Salinity

Download (aka Conficker)

This six years old worm exploits the MS08-067 vulnerability in Windows. It spreads over the Internet and through removable media and network shares.
Windows threat landscape is filled with existing malware families—some of which has been around for years, being kept alive by unpatched machines.

### Top-10 detections

<table>
<thead>
<tr>
<th>Detection</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>DownAdup/Conficker</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-based attacks</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Java</td>
<td></td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

Rounded up by...

- Sality
- Ramnit
- Autorun
- Wormlink
- Browser Exploit
- Expiro
- Zeroaccess

### Android Malware

Android continues to be a favorite target for majority of the mobile threats. But threats directed towards iOS do exist, even if there are far fewer of them.

- **294 families or variants**
- **1 new family**

**Top-3 Android families**

- SMSSend
  - Large family of malware that sends SMS messages to premium-rate numbers.
- Fakeinst
  - Appears to be app installers, but sends SMS messages to premium-rate numbers.
- Eropl
  - Silently harvests data from the device and forwards it to a remote server.

**Top-3 demanding ransom**

- Koler: First ransomware (almost)
  - Mobile extension of the 'police-themed' Reveton ransomware. Claims to encrypt files on device, but actually only disables the Back button to keep the ransom demand prominent.
- Slocker: First TOR-encrypted ransomware
  - Encrypts image, document and video files on device; disables the Back button to interfere with user's control. Communicates with controlling server via Tor network or SMS messages.
- Oleg Pliss strikes Australia
  - In May, 'Oleg Pliss' locks the accounts of a number of users in Australia, reportedly using the 'Find My iPhone' feature, and demands ransom. Apple denies speculation of a breach in the iCloud service.
I remember setting up our first website. That was 20 years ago, in 1994. When the Web was very young and there were only a handful of websites, it was easy to forecast that the Web was going to grow. And indeed, during these past 20 years, it has exploded in size. What’s even more important, the Web brought normal everyday people online. Before the Web, you would only find geeks and nerds online. Now everybody is online.

Back in 1994, we were guessing what would fuel the upcoming growth of the Web. For it to grow, there has to be online content—content like news or entertainment. And for news and entertainment to move online, somebody has to pay for it. How would users pay for online content? We had no idea. Maybe newspapers would start charging an annual online subscription fee, just like they did for their paper version? Or maybe the web would incorporate some kind of an online on-demand payment system; the user would have an easy way of doing in-browser micropayments in order to access content. This would enable the user pay, say, one cent to read today’s Dilbert cartoon.

As we know now, such a micropayment system never happened—even though it looked like such an obvious thing 20 years ago. Instead, a completely different way of paying for online content surfaced: ads. I remember seeing the first banner ad on a website, maybe in 1995 or 1996. I chuckled at the idea of a company paying money for showing their ad on someone else’s website. I should not have chuckled; that same idea now fuels almost all of the content online. And highly efficient ad profiling engines create practically all the profit for companies like Google and Facebook.

Google is a particularly good example of just how profitable user profiling can be. Its services—like Search, Youtube, Maps and Gmail—are free. You don’t pay a cent for using them. These services are massively expensive to run: Google’s electricity bill alone is more than $100 million a year. You would think that a company that runs very expensive services but doesn’t charge for them would be making losses—but it isn’t. In 2013, Google’s revenue was $60 billion. And their profit was $12 billion. So, if we make a modest estimate that Google has one billion users, every user made 12 dollars of profit for Google last year—without paying a cent.

Frankly, I’d be happy to pay Google $12 a year to use their services without tracking or profiling. Heck, I would be ready to pay $100 a year! But they don’t give me that option. We—the users—are more valuable in the long run by having our data and our actions profiled and saved.

Of course, Google is a business. And they are doing nothing illegal by profiling us—we volunteer our data to them. And their services are great. But sometimes I wish things would have turned out otherwise and we would have a simple micropayment system to pay for content and services. Now, with the rise of cryptocurrencies, that might eventually become a reality.
GAME OVER?

The disruption of the GameOver ZeuS (GOZ) botnet by multiple law enforcement agencies[1] was a great success in many ways — but what’s next? The botnet was disrupted but not completely destroyed. Its creator was not arrested, is still at large and is currently building a new botnet to replace the old.

Why disrupt GOZ?
CryptoLocker[2], a powerful ransomware trojan dropped by GOZ, was undoubtedly a big reason why the botnet was targeted for takedown. CryptoLocker, with its ability to perfectly encrypt all the documents and data files on its victim’s hard drive, was too sinister. There was no cure other than to pay the ransom for the decryption key. So the only way to stop the scheme was to prevent it. And as GOZ delivered CryptoLocker — GOZ was targeted for a takedown.

Escalation
CryptoLocker is exactly the reason why it is so dangerous to disrupt (but not completely takedown) a botnet such as GameOver ZeuS. Ask yourself this:

“If CryptoLocker was so successful, why didn’t Slavik (GOZ’s botmaster) deploy the ransomware across his entire botnet?”

The obvious answer: because then he wouldn’t have a botnet anymore. All two million bots couldn’t drop CryptoLocker without also destroying GOZ’s infrastructure at the same time.

But what if the infrastructure is already lost due to a takedown? What prevents a future version of GOZ from initiating a “self-destruct” order (like dropping an encryption bomb) if the bot doesn’t communicate with its C&C server within a set period of time? Nothing.

Evolution
The story of computer malware is one of evolution. And that evolution is driven by a predator-prey dynamic. Each time the hunter discovers the quarry — a new defense tactic is required to avoid detection. What happens if the next defense tactic is to become poisonous?

The hunters should be wary.

“What happens if the next defense tactic is to become poisonous?”

SOURCES

by
Sean Sullivan
Security Advisor
F-Secure Labs
<table>
<thead>
<tr>
<th>INCIDENTS CALENDAR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DIGITAL FREEDOM</strong></td>
</tr>
<tr>
<td><strong>ATTACKS</strong></td>
</tr>
<tr>
<td><strong>Yahoo! attack prompts password reset</strong></td>
</tr>
<tr>
<td><strong>Wireless home/office routers hacked</strong></td>
</tr>
<tr>
<td><strong>Flexcoin Bitcoin bank robbed, folds</strong></td>
</tr>
<tr>
<td><strong>Windigo attack infects Linux servers</strong></td>
</tr>
<tr>
<td><strong>Jan</strong>: Passwords stolen from ‘third party’ database used to access Mail accounts</td>
</tr>
<tr>
<td><strong>Tech giants release FISA request data</strong></td>
</tr>
<tr>
<td><strong>TrustyCon conference held in protest</strong></td>
</tr>
<tr>
<td><strong>Windows XP reaches official end of life (EOL)</strong></td>
</tr>
<tr>
<td><strong>eBay forces password change after attack</strong></td>
</tr>
<tr>
<td><strong>Feb</strong>: Google, Facebook and others post summaries of requests made by US govt</td>
</tr>
<tr>
<td><strong>Spyeye malware author pleads guilty in US</strong></td>
</tr>
<tr>
<td><strong>2 plead guilty to Android app piracy</strong></td>
</tr>
<tr>
<td><strong>US charges 9 for Zeus malware</strong></td>
</tr>
<tr>
<td><strong>Australia arrests 2 for ‘Anon’ hacks</strong></td>
</tr>
<tr>
<td><strong>Jan</strong>: Russian national created and distributed malware used for wire, bank fraud</td>
</tr>
<tr>
<td><strong>GAMEOVER ZEUS BOTNET</strong></td>
</tr>
<tr>
<td><strong>Mar</strong>: Starts stealing Bitcoin wallets and their encryption passwords</td>
</tr>
<tr>
<td><strong>MALWARE</strong></td>
</tr>
<tr>
<td><strong>New, improved ransomware planned</strong></td>
</tr>
<tr>
<td><strong>GameOver Zeus starts stealing Bitcoins</strong></td>
</tr>
<tr>
<td><strong>TheMoon Worm spreading on routers</strong></td>
</tr>
<tr>
<td><strong>Coremax extension does browser hijacking</strong></td>
</tr>
<tr>
<td><strong>Jan</strong>: Security researchers report on development of new PowerLocker DIY kit</td>
</tr>
<tr>
<td><strong>iOS updates released to fix major SSL flaw</strong></td>
</tr>
<tr>
<td><strong>Active attacks using new IE 0-day bug</strong></td>
</tr>
<tr>
<td><strong>Flash Player 0-day hit by driveby attacks</strong></td>
</tr>
<tr>
<td><strong>Word 0-day used in targeted attacks</strong></td>
</tr>
<tr>
<td><strong>Feb</strong>: SLL vulnerability could allow attackers to intercept traffic between users</td>
</tr>
</tbody>
</table>
**NSA reportedly plants backdoors in routers**  
*May*: Exported products intercepted, modified for covert eavesdropping

**Iraq blocks social media due to ISIS threat**  
*Jun*: Moved aimed at ‘disrupting insurgents communications’

**Thailand junta blocks sites, censors reporting**  
*Jun*: Hundreds of sites reportedly blocked, forbids critical media reports

**Youtube, Twitter access restored in Turkey**  
*Jun*: Youtube unblocked, follows lifting of ban on Twitter last month

**Heartbleed exploited to hack VPN session**  
*Apr*: NYT reports attackers used flaw to enter targeted firm’s network

**AU-CERT reports rise in cyber attacks**  
*May*: Report says 56% of firms surveyed reported cyber attacks

**TrueCrypt warns software now ‘harmful’**  
*May*: Drive-encryption project says tool ‘not secure’, warns against use

**Massive DDoS attack hits Hong Kong**  
*Jun*: 300Gbps+ attack on voting system after civic referendum

**MyBulletins launched to ease updating flow**  
*May*: Service intended to simplify identifying applicable security updates

**Google debuts ‘right to be forgotten’ form**  
*May*: EU court rules search engine to remove ‘irrelevant’ links on request in EU

**Google Apps add encryption**  
*May*: End-to-end email encryption offered to enterprise users

**Reset the Net campaign launched**  
*Jun*: Coalition of groups aim to encourage use of surveillance-resistance tools

**US wants 5 Chinese hackers for espionage**  
*May*: Dept of Justice claims PLA members hacked US businesses for 8 years

**Almost 100 arrested for Blackshades trojan**  
*May*: Arrests in US, EU & other countries for sale of trojan used to spy on users

**‘Oleg Pliss’ hackers arrested in Moscow**  
*Jun*: Russian Interior Ministry says arrested 2 for iOS ransom attacks in Oz

**FBI hunts for Gameover Zeus mastermind**  
*Jun*: Indictment against Russian national issued following botnet takedown

**Virus Shield app scam in Play Store reported**  
*Apr*: Non-functional app removed, users who purchased refunded

**Police ransomware moves on Android**  
*May*: Koler malware tries to lock the affected device and displays a ransom demand

**BlackEnergy rootkit for Windows 8**  
*Jun*: Sample uploaded to VirusTotal service with stripped functionality

**Havex hunts ICS/SCADA systems**  
*Jun*: Malware used in targeted attacks checks for industrial control systems

**Heartbleed bug makes global news**  
*Apr*: Millions of sites, phones thought to be affected by OpenSSL flaw

**Java SE update fixes 37 issues, some critical**  
*Apr*: Patch addresses multiple issues, including 4 rated ‘most critical’

**Windows XP included in off-cycle patch**  
*May*: Microsoft makes exception for EOL’ed OS to receive IE8 0-day patch

**Tech giants to fund vital projects**  
*May*: Core Infrastructure Initiative to fund OpenSSL, OpenSSH, among others

**Iraq blocks social media due to ISIS threat**  
*Jun*: Moved aimed at ‘disrupting insurgents communications’

**Thailand junta blocks sites, censors reporting**  
*Jun*: Hundreds of sites reportedly blocked, forbids critical media reports

**Youtube, Twitter access restored in Turkey**  
*Jun*: Youtube unblocked, follows lifting of ban on Twitter last month

**Gameover Zeus Botnet**  
*Jun*: 2-week ‘window’ for users to clean PCs ends; botnet still recovering

**US-CERT reports rise in cyber attacks**  
*May*: Report says 56% of firms surveyed reported cyber attacks

**TrueCrypt warns software now ‘harmful’**  
*May*: Drive-encryption project says tool ‘not secure’, warns against use

**Massive DDoS attack hits Hong Kong**  
*Jun*: 300Gbps+ attack on voting system after civic referendum

**MyBulletins launched to ease updating flow**  
*May*: Service intended to simplify identifying applicable security updates

**Google debuts ‘right to be forgotten’ form**  
*May*: EU court rules search engine to remove ‘irrelevant’ links on request in EU

**Google Apps add encryption**  
*May*: End-to-end email encryption offered to enterprise users

**Reset the Net campaign launched**  
*Jun*: Coalition of groups aim to encourage use of surveillance-resistance tools

**US wants 5 Chinese hackers for espionage**  
*May*: Dept of Justice claims PLA members hacked US businesses for 8 years

**Almost 100 arrested for Blackshades trojan**  
*May*: Arrests in US, EU & other countries for sale of trojan used to spy on users

**‘Oleg Pliss’ hackers arrested in Moscow**  
*Jun*: Russian Interior Ministry says arrested 2 for iOS ransom attacks in Oz

**FBI hunts for Gameover Zeus mastermind**  
*Jun*: Indictment against Russian national issued following botnet takedown

**Virus Shield app scam in Play Store reported**  
*Apr*: Non-functional app removed, users who purchased refunded

**Police ransomware moves on Android**  
*May*: Koler malware tries to lock the affected device and displays a ransom demand

**BlackEnergy rootkit for Windows 8**  
*Jun*: Sample uploaded to VirusTotal service with stripped functionality

**Havex hunts ICS/SCADA systems**  
*Jun*: Malware used in targeted attacks checks for industrial control systems

**Heartbleed bug makes global news**  
*Apr*: Millions of sites, phones thought to be affected by OpenSSL flaw

**Java SE update fixes 37 issues, some critical**  
*Apr*: Patch addresses multiple issues, including 4 rated ‘most critical’

**Windows XP included in off-cycle patch**  
*May*: Microsoft makes exception for EOL’ed OS to receive IE8 0-day patch

**Tech giants to fund vital projects**  
*May*: Core Infrastructure Initiative to fund OpenSSL, OpenSSH, among others
General trends
The most notable trend in H1 2014 is the continued growth of ransomware and ransoming activities, on both desktop and mobile platforms. Though the June takedown of the Zeus botnet [1] has hamstrung the spread of the Cryptolocker threat (at least for a while), ransomware as a whole continues to develop, as this half year saw existing threats such as Cryptolocker updating their distribution, encryption and payment methods to stay ahead of law enforcement’s counterefforts.

Ransomware made the leap to mobile, with the Koler threat as the first attempt at gaining a foothold on the Android platform. Though this malware threatened to but doesn’t actually encrypt files, the Slocker ransomware that soon followed does. As is usual with Android threats, both these ransomware pretend to be legitimate apps in order to trick the user into willingly installing them.

Meanwhile, ransoming activity on iOS devices took a different form. Introduced in iOS 7, the Activation Lock feature is meant to remotely lock an iOS device using an Apple ID password. A malicious misuse of the feature involves criminals offering an Apple ID login and password, supposedly for access to ‘free’ content. Once a user uses the bait credentials to authorize their iOS device, the criminals change the password, locking the device and essentially hijacking it for ransom. The most notable case of ransom activity on the iOS platform was the ‘Oleg Pliss’ incident that affected users in Australia in May, for which two individuals were subsequently arrested in Moscow [4].

Meanwhile, Windows XP finally reached its end of life (EOL) mark on 8 April 2014 (notwithstanding an emergency out-of-band patch that came out shortly after its EOL). Despite pressure to upgrade to Windows 8 (or really, any OS that’s actively supported), anywhere from 10–30% of computer users worldwide [7] are thought to still be using an OS that remains a favored target for attackers and now is no longer being patched. Though some users (particularly government and enterprise customers) have extended XP support, for most users security will become increasingly ‘self-service’ from now on.

H1 2014 also saw a slew of reports alleging questionable surveillance, online censorship or data handling activities by government entities in various nations. Major tech companies have made various efforts to increase the security of their offerings, as well as pressure their respective governments for increased transparency. See our H1 2014 Incidents Calendar for more details.

PC malware
As seen in our Top 10 Detections statistics, in H1 2014 the most prevalent threats reported to our telemetry systems by users of our products are mostly the same malware families seen from the second half of last year, just in varying order. Downadup (also known as Conficker in the media) is the most reported threat in this half year period, particularly in the Middle East, South America and Asia. This six-year-old worm continues to thrive in the wild, and Windows XP’s EOL isn’t likely to improve the situation.

Apart from Downadup, Majava and web-based attacks continue to be most visible in Europe and North America this half year. The file-infector families Sality and Ramnit are also threats that have been around for a few years, but continue to trouble users in all regions except North America and Europe.

Newcomers to the Top 10 Detections are the families Wormlink, BrowserExploit and Expiro. Interestingly, a notable change in the first half of this year is that detections related to specific, known exploits (e.g., CVE-2013-2471) are no longer visible in our Top 10 Detections.
Exploiting the MS08-067 vulnerability in Windows to spread over the Internet (as well as through removable media and network shares), this worm has infected millions of computers in over 200 countries.

Six years after it first emerged, unpatched machines still keep Downadup alive. As in the previous half-year, it continues to be prominent in Brazil, the United Arab Emirates and Italy, as well as Malaysia and France this year.

Spreads mostly via infected removable and hard drives. Variants in this family include harmful payloads such as data stealers. Autorun detection reports come most often from France, Malaysia, India, Poland and Turkey.

A collection of exploits against vulnerabilities in the Java development platform. A successful attack can, among other things, give the attacker total system control. Most frequently reported by clients in the United States, France and United Kingdom.

Virus that infects EXE, DLL & HTML files. May also drop a file that tries to download more malware from a remote server. First seen in 2011, Ramnit lingers on in Asia, particularly Malaysia, India, Vietnam and Indonesia.

A collection of malware, techniques or exploits used to redirect the web browser to malicious sites, where the browser or system may be subjected to more attacks. The trend from the end of 2013 continues with reports coming most often from France, the United States and Sweden, though this year Malaysia overtakes all three to report the highest number of these detections.

A large family of viruses that infect EXE files and use entry-point obscuration to hide their presence. Variants may also kill processes, steal data and so on. First seen in 2010, Sality is especially prominent in Malaysia, Brazil, Turkey and India.

Detects malicious shortcut icons used to exploit the critical CVE-2010-2568 vulnerability in Windows to gain total system control. Reports of this threat came mostly from Malaysia, Turkey, Vietnam and India.

Remnants of this botnet continue to trouble users in France, the United States, United Kingdom, Sweden and Finland.

Detects a browser process being used to drop and run a potentially harmful program. Most reports for this detection are from the United States, Finland, France and the United Kingdom.

Infects executable files and uses a keylogger component to steal credit card details. Most commonly reported in Italy, Finland, the United States, France and Germany.
Mac malware

2014 started with almost 20 new unique variants discovered in the first 2 months alone, though this pace slowed later so that by the end of the H1 period, 25 new Mac threats had been found. Among the new unique variants, 13 belong to 5 new families, with the Mask and Clientsnow being involved in targeted attacks. The remaining 3 new families—Coinstealer, Cointchief and Laoshu—affect normal Mac users. More details of the new Mac families are on page 14.

On Mobile

Q1.2014 saw a number of notable firsts for mobile malware (detailed in our Q1.2014 Mobile Threat Report). In Q2.2014, the majority of threats our Mobile Security for Android users reported to our telemetry systems continue to be targeted at the Android platform. Trojans also remain as the main mobile malware type, heavily reliant on straightforward social engineering to gain access to the device and its stored data.

