火绒安全
HUORONG SECURITY

火绒安全 2021 终端安全情报年鉴

HUORONG SECURITY

火绒安全实验室

前言
preface

2021年是全球严防“疫情”大背景下，网络安全迈入新常态的一年。随着数字经济蓬勃发展，网络安全面临网络空间与现实边界逐渐模糊、网络攻击愈发复杂和多变的新挑战。此外，勒索事件、漏洞攻击、信息泄漏等威胁依旧层出不穷。网络攻击不再是单纯的破坏行为，而是对利益的攫取。基于此，“十四五”规划中重点提及加强网络安全，《个人信息保护法》、《数据安全法》等法规相继出台，也明确了用户的数据安全底线。

终端作为网络世界的“神经末梢”，处在网络安全防御的第一线。本报告依托“火绒威胁情报系统”、“火绒在线支持与响应平台”产生的真实的终端安全防护数据，展现2021年终端威胁趋势以及风险变化，通过分析总结，帮助各行业用户建立有效的防护机制。

本报告共分为三部分，分别从“威胁与攻击趋势”、“火绒安全响应服务”、“火绒防护体系”三个方面展开。

关键词
keyword

24亿次
2021年，火绒安全拦截终端遭遇的攻击高达24亿次。

45亿次
2021年，火绒安全共拦截（不含用户手动拦截）45亿次弹窗广告。

1000万+病毒样本
2021年，火绒安全截获黑客主动向全网投放的病毒样本超千万，以木马、黑客工具、蠕虫等恶意程序为主，其目的多是为了实施挖矿恶意行为。

6000+安全响应服务
2021年，火绒安全累计为用户提供6000余次安全响应服务。

1177个漏洞
2021年，微软对外披露1177个漏洞，其中高危漏洞773个。

Apache Log4j2漏洞
2021年12月9日，Apache Log4j2反序列化远程代码执行漏洞（CVE-2021-44228）细节被公开，震动整个国内外的安全行业，无数引用该组件的系统和开源组件受到波及。

“定制化”钓鱼邮件
“定制化”的钓鱼邮件，其主要目标为企业用户。通过精准模仿企业日常邮件的格式、称谓等，将带有病毒附件的邮件定向发送给员工，欺骗员工打开，并点击病毒链接、文档。

数百万钓鱼PDF样本
2021年，火绒安全共检测到数百万钓鱼PDF样本。2015年后，恶意PDF样本大量出现，之后每年以数倍的速度增多，其中99%用于钓鱼攻击。

勒索即服务
在火绒安全为企业用户提供响应服务的事件中，发现黑客利用“勒索即服务”（RaaS）模式，攻击各行各业，其中，金融行业、IT行业受到的影响尤为严重。

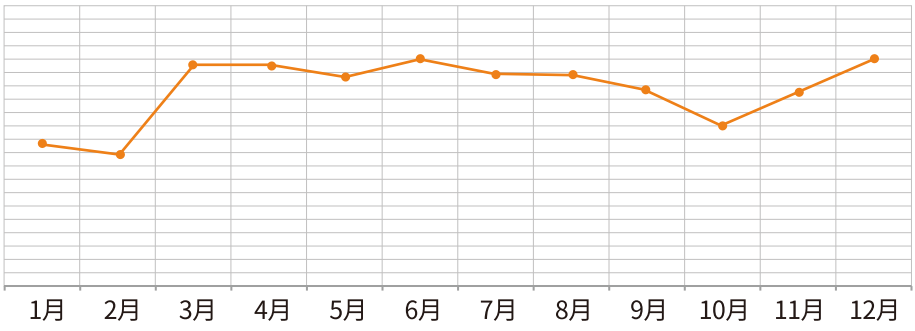
目录
CONTENTS

威胁与攻击趋势

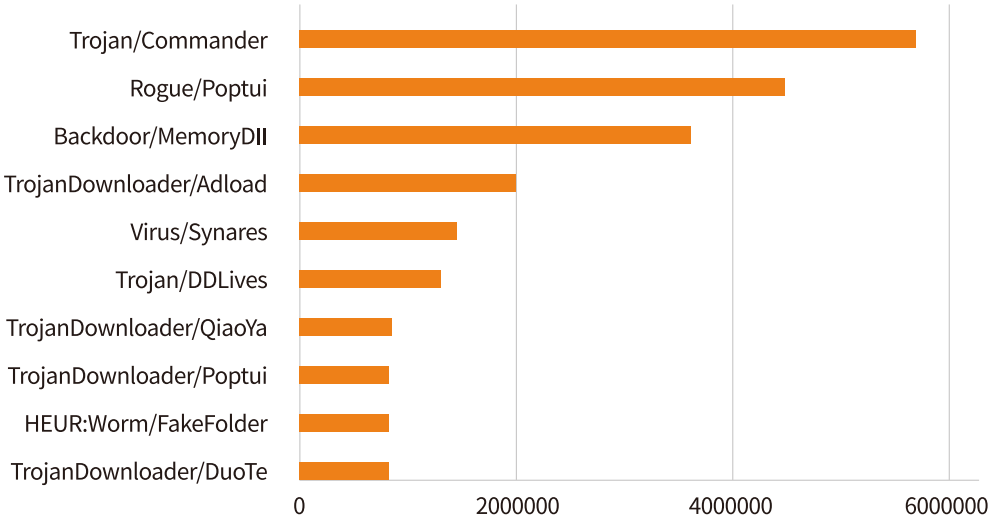
2021年，流氓软件、木马病毒、感染型病毒、蠕虫病毒等恶意程序仍在持续对用户发起攻击。此外，黑客团伙为了攫取利益，不断对病毒进行更新，并使用多样的攻击渠道：如Web服务漏洞、“定制化”的钓鱼邮件、系统漏洞攻击、横向渗透等，与安全厂商进行对抗。

一、终端遭遇攻击24亿次，整体呈现上升趋势

根据“火绒威胁情报系统”监测和评估，2021年火绒安全拦截终端遭遇的攻击高达24亿次。从攻击的趋势来看，2021年整体呈上升趋势，仅在2月份与10月份稍有下降。攻击终端的主要恶意程序包括木马病毒、流氓软件、感染型病毒、蠕虫病毒等。



2021年火绒安全威胁情报趋势

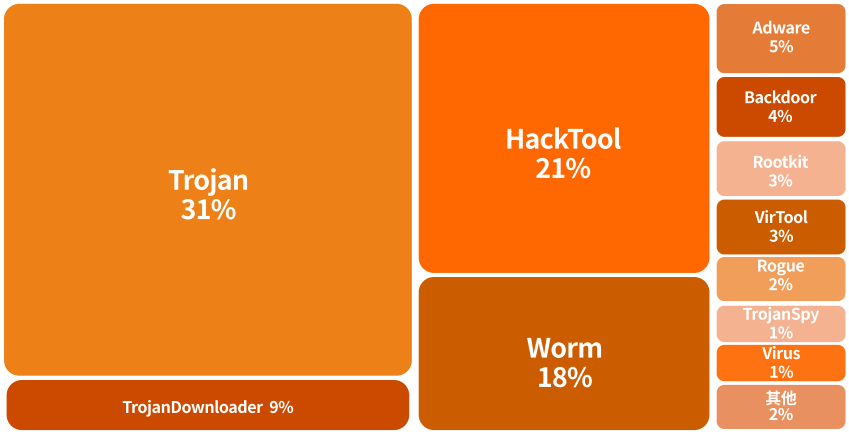


攻击终端数量TOP10病毒家族

二、截获病毒样本过千万，黑客与厂商对抗更激烈

此处病毒样本表示由黑客主动向全网投放的病毒，新增样本的数量与增长趋势显示黑客攻击的强烈程度，能够更真实的反映全网的安全状况。

2021年火绒安全共截获病毒新增样本数量超过千万，其中，木马病毒（Trojan）、黑客工具（HackTool）和蠕虫病毒（Worm）的新增样本量均超过百万，分别占据总数的31%、21%和18%。



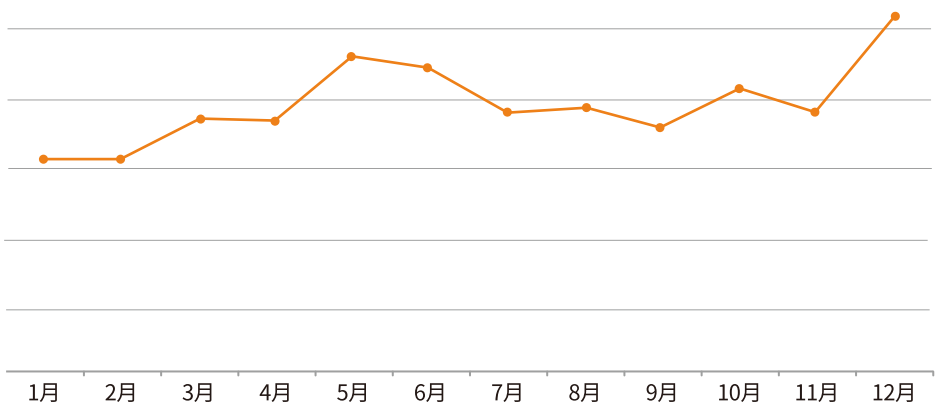
2021年火绒安全截获病毒样本情况

火绒安全实验室分析发现，2021年木马病毒（Trojan）、黑客工具（HackTool）和蠕虫病毒（Worm）增量均与挖矿病毒相关。值得注意的是，勒索病毒与挖矿病毒的传播渠道存在一定的重合度，企业与个人用户都可能成为攻击目标。但相较于勒索病毒敲诈式的获利方式，挖矿病毒更具有隐蔽性、持久性，因此成为黑客获利的首选方式。

三、攻击方式

1、Web服务漏洞攻击上升，企业首当其冲

根据“火绒威胁情报系统”监测，2021年针对用户Web服务漏洞的攻击呈现上升趋势。事实上，Web服务漏洞大部分和黑客渗透攻击有极强关联性。作为黑客入侵企业的渠道之一，Web服务漏洞攻击趋势的上升也意味着企业遭遇的攻击在增多。

