

A Look Inside the Universe of Pirated Software and Digital Assets

Three pixelated pirate ships with skull and crossbones on their sails, sailing on a blue sea. The ships are arranged in a line, with the largest one on the left and two smaller ones to its right. The style is reminiscent of early computer graphics or video game sprites.



Table of Contents

| | |
|--|-----------|
| 1. Executive Summary | 2 |
| 2. State of Digital Piracy | 4 |
| Volume and Nature of Pirated Assets | 4 |
| Software Piracy | 4 |
| Online Gaming Piracy | 5 |
| Digital Media Piracy | 5 |
| Research Methodology | 6 |
| Distribution Model for Pirated Software and Digital Assets | 7 |
| Economics And Business Implications Of Piracy | 14 |
| Role Of Unprotected Applications In Enabling Piracy | 16 |
| Vulnerabilities Of Applications..... | 16 |
| In the Software Provider (ISVs) Market | 17 |
| In Digital Media Ecosystem | 17 |
| In Gaming Market | 18 |
| Vulnerabilities of Mobile Apps | 19 |
| 3. Recommendations To Mitigate Digital Piracy | 22 |
| 4. Appendices | 24 |
| Appendix A: Footnotes | 24 |
| Appendix B: Glossary | 25 |
| Appendix C: Readily Available Tools Make It Easier To Hack..... | 26 |
| Appendix D: Overview of iThreat Cyber Group's Services | 27 |
| Appendix E: OWASP Top Ten Mobile Risks | 28 |

1. Executive Summary

The illegal reproduction and distribution of copyrighted material on the Web is extensive and growing rapidly.

Arxan and iThreat Cyber Group (ICG) analyzed data collected by ICG over the past 3.5 years that looked at the distribution of pirated software and digital assets on the Dark Web (i.e., the portion of content on the World Wide Web that is not indexed by standard search engines) and indexed sites that are focused on distributing pirated releases. Thousands of sites were analyzed, including more than 50 that are solely in the business of distributing pirated releases. The analysis revealed:

- Pirated software and digital assets are on the rise
 - There were over 1.6M pirated releases in 2014, and if 2015 continues at the same pace, there will be 1.96M pirated assets by the end of the year – an increase of 22% percent over the last 3 years.
 - 41% of pirated software was Android apps and 17% were key makers or generators that can help hackers gain unauthorized access to applications and related data.
- Online games are heavily pirated
 - If distribution of pirated games continues at the same rate for the rest of the year, we estimate that there will be over 31,000 pirated releases in 2015 – which would be double the number of pirated releases since 2012.
- The extent of digital media piracy is far more extensive than commonly perceived
 - In 2013 and 2014 an average of nearly 1M pirated releases were discovered.
 - In reviewing the pirated assets found in 2015, videos (TV, movies, etc., but excluding adult content) accounted for about 50% and adult content accounted for roughly 25%.
- The cost or un-monetized value of these pirated materials in 2014 is estimated to be more than \$800 billion⁵.

Poorly protected applications and a rapidly evolving distribution system for pirated assets are enabling the increased volume and growth of unauthorized pirated releases.

- Few applications (be they online games, software that governs access to digital media or software that executes financial or other critical business functions) are deployed with protected binary code. Unfortunately, an adversary can directly access unprotected application binary code, analyze it, and reverse-engineer it back to source-code. With the source-code revealed, pirates are able to easily copy and redistribute the software. In June of 2015, third-party independent analysis conducted by MetaIntelli found that less than 10% of the 96,000 Android apps analyzed from the Google Play store had protected binary code.
- Hackers are getting access to digital media using a number of techniques, which are outlined in the report. Most are stealing cryptographic keys that govern access to digital media and using these keys to decrypt the encrypted digital media files, and pirate them. Hackers are also stealing content from media players as it decrypts in memory via memory scraping.

- The means of distributing pirated software and digital assets has evolved and expanded rapidly to a state where hundreds of millions of Internet users worldwide are accessing pirate distribution sites. Many pirate sites survive based on advertising revenue (i.e., advertisers are paying to promote their products and services on these sites), while others charge a fee so the user doesn't have to view the ads.
 - The largest content theft sites generated more than \$200 million in advertising-driven revenues in 2014⁴.
 - Movement across the various types of pirate distribution sites (which are described in the report) typically happens very quickly. One release profiled in the report was publicly available in little over 30 minutes, which is common.
 - Traffic to these pirate distribution sites is very high. One study by NetNames/Envisional, commissioned by NBC Universal³, revealed that nearly 24% of internet traffic was going to these sites.

A concerted focus and holistic approach to protecting software – including the software that governs access to digital media is needed to thwart the growing piracy problem. Those responsible for application security should:

- Harden applications so they are not susceptible to reverse engineering.
- Build run time protections into applications (particularly mobile apps) to thwart tampering / malware attacks.
- Protect cryptographic keys so they are not visible statically (i.e., while residing on a device) or at run time in memory. White box cryptography solutions provide this type of protection.
- Rethink their security investment approach – considering how much time and money is spent on application security. The 2015 Ponemon Institute study sponsored by IBM found that 50% of organizations had zero budget allocated to protecting mobile apps.
- Lobby organizations that are responsible for setting standards and rules that penalize piracy.

2. State of Digital Piracy

Volume and Nature of Pirated Assets

Not a week goes by where we don't hear about a cyber attack. Successful attacks are arming hackers with a treasure trove of digital assets that they're exploiting in many ways.

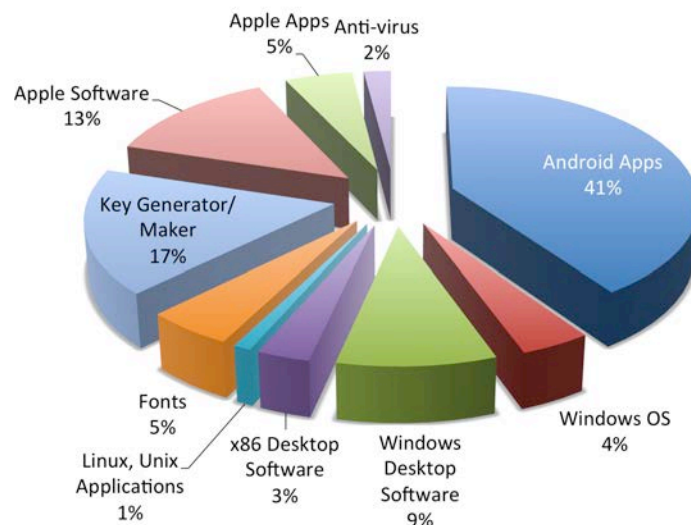
For the 2015 State of Application Security Report, we dove into the world of pirated software and digital assets to assess the illegal reproduction and distribution of copyrighted material on the Web.

Software Piracy

- In each of the last three years, infringing releases of more than 30,000 software titles were found.
 - These ranged from mobile apps to desktop operating systems and more (see Exhibit 2A for a breakdown of pirated software releases found between Jan 2012 and Mar 2015).
 - An Android app is 8.2 times more likely to be pirated than an iOS app. While there are more Android apps and many more Android users, the number of pirated Android apps is disproportionately higher than the number of iOS apps, suggesting that the security controls that Apple has in place are helping to thwart hackers.
 - According to app analytics company App Annie, there were slightly more Android apps (just under 1.5M) vs. iOS apps (just under 1.25M) at the end of 2014¹.
 - According to IDC, Android has nearly 80% of the global mobile operating system market².
 - We included in this category, software to generate keys and found nearly 9,000 key makers or generators that can help hackers gain unauthorized access to applications and related data and assets. This highlights the extent to which license and cryptographic keys are being targeted.

