

教育行业 GandCrab 勒索病毒应急处置方案



360 企业安全集团

2019 年 03 月

目录

一、病毒事件概述.....	3
二、样本分析情况.....	4
三、日志分析情况.....	7
四、病毒传播方式.....	8
五、紧急处置方案.....	9
六、病毒检测工具.....	10
七、360 应急响应联络方式.....	11

一、病毒事件概述

随着信息技术在教育行业的广泛应用和深度融合，在教育系统、教育设备、教育环境等纷纷融入信息化元素的同时，也加大了攻击者对于教育行业相关教育数据的关注程度和攻击面，使支撑教育教学的底层网络系统、业务系统等在网络安全面临的威胁也持续加大。黑客入侵教务管理平台窃取或倒卖学生学籍信息、篡改学校网站造成不良影响、植入勒索病毒到大量校园网电脑终端等信息安全事件逐渐增多，部分案例甚至造成了很大的社会影响。

近日，360 企业安全收到多起遭受 GandCrab5.2 版本勒索病毒攻击事件反馈，如广东省某中学，江苏省某教育发展中心。经分析此次病毒木马涉及到多个变种，传播途径多样包括 WebLogic 漏洞、CVE-2019-7238,NexusRepository Manager 3 远程代码执行漏洞、钓鱼邮件、网页挂马等。

例如，在某攻击邮件中会发送如下内容：

邮件标题为“你必须在 3 月 11 日下午 3 点向警察局报到!”

发件人邮箱为：Jae-hyun@idabostian.com

发件人名称：Min,Gap Ryong

如图：



运行附件内的恶意软件后，可以确认是 GandCrab V5.2 版本：

```
TERUPLOAR-MANUAL.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
---=  GANDCRAB V5.2  =---
*****UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED***
      *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****
Attention!
All your files, documents, photos, databases and other important files are encrypted and have the extensio
The only method of recovering files is to purchase an unique private key. Only we can give you this key an
The server with your key is in a closed network TOR. You can get there by the following ways:
-----
| 0. Download Tor browser - https://www.torproject.org/
| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser:  http://gandcrabmfe6mnef.onion/532f3a30447af9
| 4. Follow the instructions on this page
-----
```

GandCrab 勒索病毒家族在国内传播广泛，曾使用鱼叉邮件、U 盘蠕虫、感染压缩包、下载器、远程桌面爆破、永恒之蓝、Web 服务器漏洞等各种方式传播，在 GandCrab V5.2 版本病毒的传播途径中又开启了网页挂马方式，据 360 威胁情报中心监测显示，精心构造的挂马网站会通过色情站点等广告联盟渠道进行传播，对访客实施网页挂马攻击。当 GandCrab 被执行后会对计算机内的文件进行高强度的加密，并需要限时支付赎金后才能恢复被加密的文件。由于不能获得作者的解密密钥，目前的加密实现上也还未找到可利用的漏洞，故 GandCrab v5.2 版本暂时没有免费的解密方法和工具。

根据本次事件特征分析，除已受到攻击单位外，其它同类型单位也面临风险，需积极应对，Gandcrab 5.1 之前版本的解密工具：<http://lesuobingdu.360.cn>。

二、样本分析情况

与 5.1 版本相比，变化不大。此次更新的 GandCrab V5.2 版本，与之前 5.1 版本的更新幅度不大，主要是更新了外层免杀处理，其两个版本的花指令混淆方式保持一致。

```

.text:00405021
.text:0040502F
.text:0040502F public start
.text:0040502F start proc near
.text:00405030 push ebx
.text:00405031 push esi
.text:00405032 push edi
.text:00405032 loc_405032: ; 000E XREF: start+10 ↓ j
.text:00405032 mov ecx, 1C3D2h
.text:00405037 call near ptr loc_405046+1
.text:0040503C loc_40503C: ; CODE XREF: start+15 ↓ j
.text:0040503C cmp ecx, 1FEFF58h
.text:00405042 js short near ptr loc_405032+2
.text:00405044 jns short near ptr loc_40503C+2
.text:00405046 loc_405046: ; CODE XREF: start+8 ↑ p
.text:00405046 jmp near ptr 126454CEh
.text:00405046 start endp
.text:00405046 ;
.text:0040504B db 0E2h
.text:0040504C dd 6AE8EFh, 26E8h
.text:00405054 db 0, 0CCh