There was also no significant change in the package names used by malicious Android apps, with most either using a fake but legitimate-sounding name (e.g., com.software.app) for their packages, or simply straightforward garbage (e.g., fkjsmgjl.ceinnykas). The use of nonsense names is particularly common in the Fakeinst family.

While checking the software name remains a standard security precaution for desktop threats, the same advice is difficult to apply to Android threats, as the package name is rarely displayed to the user, being visible on the device only for running processes under the Settings > Apps > Running > Processes menu. As this is unlikely to change soon, vigilance at the point of download remains for now the most effective precaution mobile users can take to avoid trojans.

iOS malware

Actual malicious apps on the iOS platform are few and far between, but they do exist. Unlike Android, malware on iOS have so far only been effective against jailbroken devices, making the jailbreak tools created by various hacker outfits (and which usually work by exploiting undocumented bugs in the platform) of interest to security researchers. In June, the Pangu tool for iOS 7.1.1 was unexpectedly released, with some allegations that it used stolen exploits, as well as concern over a "shady" pirated apps store installed alongside the tool. Both issues were addressed in a subsequent update. Earlier in H1, reddit users reported a suspicious library file, subsequently named Unflod Baby Panda. When installed on jailbroken iOS devices, the malware listens to outgoing SSL connections in order to steal the device's Apple ID and password details. More details on iOS malware are on page 14.

Constants

Despite the various innovations or developments we saw this past quarter, many of the mobile-related findings we documented in our H2.2013 Threat Report remain unchanged. When we looked again at app store security in H1.2014 (comparing the number of malicious samples versus the total number of samples we obtained from a store), we saw no significant change from the results we documented in the previous report. Despite news of four malicious apps being found and pulled from Google's Play Store in H1, considering the vast number of apps in the marketplace, the low incidence of malicious ones (so far) and the prompt remedial efforts the team makes to deal with reported threats, the Play Store remains the safest online market for mobile apps.

There was also no significant change in the package names used by malicious Android apps, with most either using a fake but legitimate-sounding name (e.g., com.software.app) for their packages, or simply straightforward garbage (e.g., fkjsmgjl.ceinnykas). The use of nonsense names is particularly common in the Fakeinst family.

SOURCES

3. F-Secure Weblog; Locker Android Ransomware Communicates Via Tor And SMS; 16 Jun 2014; http://www.f-secure.com/weblog/archives/00000716.html
### TOP 10 DETECTIONS BY REGION

#### PER 1 000 USERS

<table>
<thead>
<tr>
<th>Region</th>
<th>Top 10 Detections</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>Majava, Web-based attacks, ZeroAccess, BrowserExploit, Autorun, Sality, Downadup</td>
</tr>
<tr>
<td>South America</td>
<td>Majava, Web-based attacks, ZeroAccess, BrowserExploit, Autorun, Sality, Downadup</td>
</tr>
<tr>
<td>Africa</td>
<td>Sality, Ramnit, Downadup, Autorun, WormLink, Web-based attacks</td>
</tr>
<tr>
<td>Asia</td>
<td>Downadup, Web-based attacks, Sality, Ramnit, WormLink, Autorun, Majava, BrowserExploit</td>
</tr>
<tr>
<td>Middle East</td>
<td>Majava, Web-based attacks, ZeroAccess, BrowserExploit, Autorun, Sality, WormLink</td>
</tr>
<tr>
<td>Europe</td>
<td>Majava, Web-based attacks, Downadup, Autorun, BrowserExploit, Expiro, Sality, Ramnit, WormLink</td>
</tr>
<tr>
<td>Asia</td>
<td>Australia, China, Hong Kong, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, Pakistan, Philippines, Singapore, Taiwan, Thailand, Turkey, Vietnam</td>
</tr>
<tr>
<td>North America</td>
<td>Algeria, Egypt, Iran, Lebanon, Oman, United Arab Emirates</td>
</tr>
<tr>
<td>South America</td>
<td>Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, Guadeloupe</td>
</tr>
<tr>
<td>Africa</td>
<td>Ghana, Kenya, Morocco, South Africa, Tunisia</td>
</tr>
<tr>
<td>Europe</td>
<td>Aland Islands, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom</td>
</tr>
</tbody>
</table>

Note: Other countries were excluded due to lack of statistically valid data.

---


First ransomware (almost)

**Trojan:Android/Koler** is the mobile extension of ‘police-themed’ Reveton ransomware. First reported in May, the app appears to offer access to adult contents but once installed, it demands a ‘fine’ for “security violations” (or similar). Though it claims to encrypt files on the device, Koler only disables the Back button to keep the ransom demand prominent.

First TOR-encrypted ransomware

Unlike Koler, the **Trojan:Android/Slocker** malware reported in June actually encrypts image, document and video files on the device. Like Koler, it also disables the Back button to interfere with the user’s control of the device. Slocker variants can communicate with their controlling server either via the Tor anonymizing network or SMS messages.

**Trojan:Android/SMSSend**

Large family of malware that sends SMS messages to premium-rate numbers

**Trojan:Android/Fakelnst**

Appears to be app installers, but sends SMS messages to premium rate numbers

**Trojan:Android/Eropl**

Silently harvests data from the device and forwards it to a remote server

Oleg Pliss strikes Australia

In May, ‘Oleg Pliss’ locks the accounts of a number of users in Australia, reportedly by using the ‘Find My iPhone’ feature, and demands ransom. Apple denies speculations of a breach in their iCloud services (some reports blamed phishing scams). In June, two individuals are detained in Moscow, Russia in connection with the attack.

**NEW FAMILIES or VARIANTS**

<table>
<thead>
<tr>
<th>Family Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan:Android/Koler</td>
<td>Mobile extension of ‘police-themed’ Reveton ransomware, demands a ‘fine’</td>
</tr>
<tr>
<td>Trojan:Android/Slocker</td>
<td>First TOR-encrypted ransomware, encrypts image, document and video files</td>
</tr>
<tr>
<td>Trojan:Android/SMSSend</td>
<td>Large family of malware, sends SMS messages to premium-rate numbers</td>
</tr>
<tr>
<td>Trojan:Android/Fakelnst</td>
<td>Appears to be app installers, sends SMS messages to premium rate numbers</td>
</tr>
<tr>
<td>Trojan:Android/Eropl</td>
<td>Silently harvests data from the device and forwards it to a remote server</td>
</tr>
</tbody>
</table>

**TOP 3 ANDROID FAMILIES**

<table>
<thead>
<tr>
<th>Family Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan:Android/SMSSend</td>
<td>Large family of malware, sends SMS messages to premium-rate numbers</td>
</tr>
<tr>
<td>Trojan:Android/Fakelnst</td>
<td>Appears to be app installers, sends SMS messages to premium rate numbers</td>
</tr>
<tr>
<td>Trojan:Android/Eropl</td>
<td>Silently harvests data from the device and forwards it to a remote server</td>
</tr>
</tbody>
</table>

**TOP REPORTING COUNTRIES**

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Great Britain</td>
<td>23</td>
</tr>
<tr>
<td>France</td>
<td>11</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>9</td>
</tr>
<tr>
<td>India</td>
<td>8</td>
</tr>
<tr>
<td>Germany</td>
<td>8</td>
</tr>
<tr>
<td>Finland</td>
<td>5</td>
</tr>
<tr>
<td>Malaysia</td>
<td>3</td>
</tr>
<tr>
<td>Brazil</td>
<td>3</td>
</tr>
<tr>
<td>Netherlands</td>
<td>2</td>
</tr>
<tr>
<td>All Other Countries</td>
<td>21</td>
</tr>
</tbody>
</table>

**SOURCES**

1. Malware don’t need Coffee; Kafeine; Police Locker land on Android Devices; 4 May 2014; [http://malware.dontneedcoffee.com/2014/05/police-locker-available-for-your.html](http://malware.dontneedcoffee.com/2014/05/police-locker-available-for-your.html)
5. Palo Alto Networks Research Center; Claud Xiao, Zhi Xu; Cardbuyer: New Smart Android Trojan Defeats Multi-Factor Verification and Steals Prepaid Game Cards; 24 Apr 2014; [https://researchcenter.paloaltonetworks.com/2014/04/cardbuyer-new-smart-android-trojan/](https://researchcenter.paloaltonetworks.com/2014/04/cardbuyer-new-smart-android-trojan/)
Shipped with Spyware
A security firm reports discovering a smartphone shipped out straight from the factory with extensive spyware (Trojan:Android/SmsSend.AC) built into the device’s firmware, which would allow the malware controller full access to data saved on the phone.

Prepaid card-stealer
Trojan:Android/Cardbuyer is reportedly able to defeat various verification processes used by online games or payment platforms, and intercepts SMS messages to quietly buy prepaid cards with the user’s account.

iDroidBot on sale
In April, Russian underground forums post ads for iDroidbot, targeting devices running iOS 7.1 as well as Android, and is capable of stealing saved credit card details and credit from QIWI wallets, among other actions.

Stealing Apple IDs
Reddit users report a suspicious library file being distributed that when installed will hook all running processes and listen to outgoing SSL connections in order to steal the device’s Apple ID and password details. The malware is subsequently named UnfIod Baby Panda.

Вирус Shield
In April, the Android Police site breaks the news that Virus Shield, security software that was the top-ranked paid app in the Google Play Store (with over 10,000 downloads and a 4.7 star rating) is in fact nothing but a scam. Google subsequently pulls it from the market and offers users who had purchased the fraudulent app a refund, plus store credit.

BankMirage
A malicious clone of a legitimate banking app for the Israeli Mizrahi Bank that steals user IDs from an in-app login form. Researchers speculate it was designed to gather data for a later attack, as the app explicitly ignored passwords. The malware is only available on the Play Store for a few days before a security firm reports it and the app is swiftly removed.

Songs & Prized
Two free apps share similar behavior to cryptocurrency mining apps found on third-party app stores. Silently performs digital currency mining while the device is charging and prevents it from going into sleep mode. Both apps were removed from the Play Store following news of the discovery.

In the Play Store

In the News

- Shipped with Spyware
- Prepaid card-stealer
- iDroidBot on sale
- Stealing Apple IDs
- Virus Shield
- BankMirage
- Songs & Prized

Legal
9. Android Police; Michael Crider; The #1 New Paid App In The Play Store Costs $4, Has Over 10,000 Downloads, A 4.7 Star Rating... And It’s A Total Scam [Updated]; 10 Apr 2014; http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/
10. Lookout Blog; Meghan Kelly; Cloned banking app stealing usernames sneaks into Google Play; 24 Jun 2014; https://blog.lookout.com/blog/2014/06/24/bankmirage/
11. ZDNet; Liam Tung; Google yanks two battery-sucking Bitcoin mining Android apps from Play store 28 Mar 2014; http://www.zdnet.com/google-yanks-two-battery-sucking-bitcoin-mining-android-apps-from-play-store-2000027828/
Mac malware between January and June 2014

**25 new variants**

Of Mac malware in total were discovered between January to June 2014.

**New Variants Count by Month**

- January: 9
- February: 0
- March: 0
- April: 2
- May: 3
- June: 10

**New Variants Breakdown**

- **60%** Backdoor
- **24%** Trojan
- **16%** Others

**Backdoor**

- Has been the most common type of malware detected.

**Trojan**

- Spread via various channels, including social media.

**Others**

- Includes a variety of malware types.

**New Variants Trends**

- The number of new variants rose sharply in March and April.
- This number cooled down towards the end of H1 as Mac malware usually come in waves.

**New Families**

- **5 new families** were discovered in H1 2014.

**Coinstealer**

- A Bitcoin stealer that poses as a leaked back office application for accessing restricted Mt. Gox trade information.

**LaoShu**

- A remote access trojan that spreads via bogus courier email notifications.

**CoinThief**

- A trojan spyware intended for stealing cryptocurrencies.

**Mask**

- A high profile cyber espionage operation.

**Clientsnow**

- Used in targeted attacks against Tibetan and Uyghur communities.

**Resources**

1. Twitter; Broderick Aquilino; 12 February 2014; https://twitter.com/BrodAquilino/status/433529401699864576
2. Threatpost; Michael Mimoso; Mac Trojan Steals Bitcoin Wallet Credentials; 10 February 2014; http://threatpost.com/mac-trojan-steals-bitcoin-wallet-credentials/104152
3. Wikipedia; Front and back office application; 24 March 2014; http://en.wikipedia.org/wiki/Front_and_back_office_application

**Note:** Numbers shown are the count of unique variants detected. This means repackaged installers are not counted and multiple-component malware are counted as one.
INCIDENTS CALENDAR

**DIGITAL FREEDOM**
1. The Guardian; Spencer Ackerman, James Ball; Optic Nerve; millions of Yahoo webcam images intercepted by GCHQ; 28 Feb 2014; http://www.theguardian.com/world/2014/feb/28/yahoo-webcam-images-internet-yahoo


3. Reuters; Thai ministry sparks alarm with brief block of Facebook; 28 May 2014; http://in.reuters.com/article/2014/05/28/thailand-politics-facebook-idINKBN0E80U520140528

4. Arstechnica; Sean Gallagher; NSA loves The Bahamas so much it records all its cellphone calls; 21 May 2014; http://arstechnica.com/tech-policy/2014/05/nsa-loves-the-bahamas-so-much-it-records-all-its-cellphone-calls/


7. CNET; Micheal Tan; After Thailand’s coup, a stifling of online dissent (Q&A); 12 Jun 2014; http://www.cnet.com/news/behind-thailands-high-tech-coup-stifling-online-dissent-q-a/


**ATTACKS**

10. Arstechnica; Dan Goodin; Hackers hijack 300,000-plus wireless routers, make malicious changes; 4 Mar 2014; http://arstechnica.com/security/2014/03/hackers-hijack-300000-plus-wireless-routers-make-malicious-changes/


16. The Register; Darren Paul; Massive DDoS attack hits Hong Kong; 23 Jun 2014; http://www.theregister.co.uk/2014/06/23/most-sophisticated-ddos-attack-hits-hk-democracy-politicians/

**SECURITY**

18. F-Secure Weblog; Sean Sullivan; TrustyCon Video; 28 Feb 2014; http://www.f-secure.com/weblog/archives/0000062e.html

19. ZDNet; Larry Seltzer; Windows XP dies at 12 1/2 after long illness; 8 Apr 2014; http://www.zdnet.com/windows-xp-dies-at-12-12-after-long-illness-7000028194/

20. BBC; Leo Kelion; eBay makes users change their passwords after hack; 21 May 2014; http://www.bbc.com/news/technology-27502990

21. PCWorld; Mark Hachman; Microsoft simplifies security updates with MyBulletins; 28 May 2014; http://www.pcworld.com/article/2207346/microsoft-simplifies-security-updates-with-mybulletins.html