Exhibit 2A: Breakdown of Software Piracy Found, Jan. 2012 – Mar. 2015

(Source: iThreat Cyber Group and Arxan Analysis, May 2015)



Online Gaming Piracy

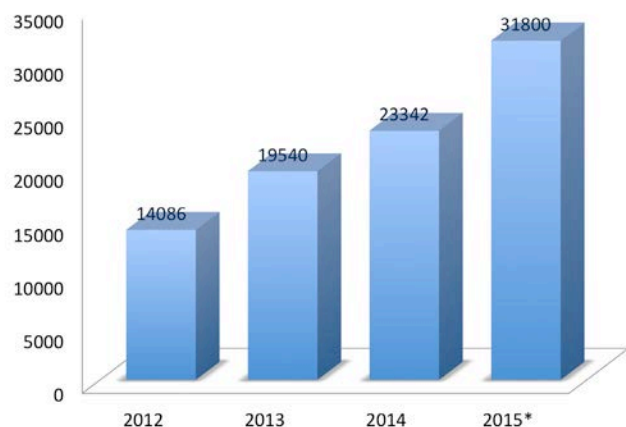
We found software-based games to be widely pirated and game piracy to be on the rise.

- In 2014 we discovered 23,000 pirated game releases
- If distribution of pirated games continues at the same rate, we estimate that there will be over 31,000 pirated releases in 2015 – which means that the number of pirated gaming releases will have more than doubled since 2012

Our findings are summarized in Exhibit 2B, on the right.

Exhibit 2B: Number of Pirated Games Found Jan. 2012 – Mar. 2015

(Source: iThreat Cyber Group and Arxan Analysis, May 2015)



*Note: 2015 pirated games are an estimate based on actual pirated releases found Jan. – Mar.

Digital Media Piracy

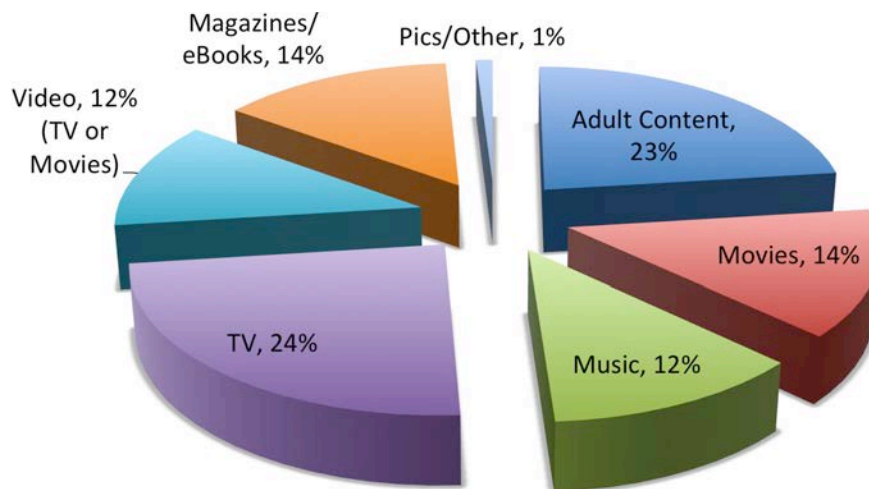
Finally, as many of you already know, digital media is being widely pirated.

- In 2013 and 2014 an average of nearly 1M pirated assets were discovered.
- If the numbers continue in 2015 at the same rate as in Q1, we predict there will be 1.3M pirated releases.
- In reviewing the pirated assets found in 2015, videos (TV, movies, etc., but excluding adult content) accounted for about 50% of pirated assets.
- Just under a quarter of pirated assets were adult content. Adult content is also one of the fastest growing areas – in 2012 there were 124K pirated releases found and in 2014 the number jumped to 204K (an increase of about 65% in just two years).

See Exhibit 2C for a full breakdown of pirated digital media.

Exhibit 2C: Mix of Digital Media Pirated Assets Found Jan. - Mar. 2015

(Source: iThreat Cyber Group and Arxan Technologies Analysis, May 2015)



Research Methodology

In May of 2015, Arxan worked with iThreat Cyber Group (ICG) to summarize the findings that ICG's tools and analysis had discovered since 2012.

ICG continually maintains access to the most prolific and notorious infringing release group sources, Internet brokers, source piracy facilitators, clandestine 'Scene' and 'P2P' release groups, private FTP and BitTorrent sites and servers. The most prolific and notorious infringing targets are identified by ICG from historical infringement, forensic geographic source information, and online infringing release attribution. Much of the access maintained by ICG is to sites focused on distributing infringing content via the Dark Web (i.e., this content on the World Wide Web is not indexed by standard search engines). Thousands of sites are analyzed in the process, including over 50 that are solely in the business of distributing infringing and unauthorized content.

About iThreat Cyber Group

ICG services have spanned three decades predicting, investigating, researching and reducing threats for their clients. Driven by technology, with oversight by highly skilled human analysts, ICG uses a method-patented process to provide big data and targeted threat-data analysis customized to the needs of each client. ICG monitors, investigates and tracks the individuals and groups who threaten companies, facilities, employees, processes and intellectual property. See Appendix for a more detailed overview of ICG's services and approach.

Distribution Model for Pirated Software and Digital Assets

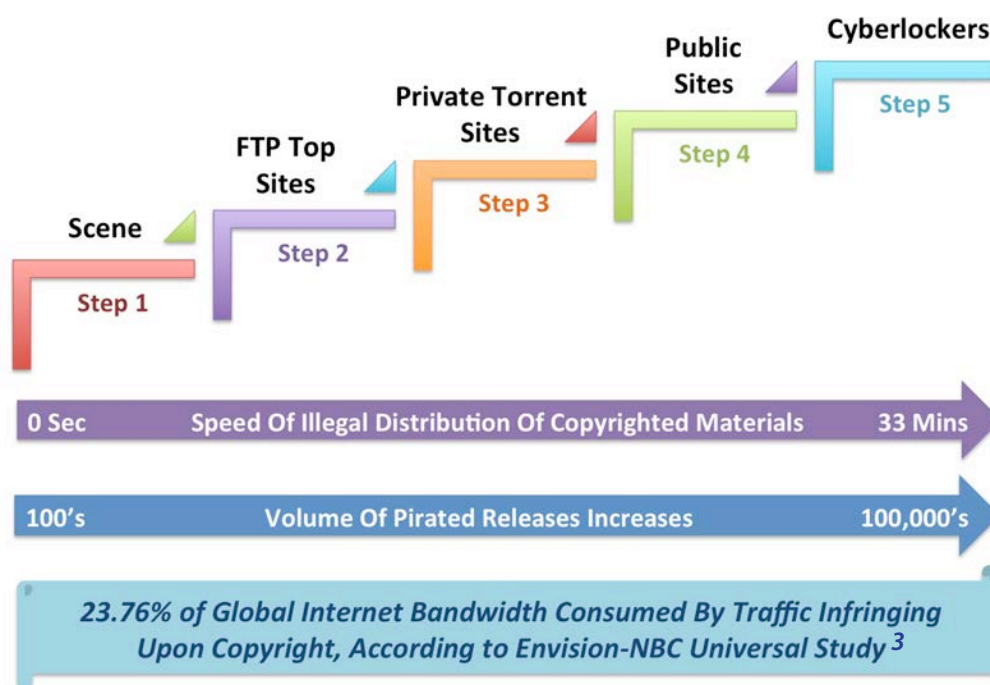
The sites that are focused on the distribution of pirated releases vary in nature. Some are revenue based, driving a profit for those who operate them. Many of these sites survive based on advertising revenue (i.e., advertisers are paying to promote their products and services on these sites), while others charge users a fee or request donations from their users. The payments provide the users with continued access to a steady stream of infringing releases, sometimes provide early access to new infringing releases prior to non-paying members for some period of time, and/or prevent the users from having to view advertising. Many of these sites, however, are free. At these sites, visitors are able to take whatever they wish, or may be constrained to download only as many pirated assets as they have contributed to the site. The motivations of those operating these distribution sites are as varied as the motivations across the human population.

The means of distributing pirated software and digital assets has evolved and expanded rapidly to a state where hundreds of millions of Internet users worldwide are accessing these sites. It is difficult to say where these sites are located, but, for the most part, English is the universal language used to distribute pirated releases.

There are hundreds of sites involved in the process and many different types of sites.