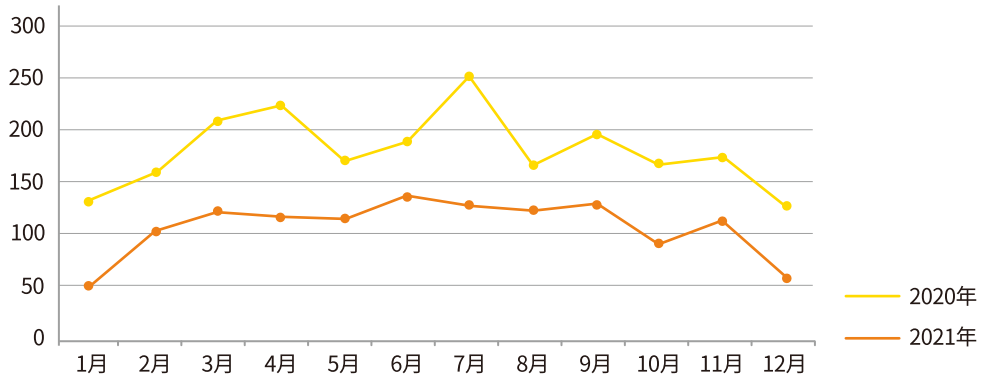


2021年Web服务漏洞攻击趋势

例如2021年8月份，我们发现蠕虫病毒DTStealer出现新变种，该变种增加了针对Linux平台服务器的漏洞攻击逻辑，病毒使用的漏洞包括：Yarn未授权访问漏洞、Redis未授权访问漏洞、WebLogic（CVE-2020-14882）、Elasticsearch（CVE-2015-1427）、Solr（CVE-2019-0193）、Docker（Remote API）。

2、系统漏洞潜藏更大危害，补丁修复任重道远

2021年，微软对外披露1177个漏洞，其中高危漏洞773个，在整体数量、攻击频次上均较2020年有所放缓（如下图）。



微软漏洞全年增长趋势

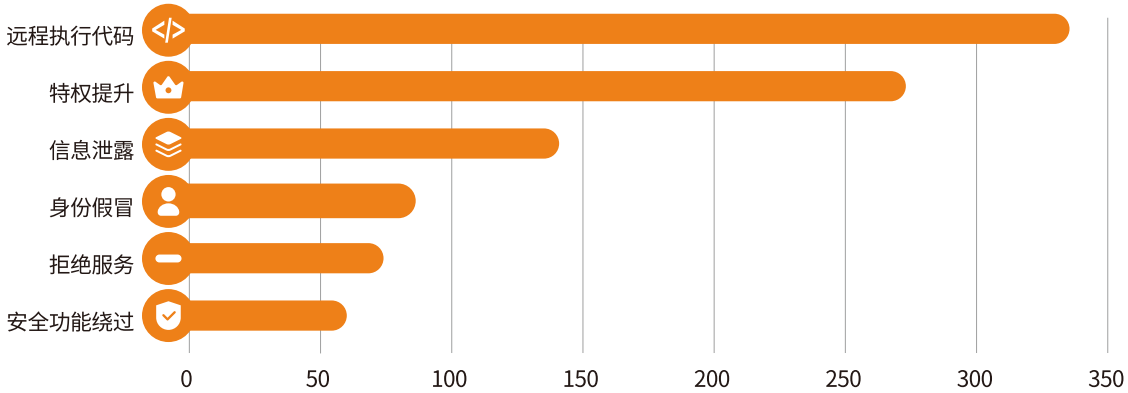
从单个漏洞来看，2021年利用微软系统漏洞发起的攻击数量中，旧漏洞依旧占据多数，“永恒之蓝”(EternalBlue)与MS09-050两个旧漏洞占据近乎90%。

2021年微软系统漏洞利用情况

一方面，由于旧漏洞具备实用性，与病毒相互配合，比如CVE-2020-0796（或SMBGhost）漏洞，在2020年被曝出后，立即就被引入到了一些蠕虫病毒（如DTStealer等）的横向传播模块中，从而造成了更大范围的安全威胁。

另一方面，企业用户服务器终端使用的是老旧系统，不便于停产打补丁，也给了旧漏洞被反复利用的“机会”。

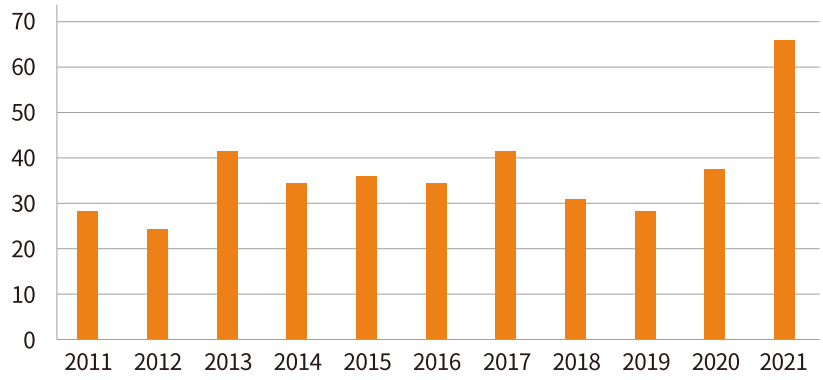
从漏洞的种类来看，远程执行代码类漏洞牢牢锁定数量第一（如下图）。远程执行代码漏洞可以帮助攻击者远程控制用户终端，进行任意操作，危害极大。



2021微软系统漏洞类型

3、零日漏洞数量超过前两年之和

零日漏洞，是指被攻击者掌握却未被软件厂商修复的系统漏洞，是攻击者入侵系统的有力武器。有数据显示，2021年零日漏洞的数量增长了一倍，价格增长了十倍，攻击回报增长了百倍。Zerodium（美国的一家漏洞悬赏创业公司）上公开的零日漏洞价格显示，过去三年中，甚至有些零日攻击的回报上涨了1150%。

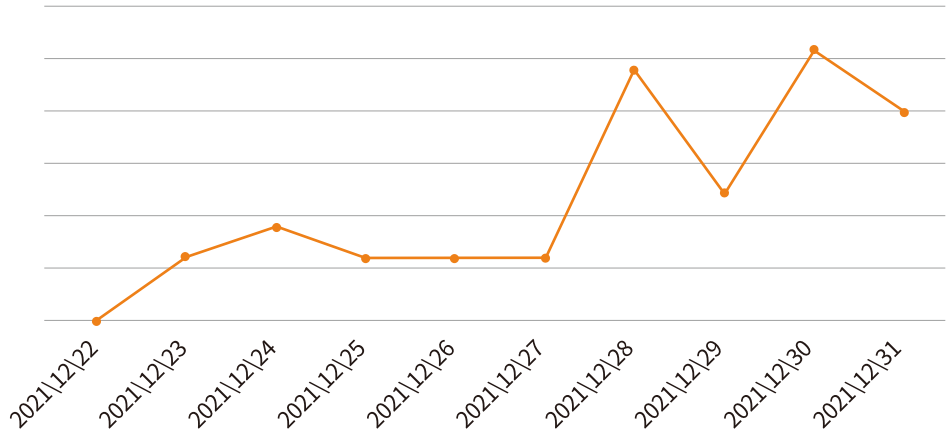


注：2021年数据截止到9月份

零日漏洞数量

4、2021的“王炸漏洞”——Apache Log4j2

2021年12月9日，Apache Log4j2反序列化远程代码执行漏洞（CVE-2021-44228）细节被公开，攻击者可利用该漏洞构造恶意请求，触发远程代码执行。作为Java的底层组件，Log4j2被广泛应用于业务系统开发上，包括OA系统、财务系统、数据库等，同时被应用于大量主流开发框架，以至影响范围极大。不仅如此，该漏洞还具备攻击成本低的特性，这使得该漏洞一经公开就遭到大批量在野利用。据“火绒威胁情报系统”监测显示，直至目前，受该漏洞影响的终端数量依旧在持续上升。

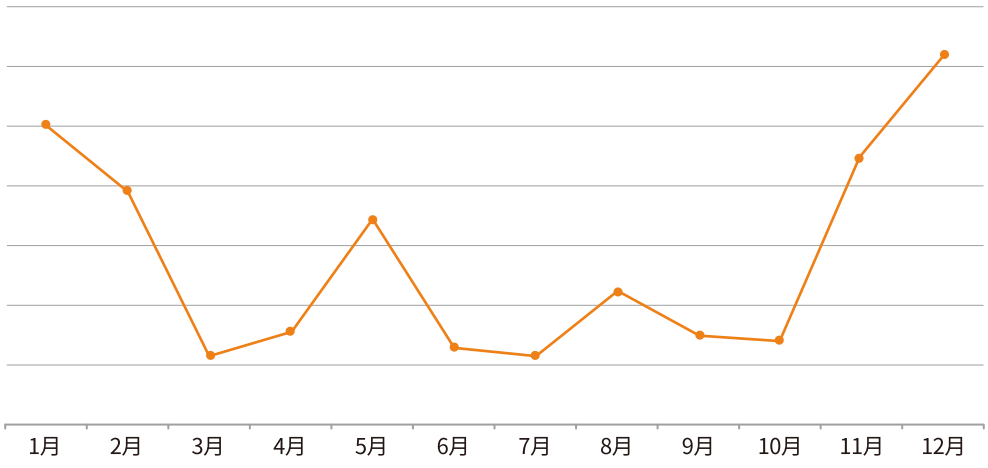


Apache Log4j2 漏洞利用情况

四、钓鱼邮件

1、鱼叉式攻击——“定制化”钓鱼邮件

火绒安全实验室通过多次在用户现场排查发现，相较于传统钓鱼邮件“广撒网”的模式，现在的钓鱼邮件更倾向于“定制化”的鱼叉式攻击，并借助蠕虫、木马等病毒进行大面积渗透。以Emotet家族为例，该病毒在2021年中多次集中爆发，正是借助“定制化”的钓鱼邮件，对企业用户发起鱼叉式攻击。

