2021 守内安信息科技 & ASRC 电子邮件安全趋势回顾



2021年依旧笼罩在新冠疫情之下,相较于2020年,大家也都慢慢开始适应WFH (Work From Home 居家办公)的工作型态,信息安全设备的部署不再只是慌乱应对远程工作所带来的安全隐患,而是全新型态的适应性部署。

电子邮件安全趋势

守内安与ASRC研究中心针对去年邮件安全汇整,相较于2020年,2021年度的垃圾邮件总量增长幅度约为8%,但垃 圾邮件的大小却增长了43%,这对邮件服务器的储存空间,以及邮件扫描过滤的效能带来了不小负担;但垃圾邮件乱 枪打鸟式的滥发滥寄情况,却呈现下降的趋势。威胁邮件的部分:利用可以快速生成钓鱼页面的免费平台进行的钓鱼 攻击增长了210%;一般诈骗邮件上升了近60%;伪冒为快递、邮政相关诈骗增长了近25倍;针对企业交易时所进行的 BEC(Business Email Compromise)商务邮件欺诈,攻击数量,则较2020年增长了近8倍。在WFH(居家办公)的工作 型态下,伪冒、诈骗等社交工程手法的攻击变得更加猖獗;多数企业也察觉了这样的趋势,因此,2021年企业内部实施 社交工程演练的邮件量较2020年上升了近90%。

APT攻击与漏洞利用

APT攻击大多以电子邮件为起点,直接发送利用Office漏洞的恶意文件。以此来尝试入侵企业内部,以进行窃资、部署 勒索软件等目的。但是既有Office漏洞利用并非APT攻击的专利,大量滥发的病毒邮件中,也充斥着漏洞利用的手法。

2021 年常见的既有 Office 漏洞利用状况整理如下:

排名	漏洞编号	数量增幅比例	漏洞说明
1	CVE-2018-0802	549.13%	Microsoft Office 内存损坏漏洞
2	CVE-2017-0199	334.12%	Microsoft Office OLE2Link 漏洞
3	CVE-2017-8570	316.68%	Microsoft Office OLE 逻辑漏洞
4	CVE-2018-20250	253.33%	WinRAR 路径目录穿越漏洞
5	CVE-2012-0158	200%	Microsoft Office 缓冲溢出漏洞
6	CVE-2017-11882	36.28%	Microsoft Office 内存损坏漏洞



Purchase Order		
Kara Lee (ka	.com) 添加联系人	2021/12/23 下午 0
收件者:sales	com;	
N Purcha X≣ se_Or der		
Good Morning!		
This is He e from	Technology Co., Ltd	
Kinldy Pls Find The A	are highly needed by clients. ttachment of Purchase Order Dec 202 to let me know if you can delivery befo	
Best Regards K e		
Co., Ltd		
182 2122 0580		

▶ 利用 CVE-2018-0802 漏洞滥发病毒邮件

邮件攻击趋势

恶意文件内的恶意文件

2021年有大量的恶意Office文件,文件中并无利用漏洞进行攻击的迹象;也没有VBA的使用,它利用的是Office的XML结构来隐藏远程真正包含攻击意图的另一个恶意文件。当收件者打开恶意Office文件时,Word就会去远程抓取另一个恶意Word文档,并尝试打开,进一步入侵受害者的计算机。

这样的攻击形式,让恶意文件不容易被防御机制抓取分析,也能在接触到真正要攻击的对象时,才暴露出本体。



▼利用 Office 的 XML 结构抓取外部设定,实际是抓取另一个恶意文件,并尝试开启

1 La 17 - U IT		81)-H7011-13021-18.doc: (Compati	bility Mode] - Microsoft Word	091
Fale Home Insert Page ▲ Cut ■a Copy Nunito 5 Paste ✔ Format Painter ■ I Clipboard ™ ■ I	ie Layout References Mailing ans $ $ 2 $ $ $A^* A^* $ $Aa^* $ \underline{U} - $Aa x$, $x^* $ $Aa^* = 2$ Font	≡≣ :⊧· ,@+⊞+	TNormal TNo Spaci Heading 1 Heading 2 Title Than Style	
Sevich Document	The link 3 (https://mutilo Chit-Click to follow lin Back to lýme	because the campaign ended	or the link was disabled. If you have any questions, feel free to contact u	L.
https://inurl.io			(1) (2) (3) II 100% (-	0 4
	a 🗔			0 Do 9-15 AM