22. PC Mag; Stephanie Mlot; Google launches ‘right to be forgotten’ form; 30 May 2014; http://www pcmag.com/node/2/0.2817245836.00.asp

23. Forbes; Ben Kepes; No More Scroogled, No More NSA, Google Apps Gets Encryption; 21 May 2014; http://www.forbes.com/sites/benkepes/2014/05/21/no-more-scroogled-no-more-nsa-google-apps-gets-encryption/

24. The Guardian; Dominic Rushe; Edward Snowden calls for greater online privacy in Reset the Net campaign; 5 Jun 2014; http://www.theguardian.com/world/2014/jun/05/edward-snowden-privacy-reset-the-net

**ENFORCEMENT**


28. The Register; Simon Sharwood; ‘Anons’ cuffed by Australian Federal Police; 22 May 2014; http://www.theregister.co.uk/2014/05/22/anons_cuffed_by_australian_federal_police/

29. The Register; Iain Thomson; US authorities name five Chinese military hackers wanted for espionage; 19 May 2014; http://www.theregister.co.uk/2014/05/19/us_authorities_name_five_chinese-military_hackers_wanted_for_espionage/

30. SC Magazine UK; Doug Drinkwater; 100 hackers arrested over Blackshades Trojan; 19 May 2014; http://www.scmagazineuk.com/100-hackers-arrested-over-blackshades-trojan/article/347488/


MALWARE

33. Malware Must Die; Threat Intelligence - New Locker: Prison Locker (aka: Power Locker...or whatever those bad actor calls it); 3 Jan 2014; http://blog.malwaremustdie.org/2014/01/threat-intelligence-new-locker-prison.html

34. F-Secure Weblog; Sean Sullivan; Gameover ZeuS Jumps on the Bitcoin Bandwagon; 14 Mar 2014; http://www.f-secure.com/weblog/archives/00002695.html

35. InfoSec Handlers Diary Blog; Johannes Ullrich; Linksys Worm "TheMoon" Summary: What we know so far; 13 Feb 2014; https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633

36. F-Secure Weblog; Coremex Innovates Search Engine Hijacking; 1 Apr 2014; http://www.f-secure.com/weblog/archives/00002695.html

37. Android Police; Michael Crider; The #1 New Paid App In The Play Store Costs $4. Has Over 10,000 Downloads, A 4.7-Star Rating...And It's A Total Scam [Updated]; 10 Apr 2014; http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/


40. F-Secure Weblog; David Hentunen; Havex hunts ICS/SCADA systems; 23 Jun 2014; http://www.f-secure.com/weblog/archives/00002718.html

VULNERABILITIES

41. ZDNet; Violet Blue; Major Apple security flaw: Patch issued, users open to MITM attacks; 22 Feb 2014; http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/

42. KrebsonSecurity; Brian Krebs; Microsoft Warns of Attacks on IE Zero-Day; 27 Apr 2014; http://krebsonsecurity.com/2014/04/microsoft-warns-of-attacks-on-ie-zero-day/

43. PCWorld; Ian Paul; Adobe releases emergency Flash patch for Windows and OS X systems; 8 Feb 2014; http://www.pcmag.com/article/2027624/adobe-releases-emergency-patch-for-windows-and-os-x-systems.html

44. ArsTechnica; Dan Goodin; Zero-day vulnerability in Microsoft Word under active attack; 25 Mar 2014; http://arstechnica.com/security/2014/03/zero-day-vulnerability-in-microsoft-word-under-active-attack/

45. CNet; Richard Nieva; Heartbleed bug: What you need to know (FAQ); 11 Apr 2014; http://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/


47. Bit-tech; Gareth Halfacree; Windows XP gets first post-EOL security patch; 2 May 2014; http://www.bit-tech.net/news/bits/2014/05/02/winxp-eol-patch/

48. SCMagazine; Marcos Colon; Tech giants to fund vital projects; 29 May 2014; http://www.scmagazine.com/core-infrastructure-initiative-to-fund-openssl-audit/article/349068/
F-SECURE INTERNET SECURITY

The best protection in the world for surfing, banking and shopping online.

Complete protection for surfing, shopping, banking and using social media. F-Secure Internet Security protects your digital content and you with real-time protection against malware, hackers and identity theft. Your online transactions are secured with banking protection, and you and your children are protected against harmful and unsavory web sites.

AV-TEST BEST PROTECTION AWARD
www.av-test.org

PREISTIPP LOGO FOR GOOD VALUE
www.com-magazin.de

PC ADVISOR ONLINE
www.pcadvisor.co.uk

F-SECURE FREEDOME

We’ve gathered the most sophisticated security features — VPN, anti-virus, anti-tracking, and anti-phishing — into one intuitive service. With the push of a button, Freedome watches your back.

Available in Europe, North America, Latin America, Thailand, Turkey and Russia.

“If you want a secure connection between your IOS or Android device and the online world, Freedome provides it.”

- PCWorld on Apr 25, 2014

GET IT ON
Download on the
Google play
App Store
SWITCH ON FREEDOM

© F-Secure Corporation 2014. All rights reserved.