Exhibit 2D illustrates how it all works.

Exhibit 2D: Pirated Software Distribution Process

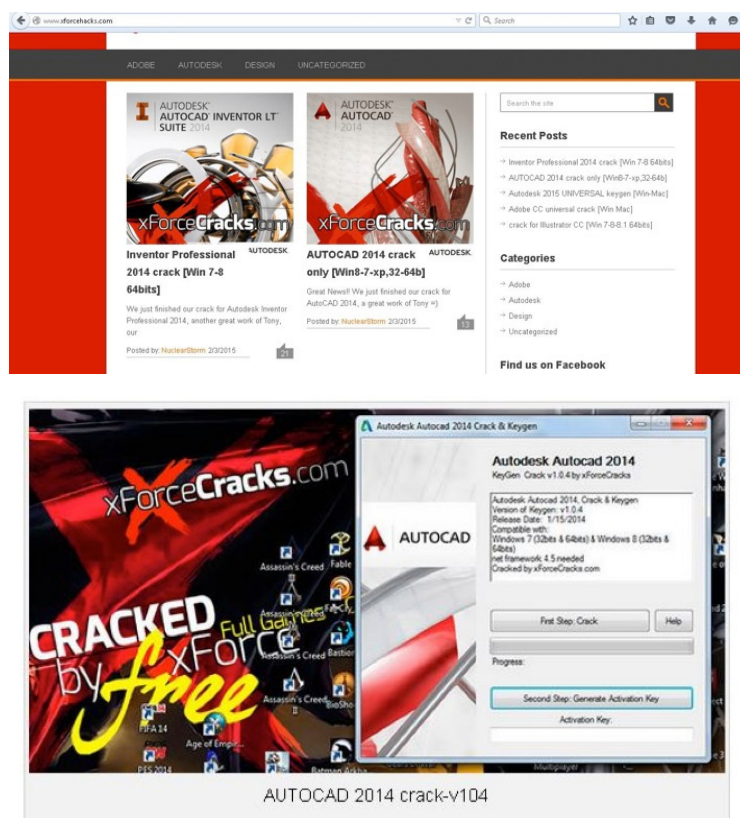


Step 1: Scene release

A software release is first packaged and released to private scene FTP Topsites(s) affiliated with the source release/cracking group. This is typically known as a “scene” release. Members of the source release group and other closely affiliated groups/members of these sites can now consume this release. Scene release groups are typically small groups with consumers in the hundreds. The primary motive for releasing this content is for the prestige of getting and cracking it first. Groups compete with each other by “racing” to be the first to release the content. The more elite FTP sites that the group is affiliated with, and the more assets available on those sites, the higher the group ranks. The more prominent the group becomes, the more likely someone with the ability to crack software and/or access software content would reach out to the group; usually to trade for access to FTP sites.

There are some exceptions, however, including reckless/insecure public release groups, like xforce (see Exhibit 2E) that post directly on their blog site and anyone can download it from their servers right away.

Exhibit 2E: xforce Images



Autodesk Autocad 2014, Crack & Keygen

Version of Keygen: v1.0.4

Release Date: 1/15/2014

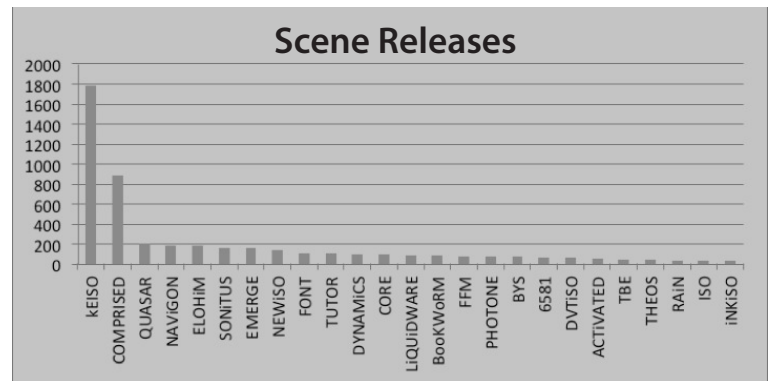
Compatible with:

Windows 7 (32bits & 64bits) & Windows 8 (32bits & 64bits)

net framework 4.5 needed

Cracked by xForceCracks.com

Exhibit 2F: Number of releases by top scene piracy release groups over the past year



Step 2: Private FTP Topsites

After the initial release, usually within seconds or minutes, the software package is spread to additional private scene FTP sites affiliated with other release groups in the scene. "Couriers" compete to be the first to race the content from the release group's affiliated sites to private FTP sites not affiliated by the responsible release group, making the content available to all members of any release group in the scene. This is still a small group (thousands of consumers).

See exhibit 2G for an image of a welcome page for a now defunct scene FTP site. The welcome page provides details such as size, location, speed, group affiliates and IRC (Internet Relay Chat) channel

Exhibit 2G: Welcome page for the now defunct Scene FTP Site 'ASP.us'

[illegible]

Step 3: Private Torrent Sites

The content is then downloaded by persons with access to private scene FTP sites (operators, couriers, group members) and then, usually within minutes, made available to private torrent sites known for competing to have the best “pretimes” (a word private torrent sites use to describe how quickly they obtain FTP scene content and make it available to members of their private torrent sites). Private torrent sites of this nature vary in membership from less than 100 members to 50,000 or more, and there are at least 30 top-tier “pretime” sites related to software releases and hundreds of private sites in total. Some private torrent sites are known as “pay for access” type sites, where the tracker operator profits from site registrations and/or donations. At this point, the pirated asset is accessible to a relatively small consumer population (i.e., tens of thousands of consumers).

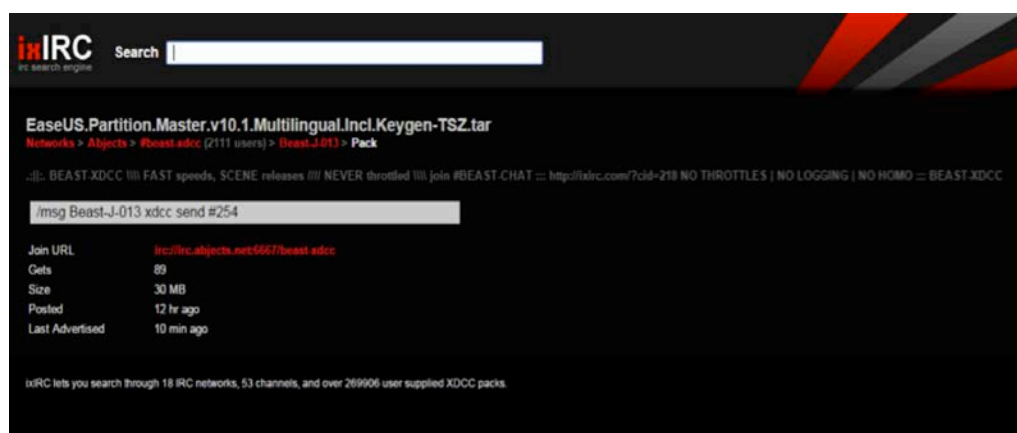
Step 4: Public Sites

In addition to private torrent sites, and almost as quickly, the content then spreads to other avenues of mass consumption that represent potentially many millions of pirate consumers:

- Public torrent sites (piratebay/kickass/extratorrent/etc.).
- xdcc/fserv/dcc IRC bots/scripts on major and private IRC (Internet Relay Chat) networks.
- dc++ hubs and other truly p2p pirate networks (bearshare/limewire/napster/etc.).
- UseNet/NZB/Newsgroup releases.

Exhibit 2H shows a publicly available file posted online received 89 downloads in 12 hours.