▶ 攻击者可随时移除、变更恶意文档;或排除非目标

Excel 的花式攻击手段

我们也发现Excel在2021年,有着各种花俏的攻击手段,除了前述提及的利用XML结构的攻击形式外,由于Excel可以 针对文件、窗口或VBA程序代码做局部或全部的加密,再加上使用Microsoft Excel电子表格的VelvetSweatshop默认 密码,就能让恶意文件躲过安全扫描;而将恶意的Excel文件保存为.xslb格式,也具有让恶意代码不被检查出的效果。

	ut opy * ormat Painter ard 12	в <i>I</i> <u>U</u>	• 🗄 • Font	• A	≡			Wrap Text Merge & Ce	nter •	š - % Numi	• 1 %8 a	• 28 Ft	onditional Fe ormatting * as Style		Insert	Delete Format	Σ AL Fil Q Cl	
A	B	с	D	E	F	G	H	1		1	ĸ	L	M	N	0	P	Q	
1.0			n.	-	1111-11-1	Micro		aft Excel is w	_	ок			an OLE action.					

「加密手段能让恶意的 Excel 文件躲过安全扫描

#47821558 Invoice	
PO #47821558 Due 25-10-2021 (Lilia ro.com) 添加联系人	2021/11/25 上午 12:54
收件者: To: '	
6 08236 55551 4835	
Dear Wsch 08236555514835947.xlsb (88.7 KB)	^
This is a notice that an invoice has been generated on 11/24/2021.	
Invc 8	
Am 3.73 USD	
Due /2021	
Invoice Items	
Sub Total: 099.71 USD	

「原用于提高 Excel 档案运行速度的 xlsb,成为掩饰恶意代码的好方法

合法服务遭到滥用

攻击者深知,要发送一个不易被安全措施侦测出的攻击邮件,首先要从合法来源寄出,并且尽量避免直接夹带恶意文件或程序代码,真正的攻击,应该放在夹带的外部超链接。我们在2021年也看到了许多合法来源发送的攻击邮件,数量较多且较为知名的,都是电子报或营销邮件的投递系统,诸如:Salesforce、Sendgrid...等。

遭到滥用的投递系统,似乎不是因为某种系统bug而是直接被用来投递恶意邮件,更像是一些合法账号遭到了钓鱼、或 从其他方面泄漏了敏感信息后,利用这些敏感信息合法登入投递系统后再进行的投递。

外部超链接部分,除了一般常见的免费页面生成器被用于钓鱼外,许多云端服务的API也被用于撰写钓鱼页面或储存 恶意文件。



信赖成为新的挑战

过去,白名单、内外网、安全区域的区别,都在于信赖的是一个特定的对象或区域。并且信赖的「对象」或「区域」一旦设定完成后,几乎没有一个重新审视的基准或周期。攻击者会设法入侵或控制这些被信赖的「对象」或「区域」,如此一来就可用特权进行深度的数据窃密或破坏。疫情影响下的世界,远程操作、隔着屏幕的人际互动,都让人难以判断原本信任的对象是否受到控制或入侵。新的一年,不论疫情是否结束,攻击者仍会以社交工程、诈骗手法来让自己带上"熟人"的面具,所以零信任的信息安全架构将会是未来的主流防御措施。

关于 ASRC 垃圾讯息研究中心

ASRC 垃圾讯息研究中心 (Asia Spam-message Research Center),长期与守内安合作,致力于 全球垃圾邮件、恶意邮件、网络攻击事件等相关研究事宜,并运用相关数据统计、调查、趋势 分析、学术研究、跨业交流、研讨活动等方式,促成产官学界共同致力于净化因特网之电子 邮件使用环境。





© 2022 Asia Spam-message Research Center. All Rights Reserved.