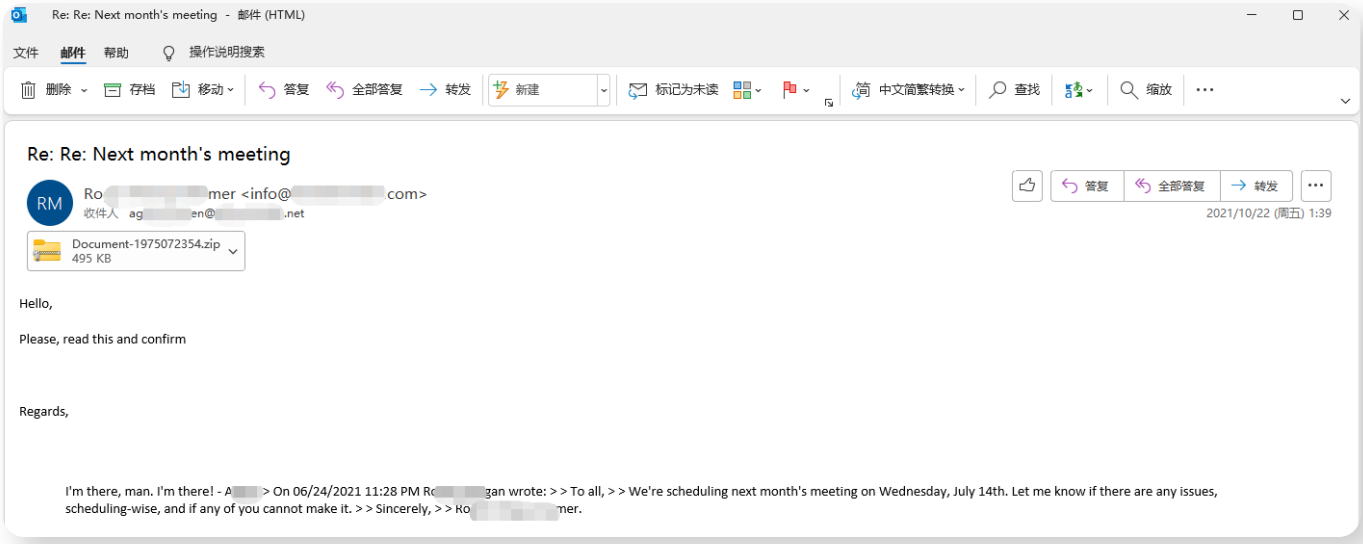


2021年Emotet病毒样本量趋势

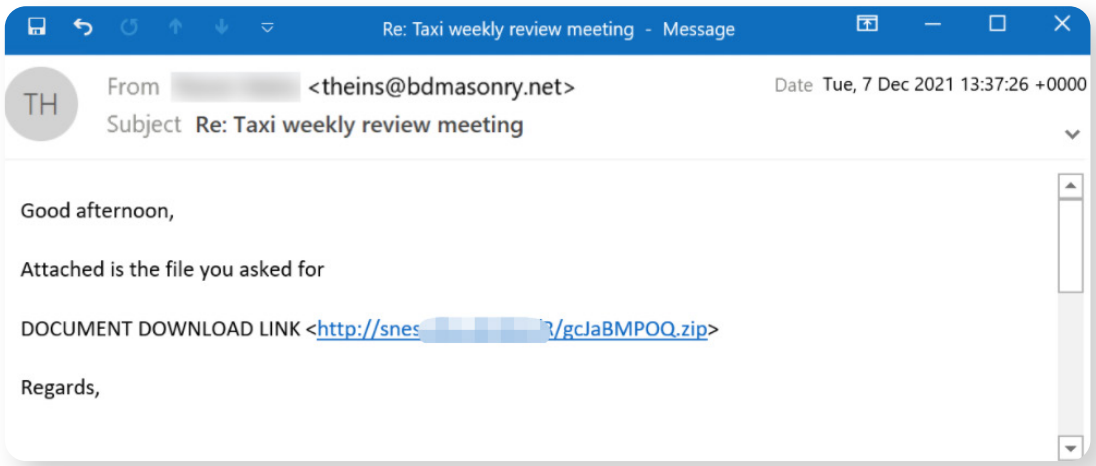
鱼叉式攻击通过精准模仿企业日常邮件的格式、称谓等，将带有病毒附件的邮件定向发送给员工，诱导员工打开，从而点击病毒链接、文档。由于鱼叉式攻击主要针对特定用户、组织或企业，会严重威胁企业信息安全。

(1) 模仿企业邮件格式、称谓的鱼叉邮件展示

- 定制化的鱼叉邮件示例一：模仿企业邮件回复。



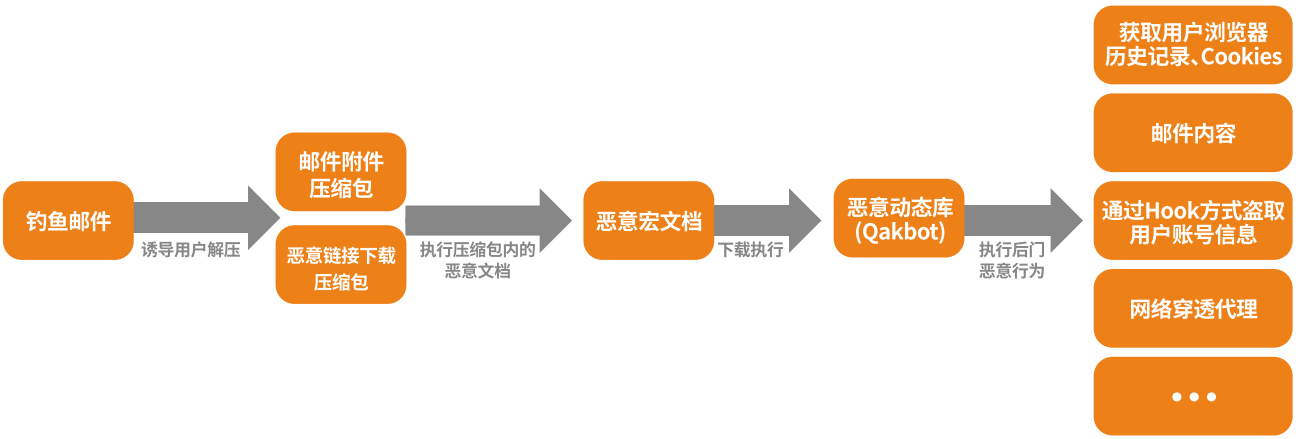
- 定制化的鱼叉邮件示例二：模仿企业邮件会议邀请格式。



(2) 利用鱼叉邮件传播的典型病毒

- Qakbot（银行木马）病毒

2021年，火绒安全实验室在用户现场捕获多起Qakbot（银行木马）病毒，均通过高度欺骗性的仿真企业邮件进行传播。

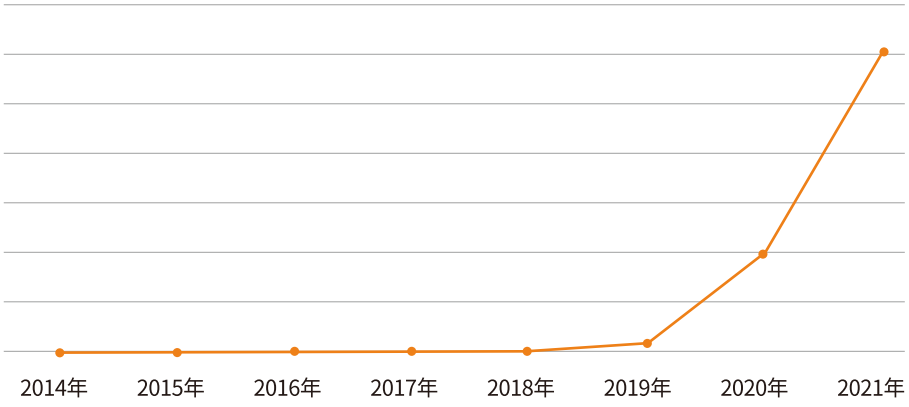


- Emotet木马病毒

“火绒威胁情报系统”监测到今年Emotet木马病毒从死灰复燃到再次大规模爆发，主要通过鱼叉邮件方式进行传播。鱼叉邮件中会将恶意文档（通常为doc、docx、xls、xlsx等）伪装为企业内部业务相关的沟通信息文档，从而诱导用户打开。当用户点击运行邮件附件后，病毒就会被激活，并在终端后台盗取各类隐私信息。

2、钓鱼PDF样本成倍增长至数百万

根据“火绒威胁情报系统”监测，2015年后，恶意PDF样本大量出现，之后每年以数倍的速度快速增长，其中99%用于钓鱼攻击。至2021年，共检测到数百万钓鱼PDF样本。

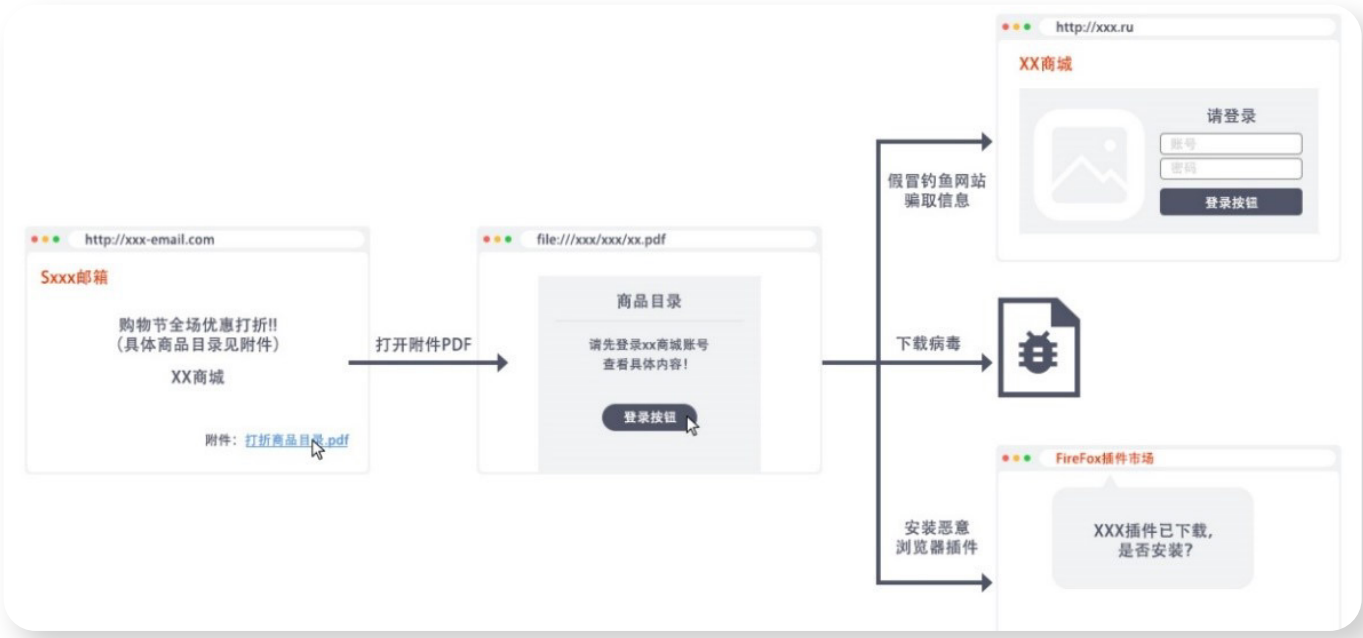


钓鱼PDF样本数量增长趋势

这些钓鱼攻击频繁使用PDF格式的原因，一方面是PDF有丰富的展现形式,极具迷惑性，较邮件、短信等纯文字而言，更难以被检测；另一方面，PDF文件日常使用广泛，当邮件中的钓鱼PDF在浏览器中显示时，用户容易误认为是网站提示而点击

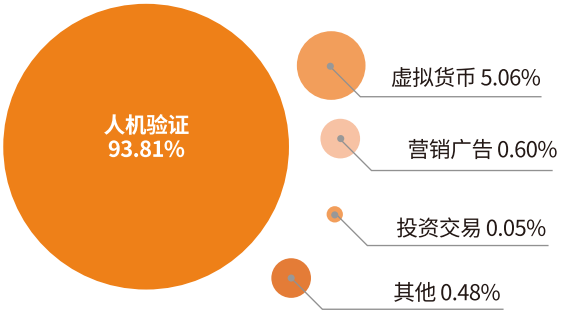
(1) 恶意钓鱼PDF攻击流程

攻击者以电子邮件等传统途径作为初步传播方式，然后在邮件中附上恶意PDF。PDF多为用户感兴趣的虚假信息，以此诱导用户浏览时点击。用户点击后，攻击者会通过钓鱼网站、恶意程序、恶意浏览器插件等方式进一步实施攻击。



(2) 样本类型占比

在火绒安全截获的样本中，人机验证类型最多，占比达93%。当攻击者进行针对性更高的鱼叉式攻击时，由于目标的不同，PDF的页面也变化为不同类型，如虚拟货币、营销广告、投资交易等。钓鱼PDF样本类型比例如下图所示：



钓鱼PDF样本类型比例

(3)典型案例:APT-C-36组织针对哥伦比亚钓鱼文档攻击

黑客在入侵企业之前,通常会在初始阶段使用钓鱼邮件等社工攻击方式。

自2018年4月,APT-C-36组织就针对哥伦比亚政府机构和大型公司(金融、石油、制造等行业)发起有组织、有计划、针对性的长期不间断攻击。攻击者习惯将带有恶意宏的MHTML格式的Office Word诱饵文档通过RAR加密后配合钓鱼邮件对目标进行投递,然后将RAR解压密码附带在邮件正文中,具有很好的躲避邮件网关查杀的效果。

"Subject: we have sent a seizure order to the bank accounts matching your name

Dear taxpayer,

For your information, our intelligent IT system detected that your income statement at the Direccion de Impuestos y Aduanas DIAN has 180 days of arrears. For that reason, we will proceed as stated in the law, article 823 until 843-2.

We attach the information and your debt with the password : dian"

Message | Orden de Embargo.pdf (66 KB)

Asunto: **Hemos emitido una orden de embargo a las cuentas bancarias encontradas a su nombre**

Respetado contribuyente,

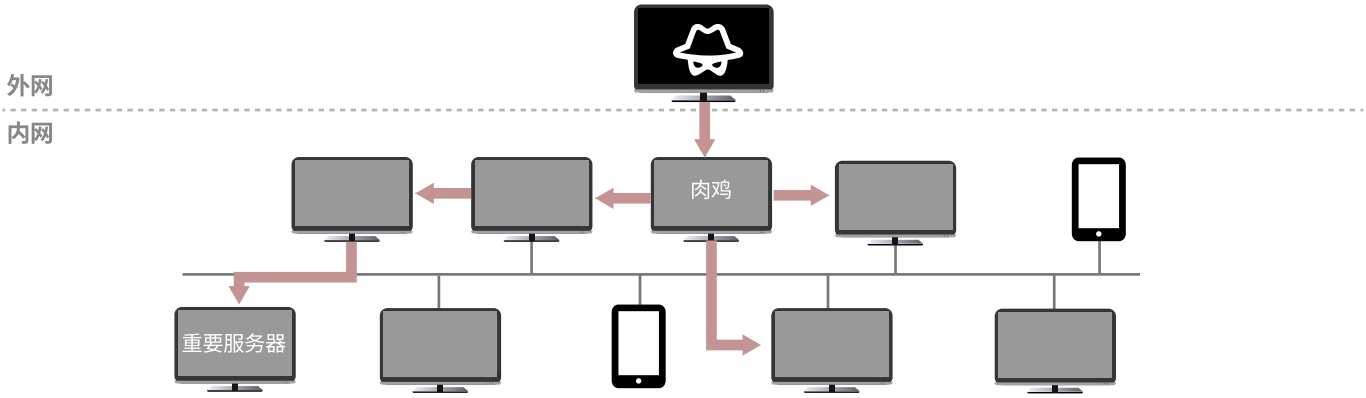
Para lo dé su conocimiento, nos permitimos informarle que nuestro sistema de información inteligente ha detectado que el estado de su declaración de renta con la dirección de impuestos y aduanas nacionales **DIAN** se encuentran en mora de 180 dias por este motivo se ha determinado proceder conforme lo estipula la ley Art.823 hasta 843-2.

Adjuntamos la información y su deuda a la fecha con una clave la cual es : dian

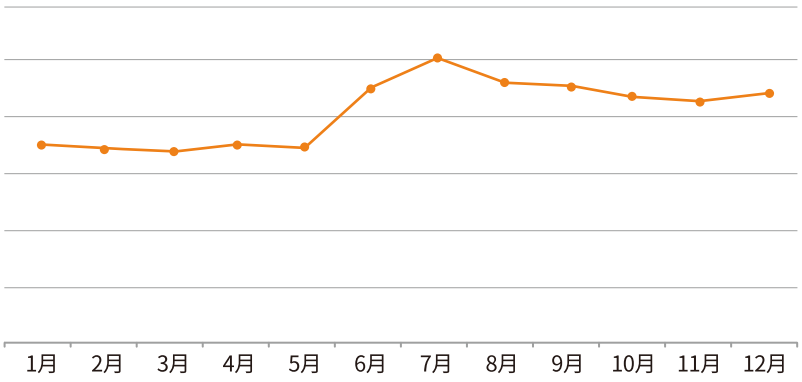
图:一封冒充哥伦比亚国家税务海关总局的电子邮件

五、横向渗透攻击

横向渗透攻击是指黑客以已经被入侵的部分主机为跳板，利用横向渗透技术，攻陷其他相关网络和设备进一步获取邮箱、密码、文件等隐私数据和资源，从而实现控制整个内网。也就是说黑客利用横向渗透手段，可以实现“由点到面”的攻击，达到使内网沦陷的目标。



数据显示，2021年横向渗透攻击呈现上升趋势。黑客利用默认共享和远程WMI调用进行横向渗透攻击为主，分别占比53%和27%。正因为默认共享等系统自带的功能容易被利用，所以常被黑客、病毒利用在内网进行横向渗透攻击，比如知名的DTStealer、WannaMine等蠕虫病毒，均是用了此类攻击方式，在企业内进行传播。



2021年横向渗透攻击趋势

黑客一旦从外网进入目标局域网控制某一个终端，就可以利用同一局域网的信任关系，如共享权限、密码、凭据等，入侵其它终端，做更大范围的渗透攻击，由点到面，不断获取并控制高价值的目标终端，最终穿透整个局域网。

更具威胁的是，横向渗透还是组合攻击的标配。如与勒索病毒、后门程序、蠕虫病毒等高危病毒合作，实施加密文件索要赎金的行为，榨取目标用户更多利益；另外，横向渗透还是APT攻击（高级可持续性威胁）攻击方常用的“战术”之一。

火绒安全响应服务

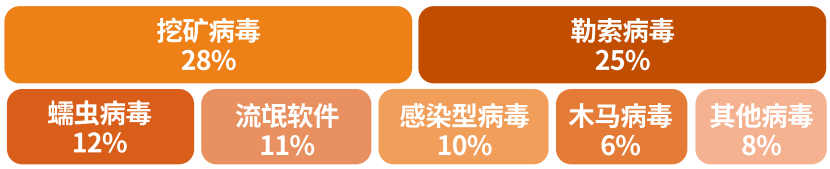
火绒安全响应服务通过处置具体的安全事件或线索，帮助企业发现更多潜在的威胁，做到早发现、早防御、早处置。而针对客户的紧急安全事件也可以提供及时的技术支持，并提供更符合实际场景的防护方案。

2021年全年，火绒安全响应服务团队累计为用户提供6000余次安全响应服务，分析并处置了包括高危病毒、漏洞、恶意软件在内的各类终端威胁。

一、企业用户

1、病毒攻击年末进入高峰期

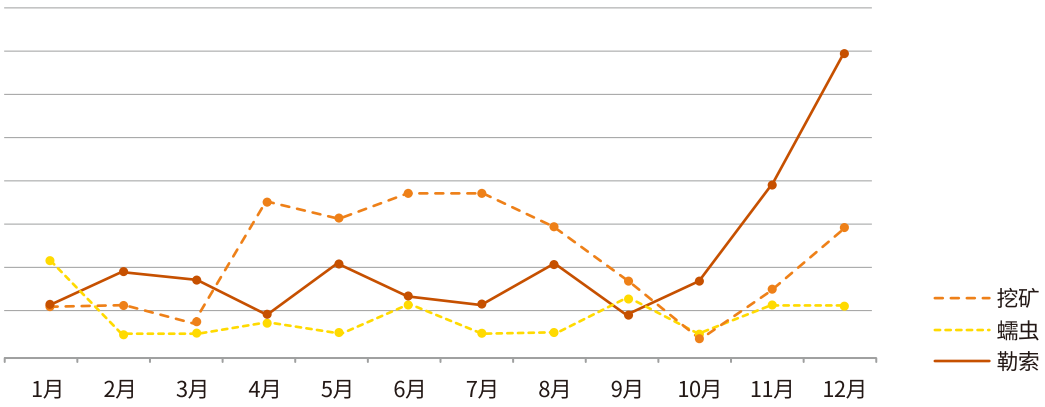
2021年火绒安全响应服务团队累积为企业用户提供应急响应2637次。根据“火绒在线支持和响应中心”统计的数据显示，企业用户遭遇的病毒类攻击中，以挖矿病毒、勒索病毒、蠕虫病毒等类型为主，分别占据攻击总数的28%、25%和12%。



企业终端常见病毒占比

从占比前三的病毒攻击趋势来看：

- (1) 挖矿病毒集中在3月到9月份爆发，或与“疫情”影响下企业复产复工有所关联。
- (2) 蠕虫病毒全年表现较为稳定，仅在1月份因“incaseformat蠕虫病毒事件”出现短暂的爆发，具体可见后文“典型应急响应事件”。
- (3) 勒索病毒则在稳定活跃大半年后，在9月份后变为快速上升趋势。
- (4) 三大类型病毒均在10月份后呈现快速上升趋势，并在年末到达峰值。



2021年企业常见病毒攻击趋势

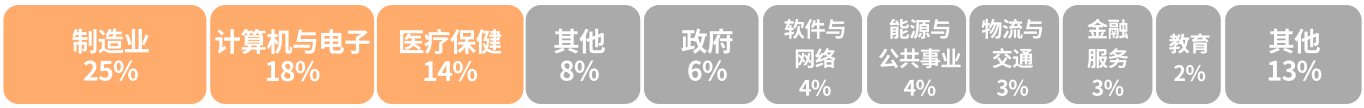
2、企业内网常见病毒情况

火绒安全实验室分析发现，在企业内网中持续传播的病毒类型中，感染型病毒最为常见，其次为蠕虫病毒和黑客工具。此类病毒和恶意程序凭借隐蔽的传播特性，可长期感染、驻留在企业内网中，难以被用户发现。即使发现病毒也会出现“不敢杀”、“不会杀”的局面，最终任由病毒四处扩散，威胁终端安全。根据“火绒威胁情报系统”监测和评估，感染型病毒中Synares、Ramnit两大家族感染终端数量均超过数百万。企业内网常见病毒占比情况如下图：

企业内网常见病毒占比情况

3、各行业遭遇安全事件情况

从各行业遭遇的安全事件占比来看，制造业遭遇的安全事件最多，占据火绒安全响应服务企业总数的25%，紧随其后的是计算机与电子行业和医疗保健行业，分别占据总数的18%、14%。

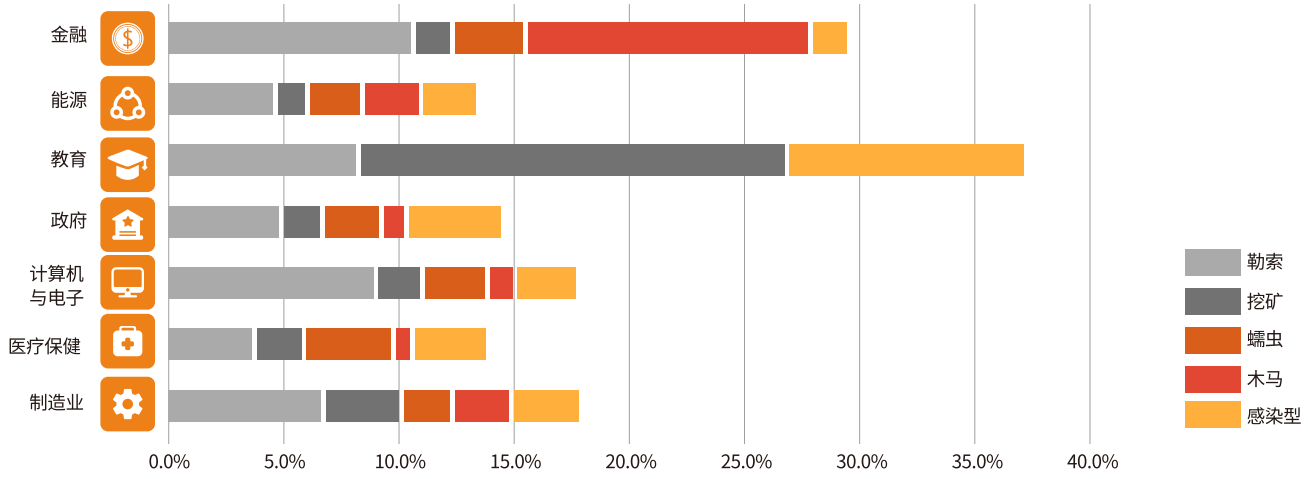


各行业遭遇的安全事件占比

4、各行业遭遇的病毒类型情况

从主要病毒活跃样本在各行业的占比来看：

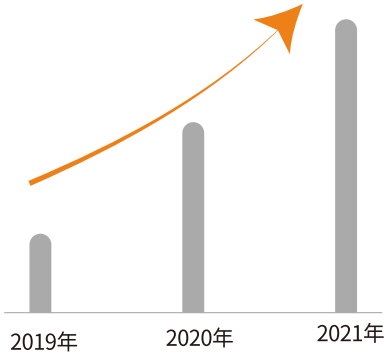
- (1) 勒索病毒在各行业均有较高的比重，受影响行业前三分别为金融行业、计算机与电子行业、教育行业。
- (2) 除勒索病毒外，金融行业中木马病毒占比最高；医疗行业、制造业中蠕虫病毒占比最高。
- (3) 教育行业遭遇的病毒类型中，勒索病毒、挖矿病毒、感染型病毒占比均较高。由于学校网络复杂，校园网、互联网之间相互连接，在使用终端时容易带来病毒入侵的风险。教育行业的终端安全亟待加强。



各行业遭遇病毒类型占比

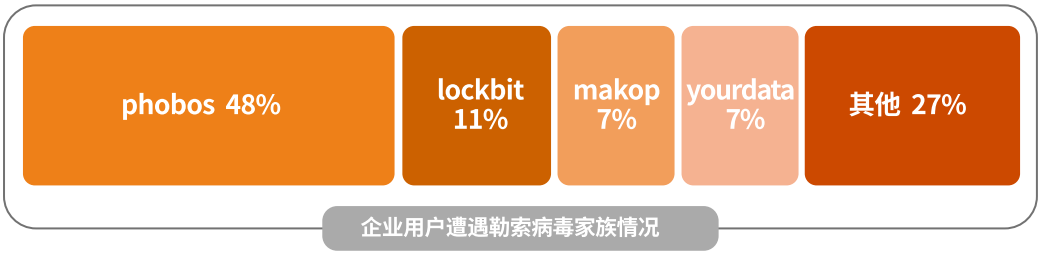
5、勒索病毒持续对企业发起攻击

企业用户近三年遇到的勒索病毒一直呈上升趋势。这其中，除了Web服务漏洞、横向渗透等攻击方式不断增加和更新外，企业的高价值资料、信息也更具备勒索价值，促使黑客主要以企业作为入侵和勒索的目标。



企业用户近三年遭遇勒索病毒攻击情况

火绒安全实验室对企业遭遇的勒索病毒进行分类发现，以希腊恐惧之神命名的Phobos勒索病毒家族发起的攻击最多。目前，勒索软件通过RaaS（勒索软件即服务）的形式在黑市被广泛出售，这意味着，即使是不懂技术的购买者也可以成为勒索病毒的投放者；甚至一些勒索病毒会在用户提供赎金后，附赠企业的漏洞信息，变得愈发商业化。



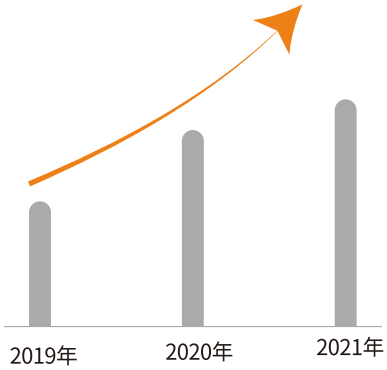
企业用户遭遇勒索病毒家族情况

事实上，2021年中，勒索病毒还在全球范围内不断发起攻击，包括计算机、航空、政府、能源、零售等不同行业均受到波及。部分被攻击的企业在未支付赎金的情况下，其内部信息也被攻击者直接公开，造成严重的经济损失。2021年全球范围内企业遭遇勒索病毒攻击主要案例如下：

- 3月，计算机巨头企业遭 REvil 勒索病毒入侵
- 4月，华盛顿警察局被勒索攻击
- 5月，美国最大成品油管道运营商被勒索软件攻击
- 7月，意大利拉齐奥大区遭RansomEXX勒索软件攻击
- 8月，曼谷航空遭到LockBit勒索软件攻击
- 11月，欧洲零售巨头MediaMarkt遭勒索攻击
- 12月，全球最大的照片服务公司Shutterfly遭勒索病毒攻击

6、挖矿病毒利用漏洞攻击，危及Linux系统

除勒索病毒以外，挖矿病毒同样是企业面临的主要威胁之一。虽然挖矿病毒并不会像勒索病毒一样使得业务瘫痪，但会严重影响终端性能，造成电脑卡慢，不仅降低员工办公效率，还会挤占企业服务器运算资源，最终影响整个企业的生产制造。