```

图表 GandCrabs.2

```

.text:00405716
.text:00405716
.text:00405716 public start
.text:00405716 start proc near
.text:00405716 push ebx
.text:00405717 push esi
.text:00405718 push edi
.text:00405719 loc_405719: ; CODE XREF: start+13 ↓ j
.text:00405719 mov ecx, 1C3D2h
.text:0040571E call near ptr loc_40572D+1
.text:00405723 loc_405723: ; CODE XREF: start+15 ↓ j
.text:00405723 cmp ecx, 1FEFF58h
.text:00405729 js short near ptr loc_405719+2
.text:0040572B jns short near ptr loc_405723+2
.text:0040572D loc_40572D: ; CODE XREF: start+8 ↑ p
.text:0040572D jmp near ptr 126458B5h
.text:0040572D start endp
.text:0040572D ;
.text:00405732 dw 0EFE2h
.text:00405734 dd 0E8006AE8h, 3D7h
.text:0040573C db 0CCh

```

图表 GandCrabs.1

病毒执行后，首先会进行终端信息收集，包括：计算机用户名、用户组、安装的杀软信息、系统版本、ip 地址、磁盘类型、磁盘剩余空间等：

```

v27 = DeCryptString((int)&v131); // pc_user
v121 = 0x7B267779;
v122 = -249847676;
v123 = -950319233;
v124 = -1760918377;
v125 = 2069082035;
v126 = 2069082019;
v127 = 1221002813;
v128 = 1077006204;
v129 = -1748159570;
v130 = -901509939;
v28 = DeCryptString((int)&v121); // pc_name
v90 = -530986268;
v91 = -1851372857;
v92 = -243998503;
v93 = 1408596251;
v94 = 437395641;
v95 = 437395627;
v96 = 1826413077;
v97 = 2053965931;
v98 = -2065167685;
v99 = 1741002718;
v100 = -102;
v29 = DeCryptString((int)&v90); // pc_group
v176 = -1095885809;
v177 = -462747406;
v178 = 85920836;
v179 = 274459673;
v180 = 2086624375;
v181 = 2086624369;
v182 = 1889622316;
v183 = 20881;
v30 = DeCryptString((int)&v176); // av

```

此次 5.2 版本的提权手法与 5.1 保持一致,使用 wmi、CVE-2018-8120、CVE-2018-8440 漏洞进行提权。

```

if ( !GetSystemVer() || (unsigned int)sub_40C3D9() > 0x1000 )// 判断系统版本是否为win7 且是否为system帐户
{
    if ( !sub_40105E() && sub_405000() ) // 判断区域排除 并且尝试打开互斥体BitHunder.
        // 如果打开失败则创建, 如果打开成功则不进行后续加密逻辑
    {
        sub_402105(); // 结束进程
        sub_401C10();
        InitializeCriticalSection(&CriticalSection);
        InitializeCriticalSection(&stru_4185E4);
        InitializeCriticalSection(&stru_4185FC);
        sub_4038CC();
        DeleteCriticalSection(&stru_4185FC);
        DeleteCriticalSection(&CriticalSection);
        DeleteCriticalSection(&stru_4185E4);
        sub_404C50();
        IF ( (unsigned int)sub_40C3D9() < 0x4000 )
        {
            lpAddress = 0;
            if ( sub_40C6A9((LPWSTR *)&lpAddress) )
            {
                v21 = lpAddress;
                v22 = (void (__thiscall *) (int, signed int, _DWORD, LPVOID, signed int))GetProcAddress_stub(
                    3,
                    -1671519418);
                v22(v23, 20, 0, v21, 3);
                VirtualFree(lpAddress, 0, 0x8000u);
            }
        }
        v24 = (int (__thiscall *) (int, _DWORD, _DWORD, void (__noreturn *)(), _DWORD, _DWORD, _DWORD))GetProcAddress_stub(1, 1874369264);
        if ( !v24(v25, 0, 0, sub_406E13, 0, 0, 0) )
            WaitForSingleObject(0, 0xFFFFFFFF);
        sub_406E13();
    }
    sub_40527C();
    sub_403E40(); // wmic启动自身提权
}

```

```

MEMORY[ 0x2C ] = v22 - 4;
MEMORY[ 0x14 ] = v23;
sub_40D2CC(&v45, 348);
v45 = v24;
v46 = v24;
v47 = 384;
v48 = 43981;
v49 = 6;
v50 = 0x10000;
v51 = 75497984;
v85 = &v45;
sub_40DC77(&v45);
vBits = 0;
pvBits = (int *)((char *)v84 + v72);
v89 = sub_40E471;
SetBitmapBits(hbm, 4u, &pvBits);
v25 = hbit;
GetBitmapBits(hbit, 4, &vBits);
SetBitmapBits(v25, 4u, &v89);
v26 = (HMODULE)HIDWORD(v65);
strcpy(v90, "NtQueryIntervalProfile");
v27 = GetProcAddress((HMODULE)HIDWORD(v65), v90);
dword_418684 = (int)v27;
if ( !v27 )
{
    v27 = GetProcAddress(v26, v90);
    dword_418684 = (int)v27;
    if ( !v27 )
        goto LABEL_25;
}
((void (__cdecl *)(signed int, int *)v27)(4919, &v53);
SetBitmapBits(v25, 4u, &vBits);

```

创建线程加密本地磁盘文件

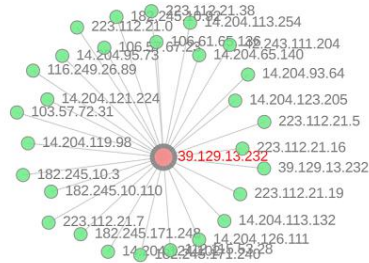
```

{
    LOBYTE(v21) = *((_BYTE *)lpAddress + v6);
    v22 = v6 + 1;
    v9 = VirtualAlloc_Stub(8u);
    v10 = (void (__stdcall *)(_DWORD *, int *))GetProcAddress_Stub(1, 749073254);
    v10(v9, &v21);
    v9[1] = a1;
    CreateThread = (int (__stdcall)(_DWORD, _DWORD, void (__cdecl __noreturn *) (LPVOID), _DWORD *, _DWORD, _DWORD));
    v12 = CreateThread(0, 0, sub_401F22, v9, 0, 0); // 创建线程加密本地磁盘文件
    v13 = v20;
    v4 = v16;
    v5[v20] = (HANDLE)v12;
    v7 = v13 + 1;
    v14 = i-- == 1;
    v20 = v7;
    if ( v14 )
        break;
    v6 = v22;
    ++v8;
}
while ( v8 < v4 );

```

三、日志分析情况

通过 RDP 远程桌面攻击服务器，可以关联分析出如下图所示情况：



四、病毒传播方式

目前已知的传播方式如下：

1. 定向鱼叉攻击邮件投放；
2. 垃圾邮件批量投放传播；
3. 网页挂马攻击；
4. 利用 CVE-2019-7238(NexusRepository Manager 3 远程代码执行漏洞)进行传播；
5. 利用 WebLogic CVE-2017-10271 漏洞进行传播；
6. 利用自动化机制病毒进行传播
(<https://mp.weixin.qq.com/s/R-Ok96U5Jb2aaybUfsQtDQ>)：
 - a) 通过 RDP、VNC 等途径进行爆破并入侵；
 - b) 利用 U 盘、移动硬盘等移动介质进行传播；
 - c) 捆绑、隐藏在一些破解、激活、游戏工具中进行传播；

7. 感染 Web/FTP 服务器目录并进行传播主要传播端口为：445、135、139、3389、5900 等端口。

五、紧急处置方案

结合教育部关于防范勒索病毒攻击的相关通知要求，针对此类病毒应急处置方案建议如下：

【紧急处置】

1. 控制已发现被攻陷主机，采取措施防止蔓延：下线已发现招攻陷主机，扫描暴露到公网的主机和端口、紧急关停。
2. 摸清楚受害主机范围，对中招主机进行处置：通过天眼网络流量分析、天擎病毒扫描或漏洞扫描等方式，筛查出受害主机范围，对中招主机下线然后查杀，及时升级服务程序并安装相应补丁。

【未感染主机与加固】

1. 在网络边界防火墙上全局关闭 3389 端口或只对特定 IP 开放。
2. 开启 Windows 防火墙，尽量关闭 3389、445、139、135 等不用的端口。
3. 避免使用弱口令，每台服务器设置唯一口令，且复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15 位、两种组合以上）。
4. 在 windows 中禁用 U 盘的自动运行功能，不打开来历不明的邮件。
5. 安装天擎防病毒（带防爆破功能）和服务器加固，及时更新病毒库。

6. 如用户处存在虚拟化环境 建议用户安装 360 网神虚拟化安全管理系统，进一步提升防恶意软件、防暴力破解等安全防护能力。
7. 升级邮件系统的防护策略，部署邮件安全检测防护系统，对勒索邮件、钓鱼邮件予以检测和拦截。
8. 部署流量监控设备，开展全流量深度分析工作，以及时发现安全攻击事件，并可对攻击事件在流量中进行追踪溯源。

六、病毒检测工具

对于 GandCrab V5.2 变种文件，360 天擎可以查杀以及拦截：相关联的所有样本已于 3 月 3 日--- 13 日 在 360 云安全中心加黑，联网客户无需升级病毒库即可支持对该病毒的查杀；隔离网用户也不必恐慌，在 3 月 13 日例行病毒库升级之后即可有效查杀所有已知变种。



此外，天擎文档防护功能有效拦截病毒的加密行为，即使用户没来得及升级病毒库，也不会受其影响。



七、360 应急响应联络方式

360 各省建立应急响应接口人，联系方式如下：

省份	接口人姓名	电话
广东省	李双喜	13168307188

360 企业安全集团提供 7*24 小时全天候应急响应服务 求助电话：4008 136

360 转 2 转 4。