信息系统安全周报

亚信安全客户服务中心

感谢您订阅由亚信安全客户服务中心撰写的《信息系统安全周报》。
我们竭诚为您提供最新的安全资讯、病毒流行趋势、系统漏洞提示及网络安全防护技巧。

病毒情报中心		系统漏洞信息
一周病毒情况报告 亚信安全热门病毒综述- Backdoor.Win64.CARBANAK.A		KB4493448
系统安全技巧		**亚信安全产品**
MegaCortex 勒索病毒预警		病毒码发布情况

一周病毒情况报告

本周用户报告感染数量较多的病毒列表

- BKDR_VOOLS 家族

亚信安全热门病毒综述

亚信安全热门病毒综述- Backdoor.Win64.CARBANAK.A

该病毒由其它恶意软件生成或者用户访问恶意网站不经意下载感染本机，其会监听 445 端口，执行远程恶意用户发送的命令，其还会利用如下漏洞：

- CVE-2013-3660
- CVE-2013-5065
- CVE-2014-4113

- 对该病毒的防护可以从下述链接中获取最新版本的病毒码：15.105.60
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 病毒详细信息请查询：
  https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/backdoor.win64.carbanak.a

系统漏洞信息

Windows 安全更新 (4493448)

Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1

描述：https://portal.msrc.microsoft.com/zh-cn/security-guidance

亚信安全产品

病毒码发布情况

亚信安全在最近一周发布中国区病毒码情况如下：

2019 年 05 月 06 日发布病毒码 14.979.60
2019 年 05 月 07 日发布病毒码 14.981.60
2019 年 05 月 08 日发布病毒码 14.983.60
2019 年 05 月 09 日发布病毒码 14.985.60
2019 年 05 月 10 日发布病毒码 14.987.60

截至目前，病毒码的最高版本为 15.105.60 发布于 2019 年 05 月 13 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/

趋势科技在最近一周发布全球病毒码情况如下：

2019 年 05 月 06 日发布病毒码 14.981.00
2019 年 05 月 07 日发布病毒码 14.983.00
2019 年 05 月 08 日发布病毒码 14.985.00
2019 年 05 月 09 日发布病毒码 14.987.00
2019 年 05 月 10 日发布病毒码 15.101.00

截至目前，病毒码的最高版本为 15.107.00，发布于 2019 年 05 月 13 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/TSUT/

系统安全技巧

近日，亚信安全网络监测实验室监测到新型勒索病毒 MegaCortex 正在美国、加拿大等多地区传播，该病毒攻击目标为大型企业，其通过域控服务器下发勒索病毒，加密后的文件扩展名为.aes128ctr。与以往勒索病毒不同的是，本次勒索赎金不要求受害者支付加密货币，而是要求受害者购买他们的软件。亚信安全将其命名为 RANSOM.WIN32.CORTEX.SM。

病毒感染流程

✓ 病毒首先获得域控制器的访问权限，然后将其配置为向网络上的其他计算机分发批处理文件和 PsExec(恶意软件的主要可执行程序之一)；

✓ 通过 PsExec 远程运行批处理文件，目的是终止 Windows 进程，并停止和禁用干扰勒索软件例程的服务；

```
taskkill /IM zoolz.exe /F
taskkill /IM agntsvc.exe /F
taskkill /IM dbeng50.exe /F
taskkill /IM dbsnmp.exe /F
taskkill /IM encsvc.exe /F
taskkill /IM excel.exe /F
taskkill /IM firefoxconfig.exe /F
taskkill /IM infopath.exe /F
taskkill /IM isqlplussvc.exe /F
taskkill /IM msaccess.exe /F
taskkill /IM msftesql.exe /F
taskkill /IM mspub.exe /F
taskkill /IM mydesktopqos.exe /F
taskkill /IM mydesktopservice.exe /F
taskkill /IM mysqld.exe /F
taskkill /IM mysqld-nt.exe /F
taskkill /IM mysqld-opt.exe /F
taskkill /IM ocautoupds.exe /F
taskkill /IM ocomm.exe /F
taskkill /IM ocssd.exe /F
taskkill /IM onenote.exe /F
taskkill /IM oracle.exe /F
taskkill /IM outlook.exe /F
taskkill /IM powerpnt.exe /F
taskkill /IM sqbcoreservice.exe /F
taskkill /IM sqlagent.exe /F
taskkill /IM sqlbrowser.exe /F
taskkill /IM sqlservr.exe /F
taskkill /IM sqlwriter.exe /F
taskkill /IM steam.exe /F
taskkill /IM synctime.exe /F
taskkill /IM tbirdconfig.exe /F
taskkill /IM thebat.exe /F
taskkill /IM thebat64.exe /F
taskkill /IM thunderbird.exe /F
taskkill /IM visio.exe /F
```