Exhibit 2H: Sample Summary from Private Internet Relay Chat Network

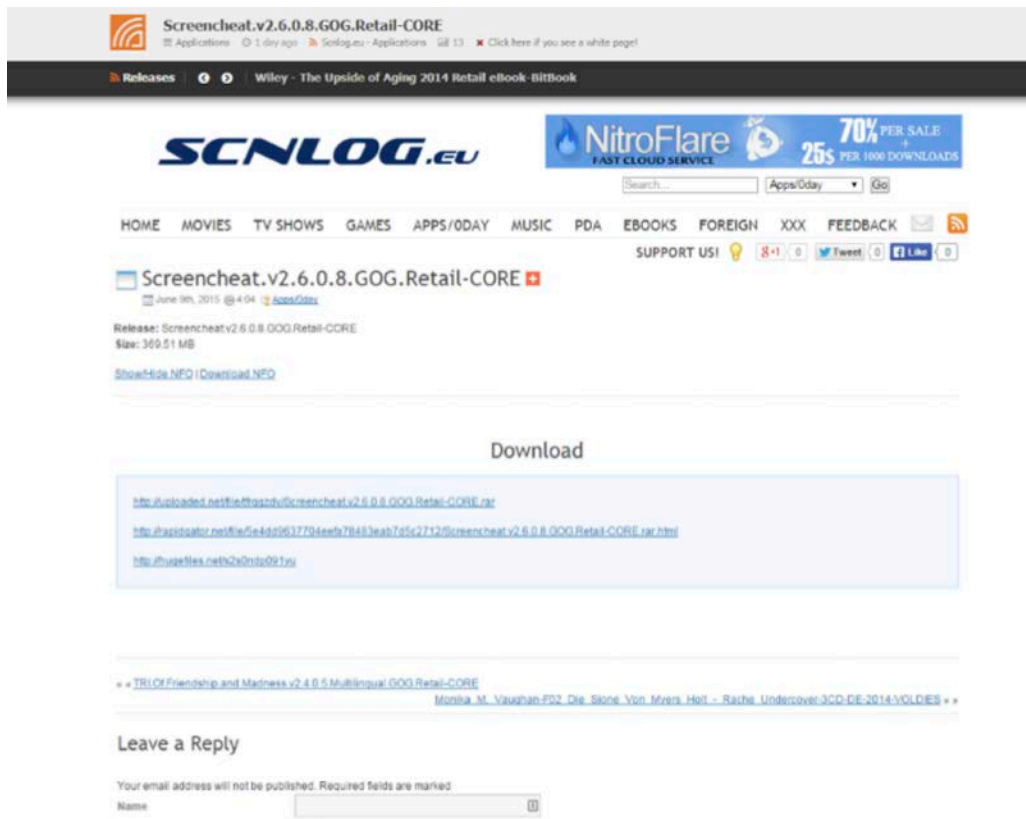


Step 5: Cyberlockers

Next, and almost as quickly as private torrent sites, the content spreads to a rising star in the mass consumption piracy world: cyberlockers and download link index blogs. Many cyberlockers compensate uploaders of popular content to their storage servers with money and download credits. There are hundreds of cyberlocker index sites that are used by millions of pirate consumers. A web browser is all that is needed to access a cyberlocker. The cyberlockers profit heavily by selling user information and advertising.

Exhibit 2I contains an image from a cyberlocker that provides multiple download links for the same file.

Exhibit 2I: Example of a Cyberlocker



Speed Of Piracy

Movement from steps one through five typically happens very quickly – in a matter of minutes and seconds.

Exhibit 2J provides a chronological snapshot of one release going down the piracy pyramid, starting from the scene, spreading from private FTP sites to public consumption sites. This one release was publicly available in little more than 30 minutes, which is common.

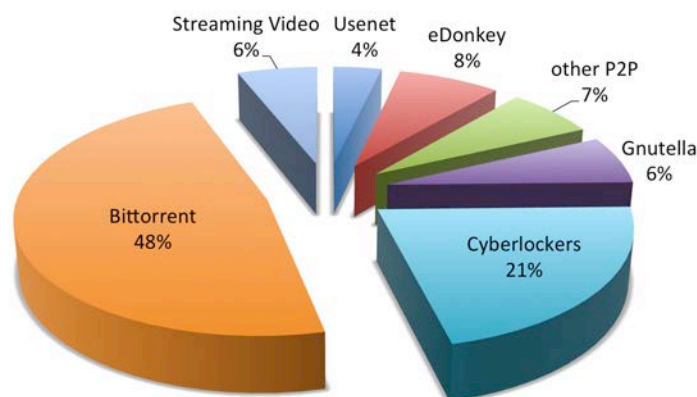
Exhibit 2J: Example of Piracy Speed

| Date | Time | Release Name | Type of Release | Step |
|------------|----------|--------------------------------------|----------------------|------|
| 2015-06-09 | 9:30:37 | screencheat.v2.6.0.8.gog.retail.core | Scene Release | 1 |
| 2015-06-09 | 9:30:37 | screencheat.v2.6.0.8.gog.retail.core | Private FTP | 2 |
| 2015-06-09 | 9:34:32 | screencheat.v2.6.0.8.gog.retail.core | Private Torrent Site | 3 |
| 2015-06-09 | 10:04:00 | screencheat.v2.6.0.8.gog.retail.core | Public/Cyberlocker | 4-5 |

A research study conducted by NetNames (formerly known as Envisional)³, commissioned by NBC Universal, had looked at the global Internet traffic to assess how much of that usage infringed upon copyright. The following exhibit provides a breakdown of the infringing traffic use – which makes up an astonishing 23.76% of global Internet bandwidth:

Exhibit 2K: Infringing (non-pornography) Traffic Use Of Global Internet Bandwidth

(Source: Study conducted by NetNames, commissioned by NBC Universal)



Good Money Going Bad

Owners of pirate distribution sites are making millions from malicious advertising on sites sharing stolen movies and television shows while placing Internet users at increasing risk, according to findings from Digital Citizens Alliance and MediaLink.⁴ The report found that the largest content theft sites generated more than \$200 million in advertising-driven revenues in 2014. Besides the \$209 million in revenue in 2014, Digital Citizens noted other troubling trends:

- **Malware and Unwanted Downloads:** One-third of the sites included links with the potential to infect users' computers with viruses and other malware. In most cases the links are hidden behind Download or Play buttons, but in many cases, it is not even necessary to click on a link to spawn the unwanted download. These downloads earn site owners millions in annual revenue.
- **Video Streaming Spurs Growth:** Consumer demand for streaming video to computers and mobile devices has fueled growth in the content theft world just as in legitimate business. Streaming sites are the growth sectors, with the number of streaming sites up 40% in 2014, allowing content thieves to benefit from higher video ad prices.
- **More Premium Brand Ads Found:** Despite industry and public efforts to crack down on content theft, researchers found more premium brand ads on content theft sites in 2014 than in 2013. This is a danger for the reputation and value of legitimate brands, and should spur even more action to throttle advertising to these sites.
- **Rampant Fraud:** Ads Mislead, Misrepresent and Misdirect: MediaLink and ad effectiveness firm DoubleVerify found that 60% of the ad impressions served by sites with available data were "laundered" – served through phony "front" sites to obscure the ads' ultimate destination. For 15% of the sites, ALL of the impressions were fraudulent in this regard.

