 2016	139/445	补丁版本号：KB4013389 下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx