安全事件通告

黑客利用聊天软件漏洞植入剪贴板木马窃取比特币

360CERT
北京奇虎科技有限公司 | 2021-04-23

报告信息

报告名称	黑客利用聊天软件漏洞植入剪贴板木马窃取比特币		
报告类型	安全事件通告	**报告编号**	B6-2021-042301
报告版本	1	**报告日期**	2021-04-23
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

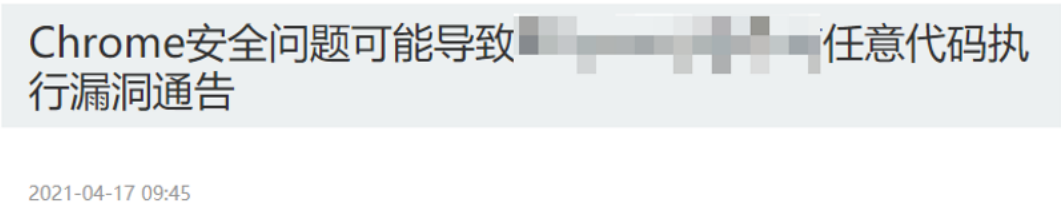
报告修订记录

报告版本	日期	修订	审核	描述
1	2021-04-23	360CERT	360CERT	撰写报告

目录

一、事件简述

近日，某聊天软件被曝存在高危漏洞，攻击者可以通过该聊天软件发送一个特制的 web 链接，用户一旦点击链接，聊天软件便会加载执行攻击者构造恶意代码，最终使攻击者控制用户 PC。出现该问题后，该聊天软件也马上做了更新，通过新版本解决了该问题。



就在漏洞曝出第二天，360 安全大脑监就测到有疑似使用该聊天软件漏洞，下发执行剪切板劫持木马的攻击。从文件时间戳(2021-04-18 22:18:55)看，该木马在漏洞曝出后进行编译。执行时持续监控剪贴板数据，替换其中的比特币钱包地址，企图通过这种方式让受害者在不知觉的情况下向木马替换后的钱包地址进行转账。

二、攻击过程

攻击者会挑选特定目标用户发起攻击，像这些用户群发钓鱼链接，当有用户不慎在 PC 端打开时，攻击即被触发。

攻击者利用该漏洞，通过聊天软件进程下发并执行剪贴板木马。攻击发起时的进程树如下图:

三、 剪贴板木马分析

该木马执行后即开始工作，每隔 300 毫秒检查一次剪贴板中数据，如果发现内容长度大于 25 则进行比特币钱包地址的搜索和替换。

搜索比特币地址方式是字符串首字母为'1'、'3'、'b'、'0'的位置。这次所发现的木马对其中 3 种格式的地址进行替换，包括'1'开头的传统地址、'3'开头的 P2SH 地址、'0x'开头的以太坊地址。

```
i = data;
while ( *data != '1' && *data != '3' && *data != 'b' && *data != '0' && *data )// 1、3、bc1、0x特征匹配
  ++data;
if ( *data && lstrlenW(data) > 25 )
{
  if ( *data != '0' || data[1] != 'x' )
  {
    if ( *data == '1' || *data == '3' )// 剪贴板头部为'1'或'3'
    {
      j = 0;
      for ( i = data; ; ++i )
```

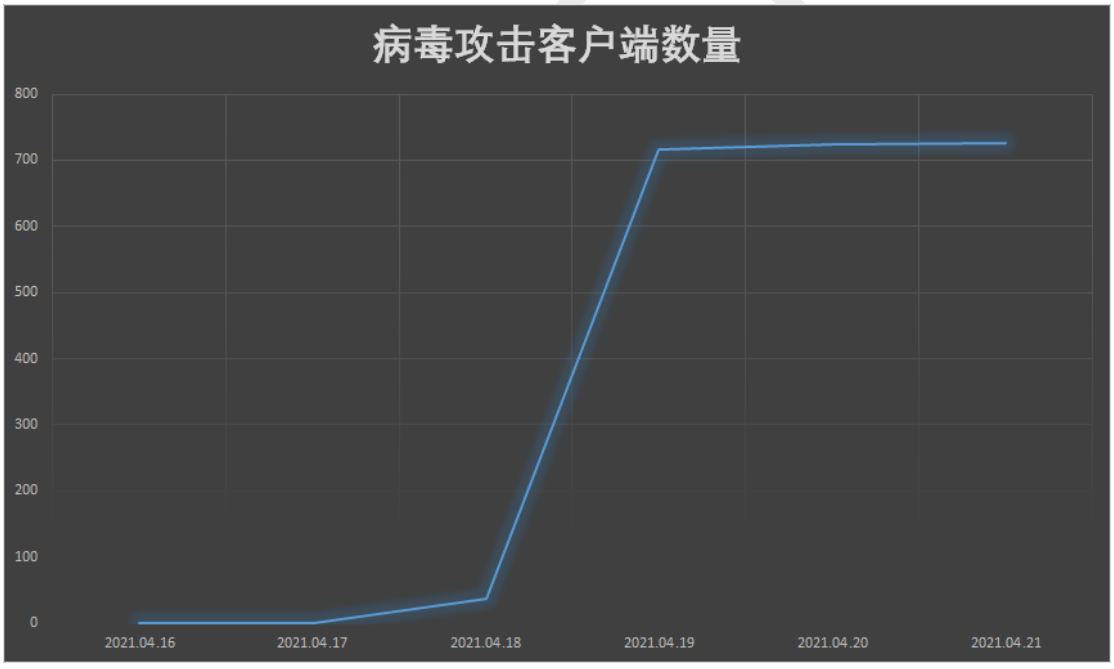
如果发现粘贴板内容能够匹配上之后，即对内容中的地址字符串进行替换，木马内置了大量钱包地址，从中随机选择。含有传统地址和 P2SH 地址各 25 个，以太坊地址 15 个。（我们在分析中发现，由于木马随机算法问题，三个地址列表中的后 2 个地址无法被使用到）。

```
if ( isalphanum )
{
  v13 = _isInReplaceBTCAddrList(data_1);
  if ( !v13 )                   // 剪切板中原始钱包地址字符串不在替换地址列表中
  {
    j = 0;
    v28 = 0;
    if ( v19 )
    {
      for ( j = 0; ; ++j )
      {
        if ( j >= 60 )
          goto LABEL_65;
        v24 = rand() % 23;      // 随机选择列表中地址
        if ( _hasBeenSetBM[v24] )
          v24 = rand() % 23;
        else
          hasBeenSetBM[v24] = 1;
```

木马内置钱包地址如下

```
.data:00403108                 dd offset a7d88656d943770 ; "7D88656d9437703aA14aD500b86eD4015745BaC"...
.data:0040310C                 dd offset a5ea560585e9168 ; "5eA560585e91689E1f0708Abca96Ae0ec3307D1"...
.data:00403110                 dd offset a3398969cd62c0d ; "3398969cd62C0d8511bDbAc46410BD4ab61C3Ba"...
.data:00403114                 dd offset aAb3d1a7e89f370 ; "ab3d1a7e89F370e5b3cEcffC734290d8eDc86d3"...
.data:00403118                 dd offset aBf2c3effcdc09f ; "Bf2c3eFFCdc09FF11E8288B07c06c403386E8C8"...
.data:0040311C                 dd offset unk_403FD8
.data:00403120 a94jre2pcpfhgtb db '94jrE2PCpFhgTbDXRtHdkMr8V9GbRQgak',0
.data:00403120                                         ; DATA XREF: .data:off_403010↑o
.data:00403142                 align 4
.data:00403144 aBdtggmkkjsz8pp db 'BDtgGmkKJSZ8PPGv4MUWeYBzFL17ouiNE',0
.data:00403144                                         ; DATA XREF: .data:00403014↑o
.data:00403166                 align 4
.data:00403168 aQdock6psukx6gu db 'QDocK6psuKX6gUkRUMh8tThN5N1jXVrkD',0
.data:00403168                                         ; DATA XREF: .data:00403018↑o
.data:0040318A                 align 4
.data:0040318C a2uxrxwrqs1kaxi db '2uXRXwrqs1KaxiQbbLvLRqJoP7vMHkJJD',0
.data:0040318C                                         ; DATA XREF: .data:0040301C↑o
.data:004031AE                 align 10h
.data:004031B0 a7inxpqu9nk8spr db '7inXPQu9nk8sPR5f2Ddzz2AwtXVagPR3z',0
.data:004031B0                                         ; DATA XREF: .data:00403020↑o
.data:004031D2                 align 4
.data:004031D4 aP19cco7qckracx db 'P19CCo7qckRacxdULr7xuecs4PXVqmNGf',0
.data:004031D4                                         ; DATA XREF: .data:00403024↑o
.data:004031F6                 align 4
.data:004031F8 a2opjtqeu4b4w13 db '2opjTQEU4B4W13PE9TPSGTLj2qRwCC9qg',0
.data:004031F8                                         ; DATA XREF: .data:00403028↑o
.data:0040321A                 align 4
.data:0040321C aDhkvzdwndnq4mh db 'DHKVzdWndNQ4MHDouKbgyg6rQeD8w3oPo',0
```

从 4 月 18 号初次出现至今，已有大量用户受到该木马影响：



四、 360 安全大脑查杀拦截

360 安全大脑建议用户，尽快将聊天软件升级至最新版，解决该漏洞问题。

使用 360 安全产品的用户也无需担心，360 安全卫士已增加对该漏洞攻击的防护，并且早在 2018 年就已推出区块链防火墙，抵御此类剪贴板木马攻击。

当用户在进行加密货币交易时，开启“区块链防火墙”功能后，如果剪贴板中“银行卡号”被篡改，360 安全产品就会弹出警示窗口。360 安全大脑建议币圈人士，都安装并开启该功能。

五、 IOCs

MD5

16529046ab84cf9addb74cfd76dbab89

六、 产品侧解决方案

(一) 360AISA 全流量威胁分析系统

针对微软本次安全更新，360AISA 已基于流量侧提供对应检测能力更新，请 AISA 用户联系 techsupport@360.cn 获取更新，尽快升级检测引擎和规则，做好安全防护工作。

(二) 360 企业安全浏览器

360 企业安全浏览器相比传统浏览器，360 企业安全浏览器兼集中管控、企业数据防护、安全大脑赋能、跨平台适配、商用密码算法支持、应用兼容等六大特点。请用户前往 360 企业安全浏览器获取对应产品。

(三) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。

(四) 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn)获取对应产品。

(五) 360 安全卫士

Windows 用户可通过 360 安全卫士实现对应补丁安装、漏洞修复、恶意软件查杀，其他平台的用户可以根据修复建议列表中的安全建议进行安全维护。

360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

(六) 360 安全卫士团队版

用户可以通过安装 360 安全卫士并进行全盘杀毒来维护计算机安全。360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

(七) 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

(八) 360 终端安全管理系统

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危

评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危