企业用户近三年遭遇挖矿病毒攻击情况

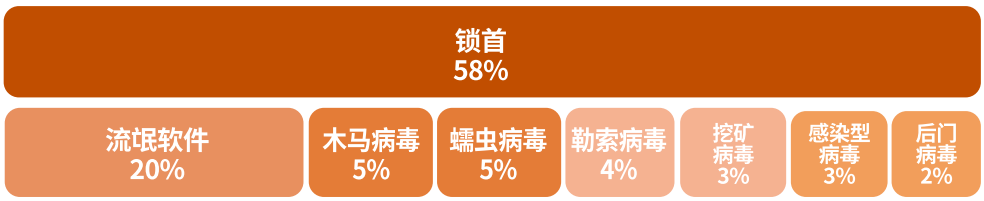
火绒安全实验室在对企业遭遇的挖矿病毒进行研究时发现，企业终端常见的挖矿病毒以DTStealer和WannaMine、Mykings三大家族为主。

DTStealer以Windows和Linux系统为感染目标，尤其是对于Linux系统还可以通过漏洞发起攻击，包括：Yarn未授权访问漏洞、Redis未授权访问漏洞、WebLogic（CVE-2020-14882）、Elasticsearch（CVE-2015-1427）、Solr（CVE-2019-0193）、Docker（Remote API）。

WannaMine可在局域网内，通过SMB快速横向扩散。由于利用了“永恒之蓝”漏洞攻击，所以被攻击的终端除了卡顿外，还有可能出现蓝屏现象。

二、个人用户

与企业用户遭遇的病毒威胁不同的是，劫持首页与流氓软件依旧是侵害个人用户的主要问题。根据“火绒在线支持和响应中心”统计的数据显示，锁首、流氓软件等问题占据火绒响应个人用户服务总数的四分之三，已远远超过其它常见病毒。



个人用户遭遇的安全事件占比

1、锁首问题持续影响个人用户

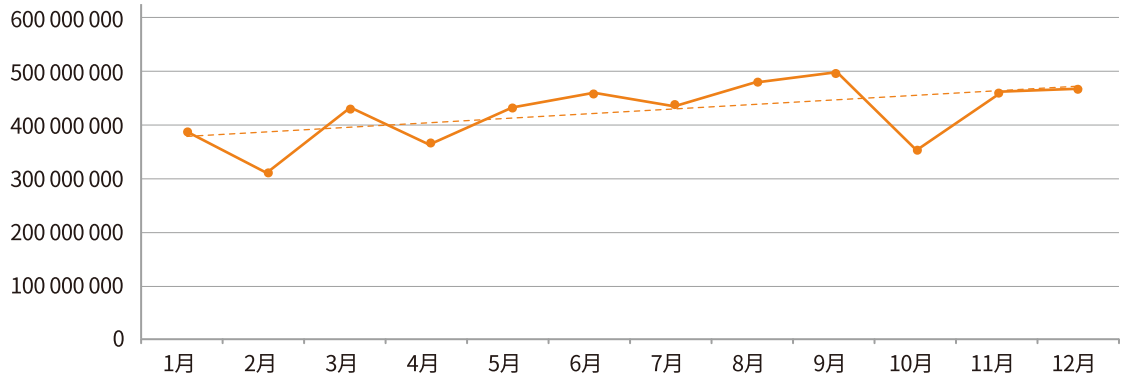
浏览器作为互联网主要入口，承载了巨大的用户流量和商业利益，正因如此，也吸引了众多不良厂商与病毒团伙将目光瞄向其中，通过劫持用户的浏览器首页，获取流量和不当利益。

通常情况下，锁定用户浏览器首页的方式有很多，包括利用驱动、通过修改配置及快捷方式、流氓软件劫持等等，这些方式多数都是通过恶意软件或浏览器插件完成的，用户一般很难发现被锁定的原因。

锁首带来最直接的影响，一是强迫用户改变使用习惯，剥夺了用户自由使用浏览器的权益；二是可能会带来其他病毒入侵等安全风险。

2、弹窗拦截全年累计45亿次

根据“火绒威胁情报系统”监测和评估，2021年中，火绒安全共拦截（不含用户手动拦截）45亿次拦截弹窗。近几年，随着《互联网广告暂行办法》等相关规定与每年两会期间对弹窗问题的关注，以及央视等主流媒体的持续披露报道，虽然在以往弹窗行为最疯狂的“618”、“双11”等电商购物节期间，没有出现短时间内爆发的状态。但从全年拦截情况查看，弹窗广告依旧是主要侵扰用户的流氓行为之一。

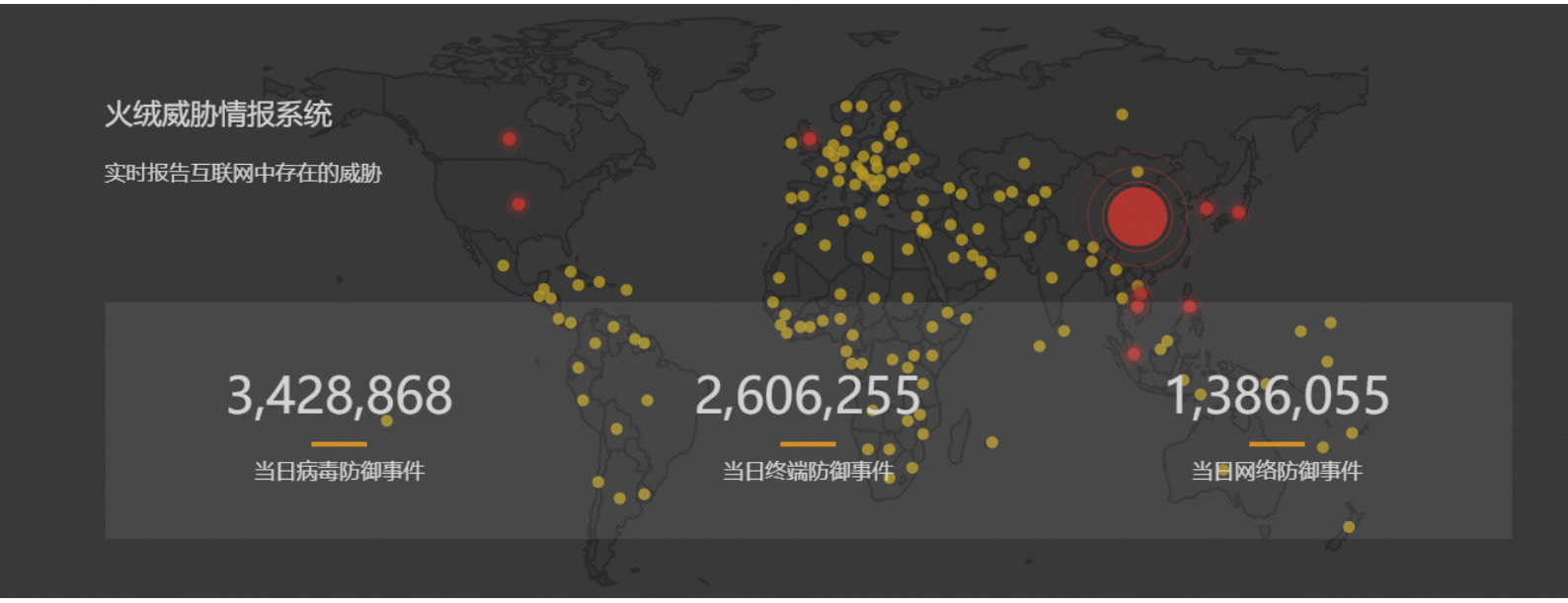


2021年弹窗广告拦截情况

火绒安全防护体系

一、火绒安全威胁情报

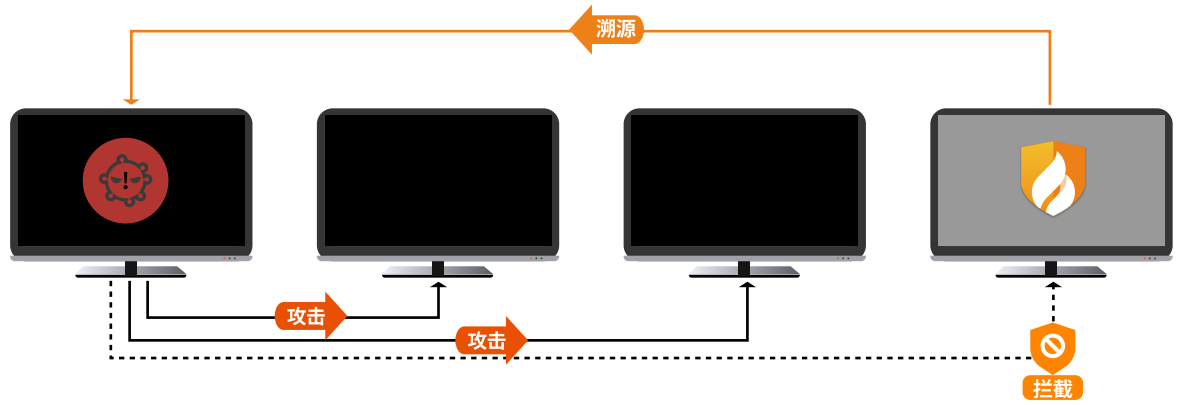
“火绒威胁情报系统”基于遍布互联网的个人用户终端为探针，实时监控全网可疑威胁，并对可疑样本及时分析，通过升级解决方案，巩固产品安全防护能力，做到将威胁处理时间前置，避免用户陷入被动。



