August 2012

Feature article: An Offer You Can’t Refuse

Table of Contents

An Offer You Can't Refuse

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

This is the tale of a 419 scammer who may have had one too many Vodka Martinis (shaken, not stirred): it's actually the merging of two articles, one for SC Magazine's Cybercrime Corner, and the other a spin-off/explanatory piece.

My friend and colleague Urban Schrott drew my attention to a spam/scam mail that caused some hilarity over at ESET Ireland. The message has the subject YOUR LIFE IS IN DANGER. It comes from someone who isn't sure whether his name is Spike Dwaggin or Dai Teatime (or possibly NIKITA…), and it runs like this.

> *As I sit here sipping a martini it is my regretful duty to inform you that you have been selected for assassination.*
>
> *I am a professional assassin (I enclose my certificate of assassination as proof) and SMERSH have contracted me to assassinate you and have specifically paid extra for a particularly nasty death which makes it look like you died in a particularly bizarre sex game gone wrong; I had already bought the shire horse stallion (he's called Henry – picture attached), the lard and the dragon dildo (from Bad Dragon of course, I only use the very best tools) when I found out that you are innocent of the accuse, so I make out this time to contact you. Unfortunately international crime syndicates won't admit to mistakes and cancel the hit so I will be forced to carry out the assassination on you. Sorry about that old chap but rules are rules.*
>
> *There is an option for me to help you in other for you to know who had paid SMERSH for your DEATH and don't forget my men had been monitoring you for the past few days and daily record of your activities is been sent to me but I have refuse to order your DEATH.*
>
> *Get back to me if you value your LIFE with all due speed or else I regret I will have to carry out my original contract to assassinate you and although he is quite charming for a horse I don't think Henry is the most sensitive of lovers.*
>
> *Toodle Pip!*
>
> *Dai Teatime*
> *International Assassin*

As it happens, I've seen quite a few 419s using this "I've been paid to kill you but I'm giving you a chance to pay me to turn the tables" ploy in the past, but I've never seen a version with such a mish mash of popular culture references.

In fact, I was inclined to think it was some kind of spoof rather than a genuine variant of this particular type of 419, but further checking on a scam-baiter forum indicated that the scammer is perfectly willing to take money from anyone who falls for this nonsense. And if you were wondering what a certificate of assassination looks like, it turns out to look like something designed on a Gameboy by a Pokemon with a propensity for doing unspeakable things to goats: yes, one of the scam-baiters asked Spike – is that a Buffy reference? – to supply it, since it wasn't attached to the original mail. No photo is available currently of Henry the Horse, or the Bad Dragon dildo.

- James Bond and SMERSH: If your knowledge of James Bond is limited to the movies, you may be unaware that a fictionalized version of SMERSH (a real Russian counter-intelligence agency that was wound up in 1946) plays a

significant part in the very early novels. Oddly enough, a lot of commentary on this 419 misses the fact that SMERSH and SPECTRE (a purely fictional criminal organization) are by no means the same thing, though there seems to be a certain amount of traffic from one to the other in terms of personnel. A bit like the AV industry…

- The Beatles (and of course, Henry the Horse dances the waltz) If the naming of the horse wasn't influenced by 'Being for the benefit of Mr Kite', from the Sergeant Pepper album, it's a remarkable coincidence.

- The Russian Empress Catherine the Great was said (quite untruthfully) have died as a result of a somewhat over-intimate relationship with a horse.

- (La Femme) Nikita was a film and subsequent TV series about an assassin.

- And even the somewhat Saintly Toodle Pip! If your knowledge of The Saint is restricted to one or more TV series or maybe a movie or two, you may not be aware of the period charm of the earlier books, which were very much of their time – the very long series of books began in the 1920s. Of course, while Simon Templar may have inclined sometime to the amoral, assassination wasn't really his thing. But Toodle Pip just brings the memory of those books back to me.