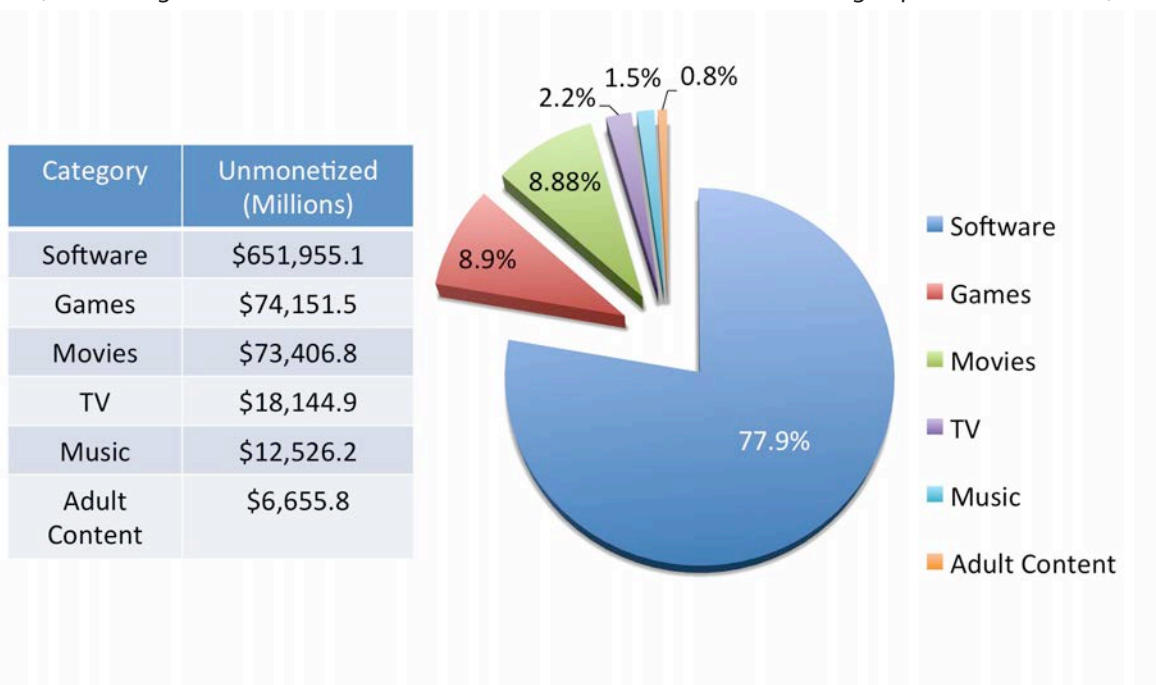
Economics And Business Implications Of Piracy

Piracy is rampant across the Web, with free copies of movies, television episodes, games, music, software, and books consumed through a variety of technical means.

According to a research report released by Tru Optik⁵ detailing the most pirated TV, Music, Movies, Games and Software, more than \$800 billion worth of content changed hands via illegal distribution networks in 2014. Exhibit 2L provides a breakdown of the unmonetized opportunity by area.

Exhibit 2L: Global Unmonetized Demand Full Year 2014

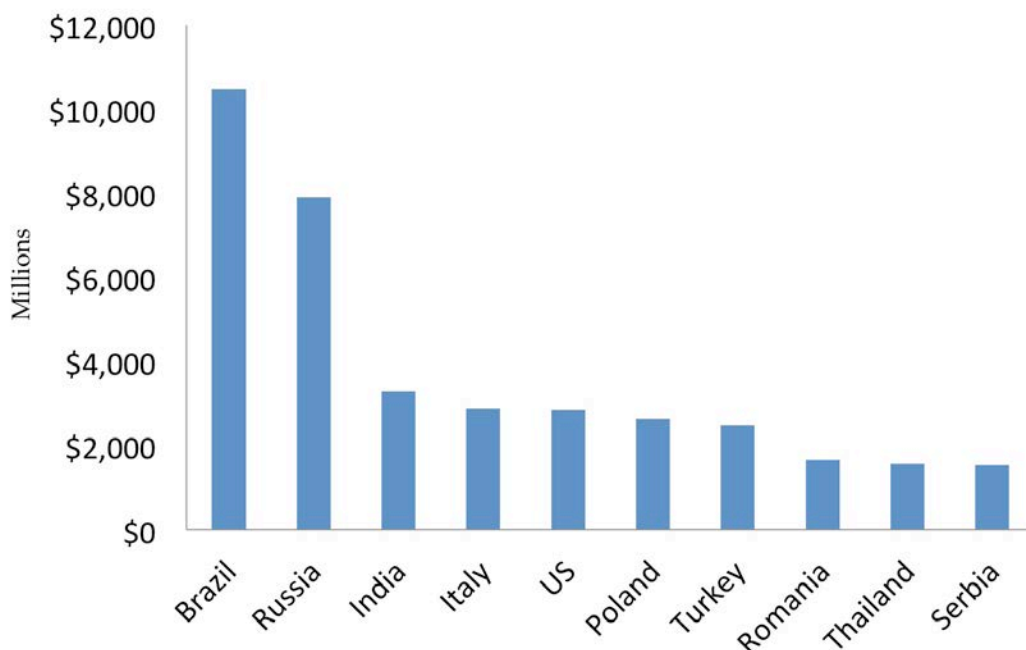
(Source: Digital Media Unmonetized Demand and Peer-to-Peer File Sharing Report: 2014 Review⁵)



Pirated software and digital assets are being exploited/pursued by people around the globe. One recent study found that the top three countries “most guilty” of using pirated content were Brazil, Russia, and India. A full breakdown of the unmonetized opportunity by country is provided in Exhibit 2M.

Exhibit 2M: Global Unmonetized Demand (in Millions) for Full Year 2014 by Country

(Source: Digital Media Unmonetized Demand and Peer-to-Peer File Sharing Report: 2014 Review)



In this study, Unmonetized Demand (UMD) is simply the market value of content exchanged on peer-to-peer networks. For each piece of content shared, Tru Optik assigns a value based on actual retail price or subscription fee. That value is applied to the number of downloads to determine UMD at the individual “file” level. UMD’s are aggregated to determine title, company, and country totals. Note that UMD reflects the value of the content itself – **it does not capture advertising revenue or other content-related monetization streams, and it includes only English language content.**

Unfortunately, with pirated software also comes malware. Malware linked to pirated software has an enormous cost to both businesses and consumers. An IDC study conducted in March 2014⁶ estimated that:

- Enterprises would spend \$491 billion in 2014 because of malware associated with pirated software, which breaks out to \$127 billion in dealing with security issues and \$364 billion dealing with data breaches on PCs and laptops. Almost two-thirds of these enterprise losses will be the result of the activity of criminal organizations.
- Consumers would spend nearly \$25 billion and waste 1.2 billion hours, in 2014, dealing with security issues created by malware on pirated software.




Role Of Unprotected Applications In Enabling Piracy

Vulnerabilities Of Applications

Digital media, gaming and software providers' applications are being deployed unprotected, thus making it easy to infringe on IP, copy and distribute the applications illegally, and modify the applications for nefarious purposes. Hackers typically target application binaries to access source code, steal or expose sensitive data or IP, and/or gain control of application functionality for malicious purposes (e.g., to modify or bypass security controls).

A few easy steps and widely available (and often free) tools (see appendix for the list of tools) make it easy for adversaries to directly access, compromise, and exploit an application's code.

Key risks that these markets face:

| Market | Key Risks (Business and Technical) |
|---|---|
| Digital Media  | <ul style="list-style-type: none">• Content Key Exposure• Stealing decrypted content from the player as it decrypts• Tampering and Reverse-Engineering Applications / Platforms• Piracy• Bypass of License Management Policies and Controls |
| Gaming  | <ul style="list-style-type: none">• Cheating and Vandalism• Piracy• Tampering and Reverse-Engineering Applications• Private Servers• In-app/in-game Purchasing• Bypass of License Management Policies and Controls |
| Software Providers (including ISVs)  | <ul style="list-style-type: none">• Piracy• Intellectual Property Theft• Tampering and Reverse-Engineering Applications• Bypass of License Management Policies and Controls• Malware Insertion• Compromising Security Components |

Vulnerabilities In Software Providers' (ISVs) Applications

An adversary can directly access unprotected application binary code, analyze and reverse-engineer it back to source code, modify the code to change application behavior, and inject malicious code. With the source-code revealed, pirates are able to copy and redistribute the software.

Many Software Providers/ISVs have established common security modules that live inside their applications and provide security functionality, such as authentication policies that govern when and how applications are used. This code can be reverse-engineered or simply extracted, and packaged into a new counterfeit software offering. These packages are generally independently branded and sold at a significantly lower price than the original, eroding the value of product lines.

Software vendors often believe that a license management solution is adequate to protect their software against unauthorized use. However, global software piracy losses are growing despite widespread adoption of license management. There is a parallel economy of professional pirates who **distribute keys and patches that disassociate license management from an application, thus unlocking the software.** Hackers can analyze and then tamper with the unprotected binary to entirely **disassociate license management from the software.** For example, license verification checks are modified to unconditionally return success. Professional pirates rapidly gain expertise in attacking popular license management systems, leading to zero-day attacks where unlocked copies are created and disseminated within minutes and hours of a new software release. Often these are sold at a huge discount through seemingly legitimate "cheap OEM software" web-stores.

Hackers can also reverse-engineer the algorithm used to generate valid keys or verify valid keys, and develop **key generation exploits that generate on demand keys to unlock the software.** Instructions to build key generators are freely available on the Internet, and key generation exploits are widely traded on P2P (peer-to-peer) networks. Hackers can also spoof the presence of a valid license by cloning a license server.

Vulnerabilities In Digital Media Ecosystem

Key discovery is the most prevalent class of threats to Digital Rights Management (DRM) systems today. In order to protect the digital media file from being pirated, DRM systems contain a software media player (in addition to other components – such as file servers, payment systems, etc.) that allows users to download the media file and play encrypted files. This media player contains cryptographic keys to decrypt the encrypted media file. An adversary can extract this key, decrypt the encrypted digital media file, and pirate it.

The second most prevalent attack on digital media applications is **stealing the decrypted content from the player as it decrypts** it via techniques such as memory scraping and grabbing buffers.

Digital media platforms can also be reverse-engineered and tampered with, with, for example to spoof authentication, disable or bypass security controls, and unlock subsidized devices such as media gateways or high-end gaming platforms. DRM technology is easily hacked and its controls are bypassed entirely, leading to rampant media tampering and piracy.

Vulnerabilities In Gaming Ecosystem

Most games include IP, such as optimized implementations, proprietary algorithms, special effects, videos and other features, which represent a significant investment. Game developers that do not prevent these components and code segments from being **reverse-engineered** or lifted are vulnerable to hackers creating counterfeit me-too products.

Cheating exploits, for example through automated bots, are a big threat to the popularity and value of multiplayer online games. Goals of cheating include manipulating a player's position or velocity, being able to see through walls, or acquiring tools or privileges without legitimately earning the corresponding points. This causes degradation of the gaming experience, diminishes the element of fun, and can lead to rapid loss of subscribers. Related to pirated games, professional pirates will **reverse-engineer the client and client-server communications to create counterfeit servers or "gray shards" and set up entire communities of gamers – directly stealing revenue from the game publisher.** Hackers in this case, distribute hacked versions of the client that drive gamers to a tampered/fake gaming experience.

Games are increasingly distributed online. E-activation scenarios include conversion from try to buy, or upgrade of a game after installation. The software routines that implement and enforce the licensing status of a game are subject to tampering attacks, as is all **license-managed software**. While some games overcome this by requiring constant connectivity to a server, always-on measures are hugely unpopular with users.

Vulnerabilities of Mobile Apps

Mobile apps applications are also vulnerable to most of the threats described above. Mobile applications are vulnerable to reverse- engineering, repackaging, republishing and are susceptible to becoming malicious weapons.

The Open Web Application Security Project (OWASP) created a list of the top vulnerabilities for mobile applications that should be addressed. These vulnerabilities are known as the OWASP Mobile Top 10, see appendix for the details.

Unfortunately, a number of these vulnerabilities are not being addressed – thus, leaving many mobile applications exposed to hacking.

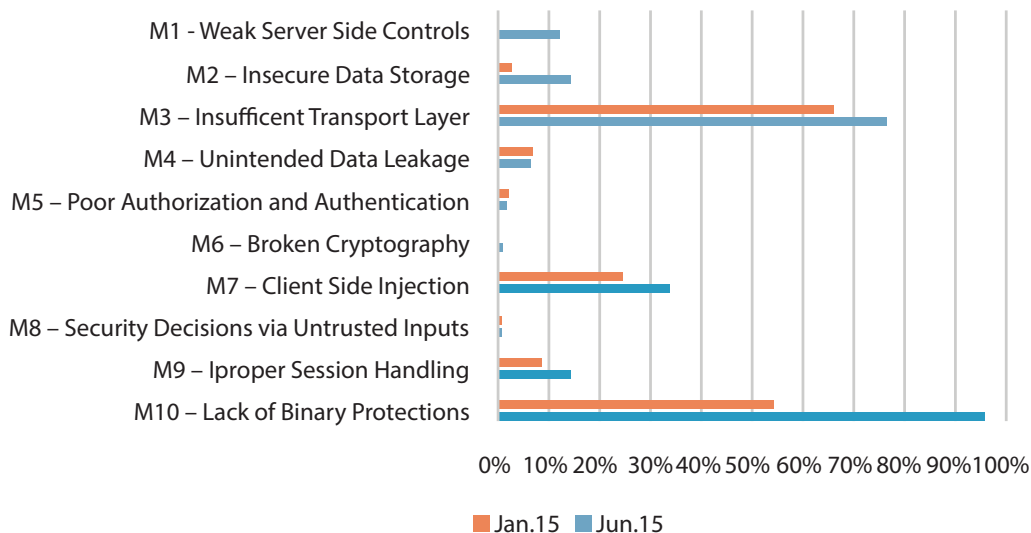
Findings generated from MetaIntelli's AppInterrogator™ platform revealed that key vulnerabilities are not being addressed, and the situation is not improving. The numbers are worse now (June 2015) than they were when last analyzed in Jan 2015 - particularly for M10 (Lack of Binary Protection) and M3 (Insufficient Data Leakage). See Exhibit 2N for details.

About MetaIntelli's AppInterrogator

The heart of MetaIntelli is the AppInterrogator™, a purpose-built fully-automated platform continuously gathers intelligence from multiple sources applying multivariate analysis that tracks down and identifies all the risks before they become threats. This also includes the ability to detect the Content, Context, Intent and Predictive Analysis for hands-off application investigation using multiple processes running asynchronously in parallel to identify, collect and report privacy and security risks. AppInterrogator gathers everything from malware to data manipulation with detailed quantitative and qualitative results to match specific security, privacy and risk needs. As an autonomic computing engine it is self-learning and continuously builds upon its intelligence base adapting to change and reassessing apps to determine if their risk posture has changed.

Exhibit 2N: Analysis of How Well The OWASP Mobile Top 10 Vulnerabilities are Addressed*

(Source: MetaIntelli Analysis, June 2015)



*Note: Analysis was done on approximately 96,000 apps from Google Play store in June 2015. The Jan 2015 analysis did not review M1 or M6

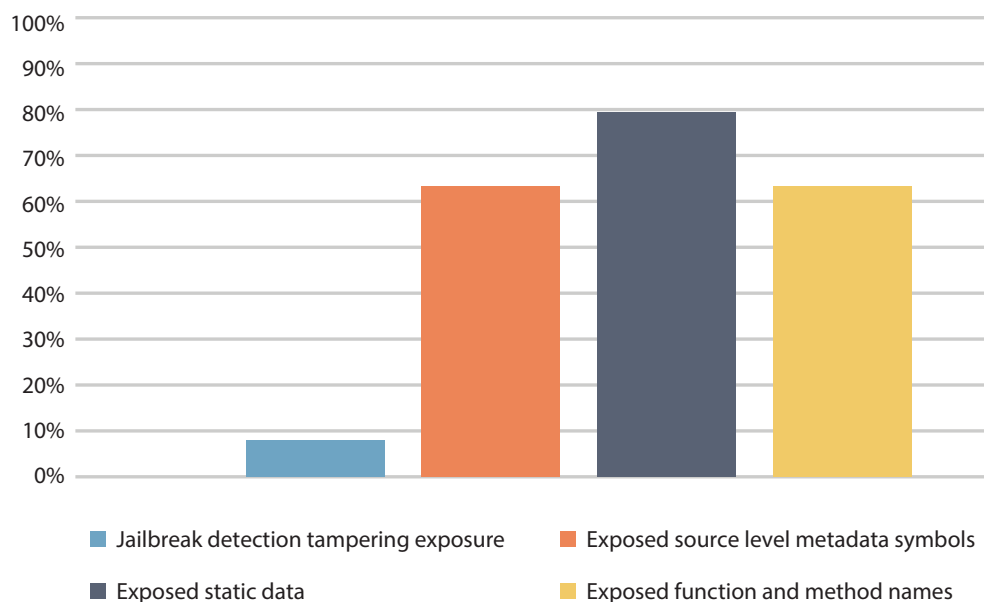
When the binary code was not protected, MetaIntelli analysis revealed a number of exposures in the applications. Specifically they found:

| Exposure area | Description The ability of a hacker to easily... |
|--|--|
| Jailbreak Detection Tampering Exposure | Bypass jailbreak or root detection logic |
| Exposed source level metadata symbols | Examine metadata information |
| Exposed Static Data | Extract static data symbols, and analyze the associated data |
| Exposed function and method names | Extract strings of interest and locate the associated code, which may help adversaries in subsequent attacks |

Exhibit 20 illustrates that the majority of mobile applications have exposed metadata symbols, static data, and function and method names – all of which greatly assist hackers.

Exhibit 20: Analysis of Google Play Apps That Do Not Offer Binary Protection

(Source: MetaIntelli Analysis, June 2015)

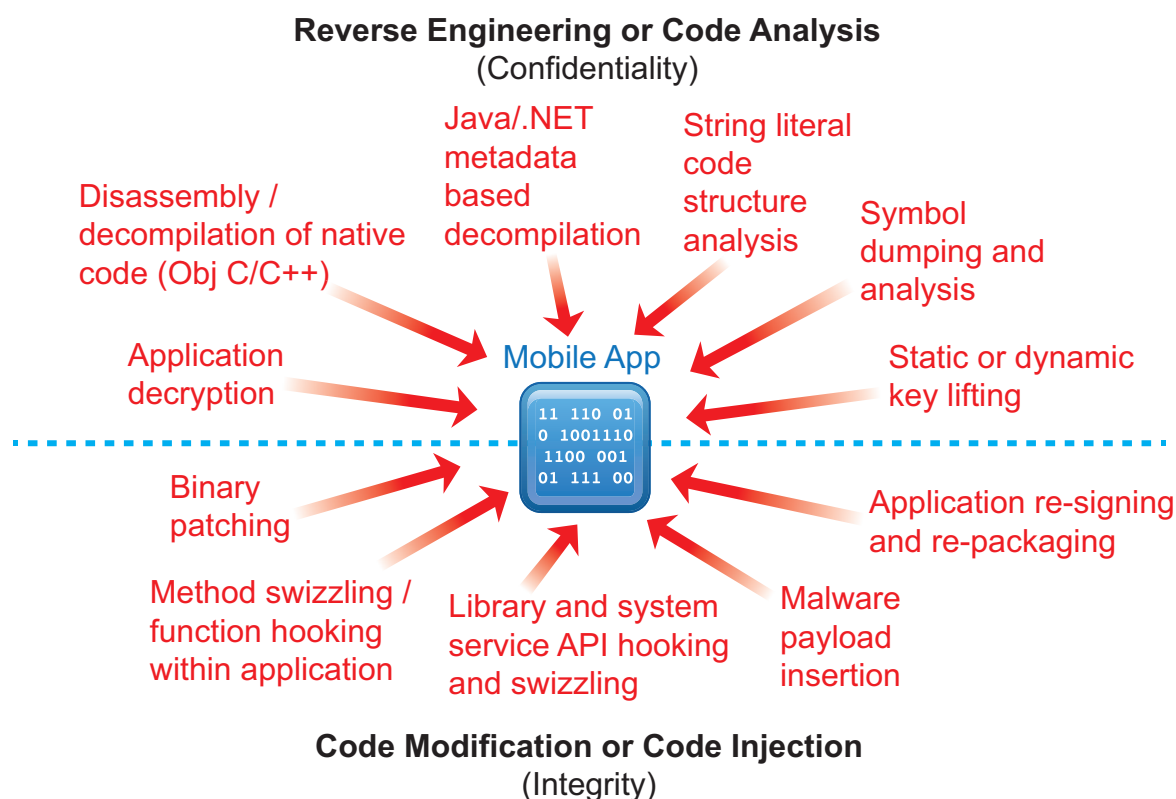


These findings did not significantly vary based on type of applications (e.g., business, medical, health & fitness, music & videos, games, finance, etc.).

Mobile apps that do not have binary protection are exposed to the threats shown in Exhibit 2P:

Exhibit 2P: Summary of Reverse Engineering and Integrity Risks that Mobile Apps, with Unprotected Binary Code, Are Susceptible To

Mobile App Attack Vectors for Binary Hacking



3. Recommendations To Mitigate Digital Piracy

A concerted focus and holistic approach to protecting software – including the software that governs access to digital media – is needed to thwart the growing piracy problem.

Those responsible for cybersecurity should:

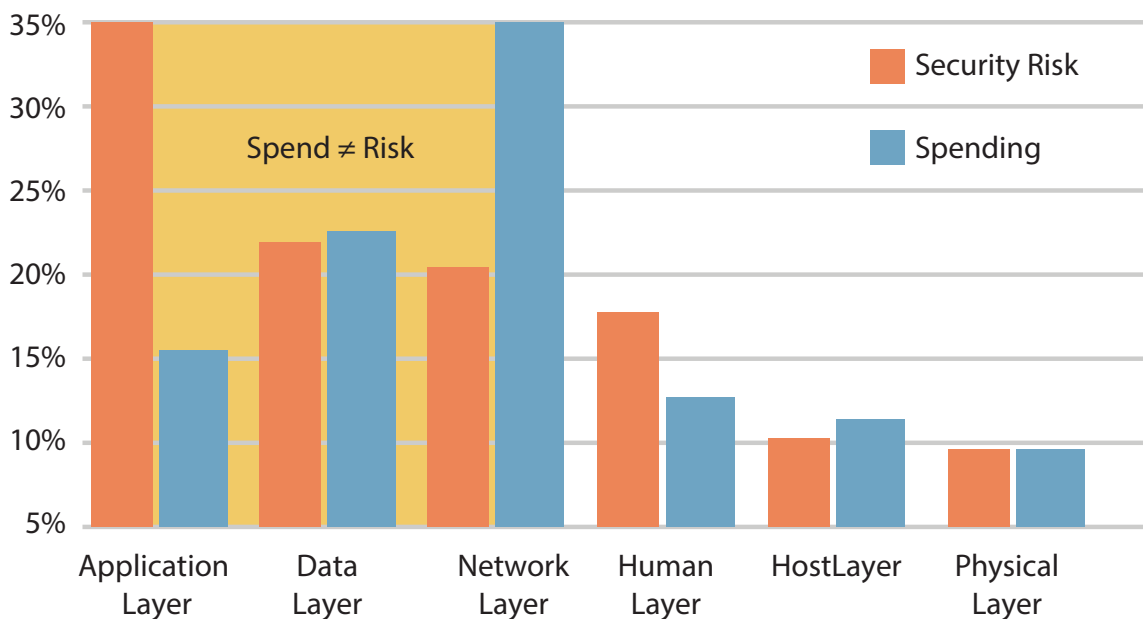
1. Rethink their security investment approach – considering how much time and money is spent on application security

Many organizations are not investing adequately in application protection. In looking at mobile applications, for example, a 2015 Ponemon Institute study sponsored by IBM found that 50% of organizations had zero budget allocated to protecting mobile apps.

The same research found that security spending was not in line with security risks, and that the spending on applications was not commensurate with the risk (See Exhibit 3A below).

Exhibit 3A: Where Are Your Security Risks vs. Your Spend?

(Source: Ponemon Institute Study sponsored by IBM Security, Mar. 2015)



Consistent with the findings from the Ponemon study, Gartner recently advised CISOs (Chief Information Security Officers) to “make application self-protection a new investment priority, ahead of perimeter and infrastructure protection”, further suggesting that “every app needs to be self-aware and self-protecting.”⁸

2. Build run time protections into your applications

Protection against “typical app break-ins,” and even more advanced break-ins, can be realized achieved through with Application Hardening and Run-Time Protection. Hardening and Run-Time Protection can be achieved with no impact to your source code, via an automated insertion of “guards” into your the binary code. When implemented properly, layers of guards are deployed so that both the application and the guards are protected, and there’s no single point of failure.