二、攻击检测与防护

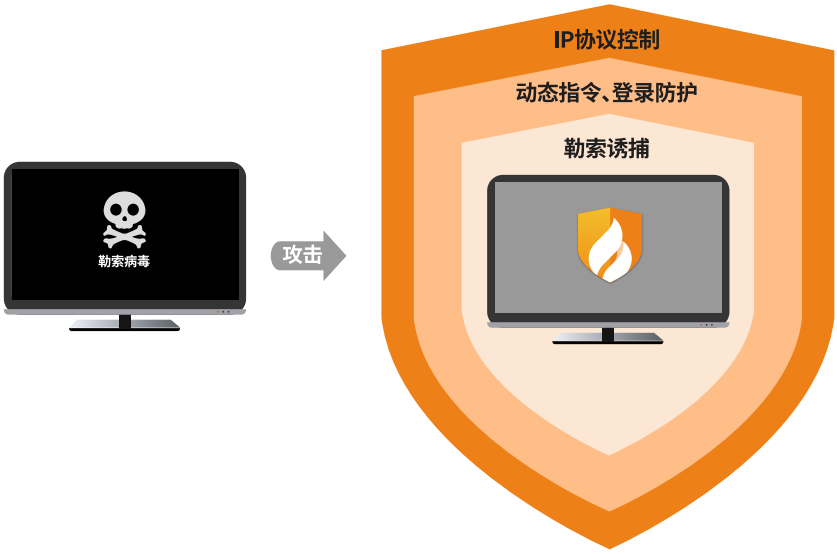
1、溯源攻击 彻底查杀挖矿、蠕虫病毒

对于挖矿、蠕虫等传染性强的病毒，火绒安全在查杀、拦截之外，还可溯源攻击源头，帮助用户彻底清除网络中的病毒，防止重复感染。



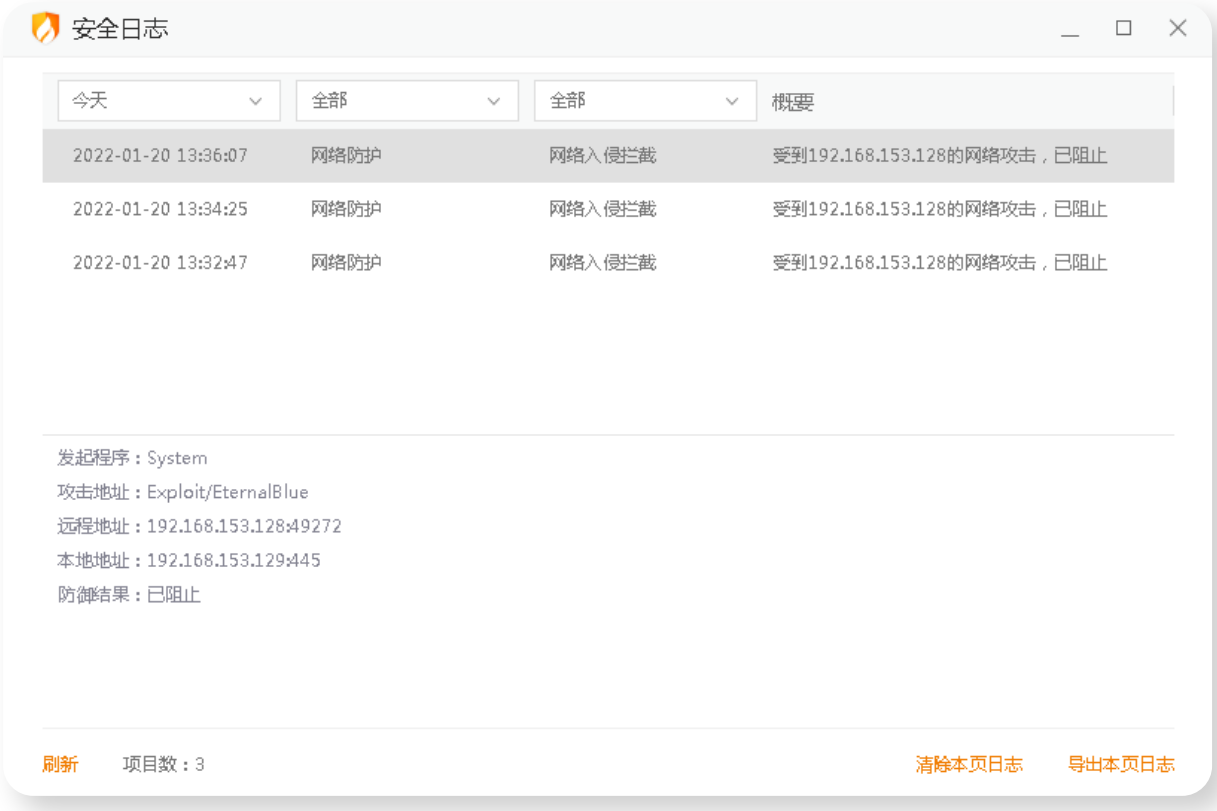
2、加固识别 层层拦截勒索病毒

火绒安全对勒索病毒除了识别与查杀，还通过层层设防的方式，封堵病毒可能潜入终端的渠道。【勒索诱捕】功能利用诱捕文件发现勒索病毒；【远程登录防护】、【终端动态口令】功能加强远程入侵防护；【IP协议控制】功能对高危端口进行管控，避免成为突破口。



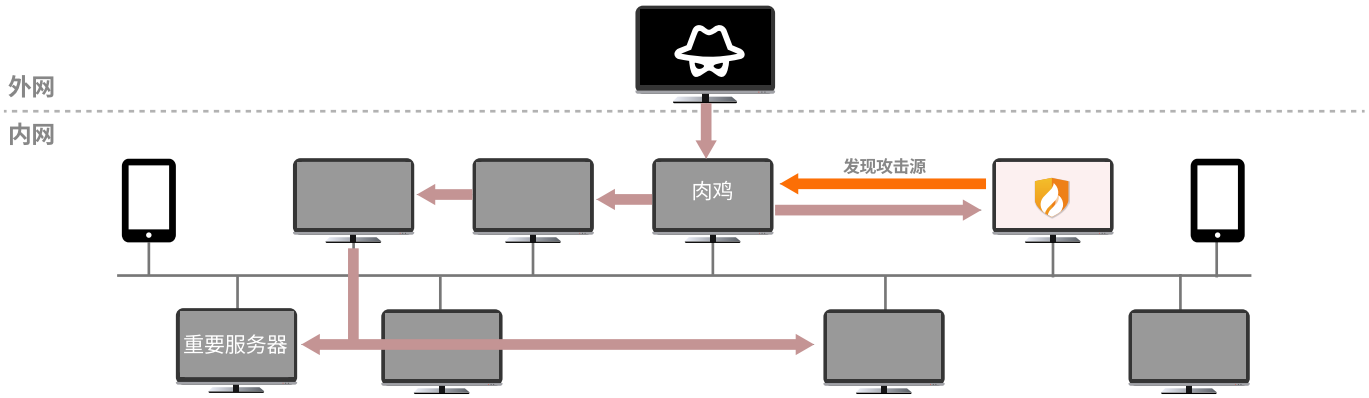
3、拦截修复 封堵漏洞攻击缺口

一方面，火绒安全时刻关注微软等厂商披露的漏洞信息，第一时间向用户推送修复补丁；另一方面，加强对已有漏洞的拦截，通过热补丁的形式拦截漏洞攻击，溯源攻击源头。



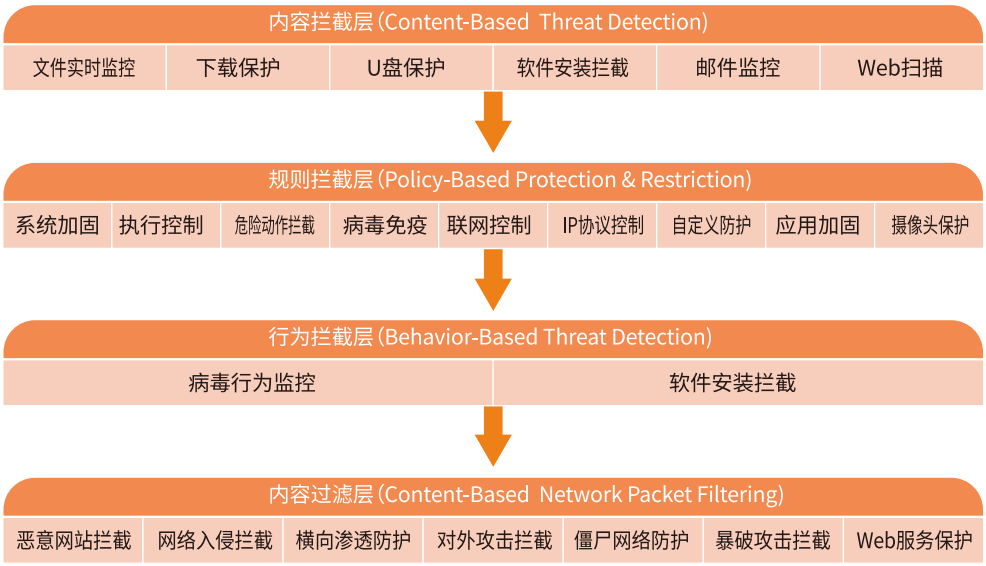
4、严防死守 阻断横向渗透

【横向渗透防护】能够阻止病毒、黑客利用共享和远程调用等形式，在企业内部造成大面积攻击。



5、纵深防护 拦截钓鱼攻击

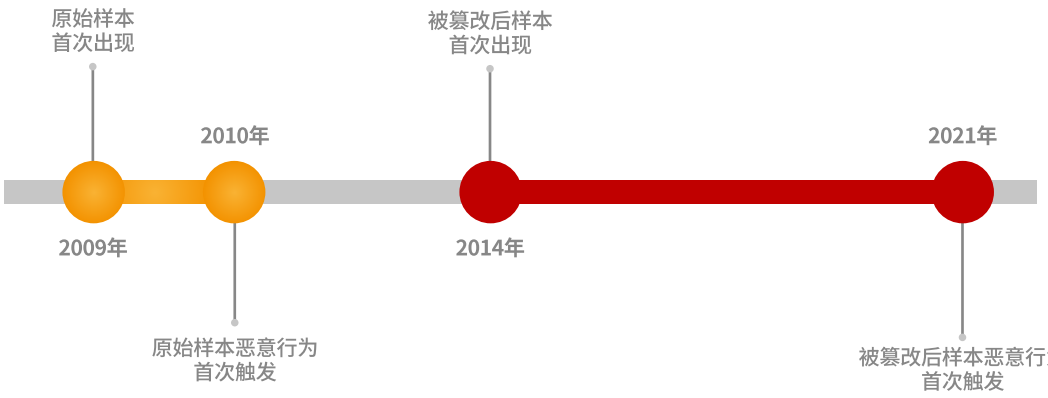
火绒安全构建了完善的纵深防护体系，可从内容拦截、规则拦截、行为拦截三个角度，充分阻止钓鱼邮件带来的鱼叉式攻击、恶意PDF威胁。