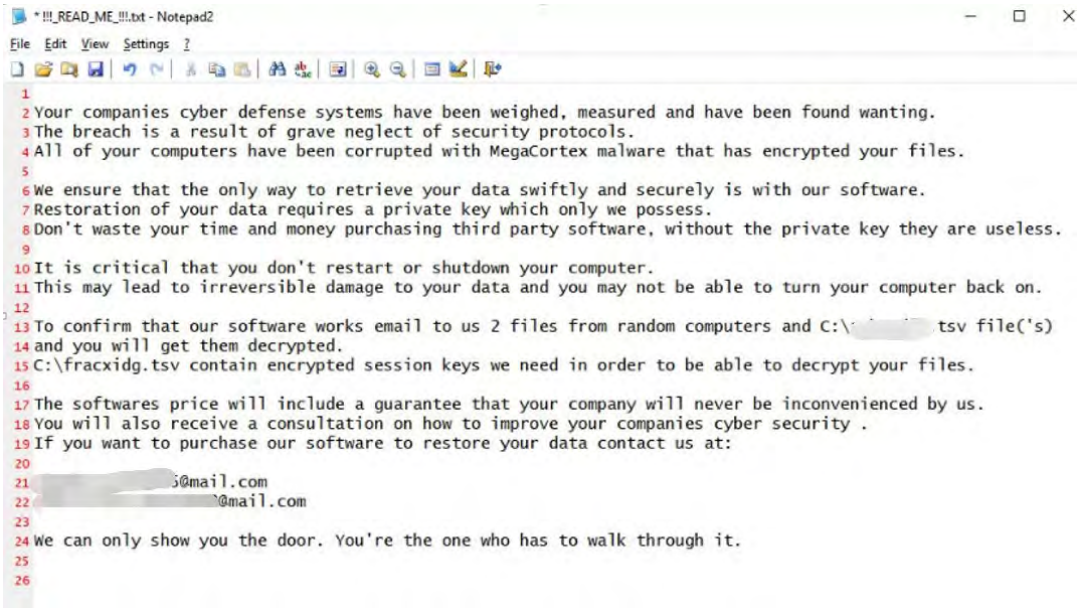
- ✓ 执行核心恶意程序 winnit.exe 后，其会提取一个随机命名的 DLL 文件，然后使用 rundll32.exe 执行它，该 DLL 负责加密计算机中的文件。

```
sc config VeeamTransportSvc start= disabled
sc config W3Svc start= disabled
sc config wbengine start= disabled
sc config WRSVC start= disabled
sc config MSSQL$VEEAMSQL2008R2 start= disabled
sc config SQLAgent$VEEAMSQL2008R2 start= disabled
sc config VeeamHvIntegrationSvc start= disabled
sc config swi_update start= disabled
sc config SQLAgent$CXDB start= disabled

iisreset /stop
c:\windows\temp\winnit.exe [redacted]==
```

- ✓ 勒索软件还会在硬盘中生成一个扩展名为.tsv 的文件，该文件包含加密秘钥。

- ✓ 最后，勒索病毒生成赎金通知文件!!! _ READ_ME _ !!!.txt，与以往不同的是，本次勒索赎金不要求受害者支付加密货币，而是要求受害者购买他们的软件。



【MegaCortex 勒索病毒提示信息】

解决方案

- ✓ 尽量关闭不必要的端口，如：445、135，139 等，对 3389，5900 等端口可进行白名单配置，只允许白名单内的 IP 连接登陆；
- ✓ 尽量关闭不必要的文件共享；
- ✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
- ✓ 不要点击来源不明的邮件以及附件；
- ✓ 浏览网页时不下载运行可疑程序；
- ✓ 及时更新系统，更新应用程序；打全系统及应用程序补丁程序；
- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案：

- ✓ 亚信安全病毒码版本 14.985.60，云病毒码版本 14.985.71，全球码版本 14.987.00 已经可以检测，请用户及时升级病毒码版本。

总结

MegaCortex 勒索病毒正在美国、加拿大等多地区传播，不排除在全球传播可能性。亚信安全提醒广大用户，提高警惕，做好勒索病毒防护工作。

IOC

81bb640d960fd68869a569f40835447971e7b235