“For critical applications, such as transactional ones and sensitive enterprise applications, hardening should be used.”⁹

3. Protect your cryptographic keys

17% of known software pirates are key-generators – so keys are under attack. There are numerous ways to protect keys, including white box cryptography solutions that mask static and dynamic keys at run-time/in memory and while applications are at rest.

4. Leverage vulnerability testing and ensure that known risks – including those identified in the OWASP mobile top 10 list, in particular, are addressed.

5. Invest in intelligence tools to understand if rogue versions of your apps are being distributed “out in the wild” – because if they are, it’s likely that they’ve been tampered with and you are losing money, and your brand it at risk, etc. Separate analysis has shown that over 50% of Fake Apps are Malicious.¹⁰

6. Lobby organizations that are responsible for setting standards and rules and penalizing/ criminalizing piracy, particularly for mobile apps. There is a need for global consistency of both rules and enforcement standards.

4. Appendices

Appendix A: Footnotes

¹ Source: <http://www.zdnet.com/article/ios-versus-android-apple-app-store-versus-google-play-here-comes-the-next-battle-in-the-app-wars>

² Source: IDC, May 2015 - <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>

³ Source: An Estimate of Infringing Use of the Internet - http://documents.envisional.com/docs/Envisional-Internet_Usage_Report-Summary.pdf

⁴ Source: Good Money Still Going Bad: Digital thieves and the hijacking of the online ad business

⁵ Source: Digital Media Unmonetized Demand and Peer-to-Peer File Sharing Report: 2014 Review

⁶ Source: Joint research by National University of Singapore and IDC on the prevalence of malware found in pirated software

⁷ Source: Gartner: "Stop Protecting Your Apps; It's Time For Apps to Protect Themselves", Sept. 25, 2014

⁸ Source: Gartner, Avoiding Mobile App Development Security Pitfalls May 24, 2013, refreshed July 7, 2014

⁹ Source: Trend Micro Research: Fake Apps Feigning Legitimacy, 2014

Appendix B: Glossary

Couriers – Couriers are a specific class of topsite users who earn their access by uploading new releases and filling requests.

Cyberlocker – An Internet hosting service specifically designed to host user files.

DC++ hubs – A free and open-source, peer-to-peer file-sharing client that can be used to connect to the Direct Connect network or to the ADC protocol.

FTP Top Site or Topsite – A term used by the warez scene to refer to underground, highly secretive, high-speed FTP servers used by release groups and couriers for distribution, storage and archiving of warez releases.

IRC [Internet Relay Chat] channel – An application layer protocol that facilitates the transfer of messages in the form of text. The chat process works on a client/server-networking model. IRC clients are computer programs that a user can install on their system.

Pretime – How quickly a tracker releases a particular scene release after other trackers.

Private BitTorrent Sites – Closed sites that require you be invited by another user and create an account in order to use the service.

Release Group – A group of people who release software, music, games, videos and other things over the internet, usually bypassing copyright protection, or offering some sort of program to help, like a keygen or no-cd crack. Often referred to on the internet as “the Scene”.

Scene or “the Scene” – An underground community of people that specialize in the distribution of copyrighted material, including television shows and series, movies, music, music videos, games (all platforms), applications (all platforms), ebooks, and pornography. The Scene is meant to be hidden from the public, only being shared with those within the community.

Topsite – A term used by the warez scene to refer to underground, highly secretive, high-speed FTP servers used by release groups and couriers for distribution, storage and archiving of warez releases.

UseNet/NZB/Newsgroup – An early non-centralized computer network for the discussion of particular topics and the sharing of files via newsgroups.

XDCC/FSERV/DCC – A computer file sharing method which uses the Internet Relay Chat (IRC) network as a host service.

Appendix C: Readily Available Tools Make It Easier To Hack

| Category | Example Tools |
|--|--|
| App Decryption/Unpacking/Conversion | <ul style="list-style-type: none">• Clutch• APKTool• Dex2jar |
| Static Binary Analysis, Disassembly, Decompilation | <ul style="list-style-type: none">• IDA Pro & Hex Rays (Disassembler/Decompiler)• Hopper (Disassembler/Decompiler)• JD-GUI (Decompiler)• Baksmali (Disassembler)• Info dumping: class-dump-z (classes), nm (symbols), strings |
| Runtime Binary Analysis | <ul style="list-style-type: none">• GDB (Debugger)• ADB (Debugger)• Introspy (Tracer/Analyzer)• Snoop-It (Debugging/Tracing, Manipulation)• Sogeti Tools (Dump key chain or filesystem, Custom ramdisk boot, PIN Brute force) |
| Runtime Manipulation, Code Injection, Method Swizzling, Patching | <ul style="list-style-type: none">• Cydia Substrate (Code Modification Platform) (MobileHooker, MobileLoader)• Cycrypt / Cynject• DYLD• Theos suite• Hex editors |
| Jailbreak Detection Evasion | <ul style="list-style-type: none">• xCon, BreakThrough, tsProtector |
| Integrated Pen-Test Toolsets | <ul style="list-style-type: none">• AppUse (Custom "hostile" Android ROM loaded with hooks, ReFrameworker runtime manipulator, Reversing tools)• Snoop-It (iOS monitoring, Dynamic Binary Analysis, Manipulation)• iAnalyzer (iOS App Decrypting, Static/Dynamic Binary Analysis, Tampering) |

Appendix D: Overview of iThreat Cyber Group's Services

Since ICG's iThreat Cyber Group's (ICG) inception, it has investigated and identified sources of information leaks facilitated by the Internet and by technology in general. This work serves as a foundation for ICG's Anti-Piracy (AP) and Intellectual Property Protection Services (IP), and has shaped ICG's unique approach in these industries. Our approach is to identify and help mitigate or eliminate the earliest and most prolific sources of infringing content. As described below, ICG believes, in almost all cases, once infringing content is released to Internet-connected systems, it quickly spreads far and wide and is made easily accessible by anyone wishing to download the infringing content via numerous possible methods of consumption. Once the source releases infringing content anywhere, it is quickly available for consumption everywhere.

ICG's source piracy analysis tools pertinent to this report include:

iDupecheck™: A proprietary ICG monitoring system which collects near-real-time announcements regarding Internet release of infringing content directly from both private infrastructure and public sources. iDupecheck™ aggregates this information into a stream of source intelligence on infringing content, including software, released on the Internet. ICG is able to query this system by software product name and by company name to find evidence of pirate release of software titles intended for use on Mac and PC systems. ICG notes most major software pirate releases include the infringed upon company name in the pirate release name, in addition to the infringed upon title name.

Mobile iDupecheck™: A proprietary ICG monitoring system which collects near-real-time announcements regarding posting of mobile device applications to unauthorized repositories enumerated by ICG. ICG considers all mobile devices using unauthorized mobile app repositories to be at-risk devices; low level malware/exploits on these devices inherent in malicious mobile applications may expose information about the user, to include login credentials and personal information entered into mobile applications published by Arxan customers and potential clients.

Appendix E: OWASP Top Ten Mobile Risks

Early 2014, OWASP, leading application security industry authority, published the Top Ten Mobile Risks based on new vulnerability statistics in the field of mobile applications. Following diagram is the representation of the mobile application threat landscape according to OWASP.



OWASP concluded that the lack of binary protections within a mobile app exposes the application and its owner to a large variety of technical and business risks, resulting in the following business impacts:

- Privacy Related and Confidential Data Theft
- Unauthorized Access and Fraud
- Brand and Trust Damage
- Revenue Loss and Piracy
- Intellectual Property Theft
- User Experience Compromise

OWASP also identified the risks involved with Client Side Injection. Client-side injection results in the execution of malicious code on the mobile device via the mobile app, and direct injection of binary code into the mobile app via binary attacks. This will result in the following business impacts:

- Fraud
- Privacy Violations