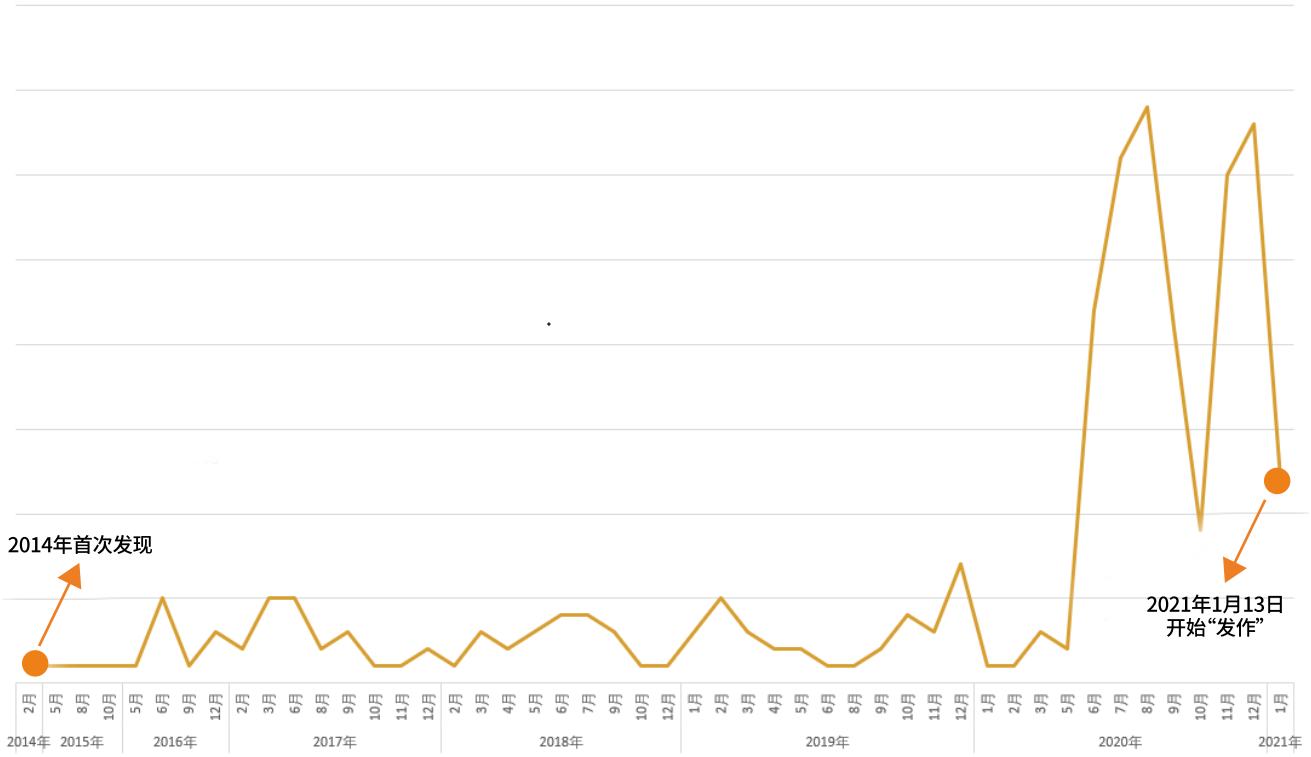
三、典型应急响应

1、incaseformat蠕虫病毒定时爆发事件

2021年1月13日，incaseformat蠕虫病毒在全网集中爆发，用户中毒后将被删除C盘以外所有文件。火绒安全实验室立即对该事件进行安全响应，通过样本溯源、病毒分析、时间梳理，发布多篇详细报告，最终发现这是一起精心策划的投毒事件。



根据火绒安全实验室分析，该病毒存在至少两个变种。推测第一个变种为原作者所做的原始病毒，最早可追溯至2009年，其爆发时间为2010年4月1日。从仅一年的潜藏时间和选择的爆发日期（愚人节）来看，不排除是原作者测试病毒的可能性。第二个则为黑客篡改后的变种，最早可追溯至2014年，并被设置在2021年1月13日爆发。



被篡改后的病毒增长趋势

对比两个变种病毒可以发现，两者在核心代码逻辑中仅有一处数据被篡改。这种篡改的方式极其细微隐蔽，更像是精心策划，目的或是为了引导病毒分析人员误以为病毒程序出现bug，增加潜伏的机会，以便继续扩散危害。

同时，通过深度溯源可以发现，在此前关于该病毒事件的众多分析报告中，不同厂商对该病毒的追溯日期偏差（包括2009年、2014年等）实际上源自对该病毒两个不同变种的混淆。实际上，火绒安全基于自主研发的反病毒引擎，能够同时查杀两个变种的全部样本。

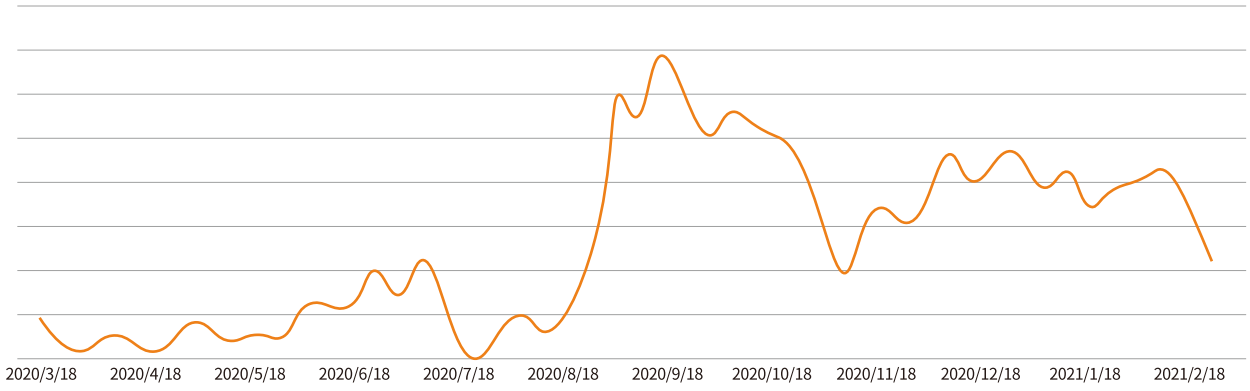
2、Apache Log4j2漏洞爆发事件

12月9日，Apache Log4j2反序列化远程代码执行漏洞（CVE-2021-44228）细节被公开，攻击者可利用该漏洞构造恶意请求，触发远程代码执行，影响范围广泛。火绒安全第一时间对该漏洞进行响应，推出修复该漏洞的热补丁，并推荐用户使用火绒安全的“Log4j2漏洞缓解工具”以进行风险自查和处置。

Log4j2漏洞细节被公开以来，火绒安全持续高度关注，并发现大量疑似利用此漏洞进行攻击的事件。除挖矿、僵尸网络外，“TellYouThePass”勒索病毒短时间内密集的对包含此漏洞的OA系统进行攻击，相关OA、WEB服务等均有沦陷可能。火绒安全在确保对病毒进行查杀的同时，第一时间升级防御方案并推送给所有火绒用户，确保不受漏洞、病毒的影响。

3、多起病毒攻击链针对企业用户事件

根据“火绒威胁情报系统”监测发现，在2021年中出现多起黑客入侵企业服务器后下载并执行后门病毒的威胁事件。火绒安全实验室溯源发现，黑客通过弱口令等方式入侵服务器后，通过SQL Server等服务启动cmd.exe来执行PowerShell脚本，最终下载运行上述后门病毒程序。而该后门病毒疑似为Quasar RAT的变种（一款国外开源远控工具），具备下载、执行、上传、信息获取与记录等常见的远程控制功能，对用户特别是企业单位具备严重安全威胁。火绒安全对该系列事件进行总结分析并发布报告提醒企业用户注意防范。



终端受影响趋势

附:部署火绒安全产品后巡检参考

防病毒情况

检查控制中心首页界面在线终端数量,确认是否有用户私自卸载了客户端,中心是否设置防卸载密码。

资产管理

检查终端是否安装了娱乐游戏等不符合公司规定的软件,可以下发卸载通知。

检查客户端是否变更过硬件信息,可以在硬件变更日志中查看。

策略部署

在终端用户电脑查看策略同步情况,是否有未连接中心情况出现。

检查中心是否设置定时任务,在终端空闲时间段进行病毒查杀或者漏洞修复。

检查中心策略中是否开启勒索病毒诱捕功能,增强对勒索病毒的防护。

检查中心策略中是否开启远程登录防护功能,防止企业内机器被远程植入病毒。

检查一些重要服务器是否开启终端动态认证功能,可以在服务器被登录或者被远程的时候进行二次验证。

检查中心策略中是否对一些高危端口进行控制,防止被黑客利用攻击。

检查企业员工和服务器的密码是否为不少于八位的强口令,防止被黑客利用进行暴力破解导致安全问题。

设备管理

检查中心是否对终端的外接设备进行管控,比如U盘,有线无线网卡等设备,防止U盘在企业内部进行病毒传播。

邮件预警

检查中心是否开启邮件预警功能,在终端电脑遭受病毒风险事件时、遭受网络攻击时、超过一周未更新时是否对管理员发送通知邮件。

邮件收发

检查是否开启邮件保护功能,对员工收发的邮件进行检测,防止不当操作导致文件被加密等隐患。

漏洞修复

检查是否有客户端中存在大量高危漏洞未修复,导致可能被黑客利用攻击。

事件日志

检查事件日志中终端的防病毒情况,对一些易受攻击的终端添加特殊的防护规则。

查看安全分析报告,定期了解全网的安全态势,及时作出防护措施。

火绒安全
HUORONG SECURITY

聚焦专业技术 专注终端安全

查看最新
安全行业资讯

试用有礼
安全报告下载

公 司:北京火绒网络科技有限公司
地 址:北京市朝阳区红军营南路15号瑞普大厦D座4层
网 址:https://www.huorong.cn

电 话:400-998-3555