And surely Dai Teatime (despite the murderous pun) must be either a friend of Bertie Wooster's or some kind of homage to ESET's former counselor for comment spammers, Letitia Teaspoon, now carrying on the good work at Small Blue-Green World. In fact, she's even now giggling girlishly in the next office.

It's hard to imagine anyone taking this seriously, but it's been circulating for a while, and not only in Ireland, so either the scam works often enough for the scammer to think it still has some mileage, or else he's letting it run while he works on his next persona: Conan the Barbarian, perhaps, or Doc Ock, or possibly Kraken D'Waggin. As it happens, I'd never heard of that last one, but I figured a Google search for the scammer's name was going to turn up some kind of pop-culture reference, and I wasn't disappointed. However, a comment on my Chainmailcheck article from Robert provided me with even more information. He told me that "spike dwaggin (dragon) is the little dragon from my little pony, friendship is magic. dai teatime is equally funny: if the letters of the word dai are converted to numbers, it forms 419. and Mr. Teatime (spelled teh ah ti meh) is the assassin from Terry Pratchetts diskworld-book Hogfather."

All very bizarre and amusing, but it's definitely not a message that should have you reaching for your cheque-book.

The Industrialization of Criminal Malware

Stephen Cobb, CISSP, ESET Security Evangelist

Industrialization in the context of malware threats refers to a number of trends that collectively contribute to increasing the efficiency with which criminals can use malicious software to make serious money. Industrialization has been a common theme in discussions of cybercrime and malware for some time now, but many organizations are still unaware of how this phenomenon drives the emergence of new threats (and the corresponding implications for system security posture). This article is an effort to explain how and why this industrialization of malware is happening.

How it happens is through the application of well-established industrial or commercial methods to malicious code creation, distribution, and exploitation. We think five methods are central to the phenomenon: division of labor, specialization, markets, standardization, and modularity. Why it happens is to maximize profit, which we illustrate with a threat that is ongoing in numerous countries, the use of ransomware to frighten people into paying a phony fine to the police.

In the early days of criminal malware—defined as code such as viruses and worms that is employed to steal from people and organizations—the malware author and the criminal were often one and the same person. For such a person to steal money or data using malware required multiple skills, from coding to network manipulation, from marketing to money laundering. You had to come up with an effective way to trick people, write and distribute the code required, and then reap the financial rewards without getting caught.

(See Annex - Image 1)

Over time, a market-based economy has arisen to supply all of those skills, for a price. A criminally-minded person can now shop around to put together all the pieces of a cyber-crime operation without personally possessing all of those different skills. This is a classic case of division of labor, which in turn fosters specialization.

Someone skilled at malware coding can get paid for that skill, and thus improve it, free from the distraction of developing a payment system, and also free from many of the risks inherent in crimeware deployment. The malware coder can sell his skills and output at the going rate in a thriving underground market, but the industrial malware model does not end there.

Driven in part by the law enforcement and Internet Service Provider crackdown on spammers in the last decade, malware authors perfected the technology with which to secretly control large numbers of infected/compromised computers working together as a botnet. Economies of scale drove the very logical evolution from the single-purpose botnet, perhaps deployed for either spamming or denial of service attacks, to the multi-purpose botnet, the modular design of which allowed different tasks to be pushed to the same collection of compromised machines without having to repeat the infection process. Here is how ESET Malware Researcher Jean-Ian Boutin describes Win32/Gataka, an information-stealing Trojan that can read all of your web traffic and alter the balance displayed on your online banking page to hide fraudulent transfers: “It exhibits a modular architecture similar to that of SpyEye, where plugins are required to achieve most of the malware functionality.”

In other words, the infection process can be perfected separately from the exploitation process and efficiently leveraged through markets. A person might choose to make money from selling or renting infected machines which are then exploited by someone skilled at monetizing any one of the many possibilities that a botnet presents: DDoS, data harvesting, spamming, spying, fraudulent bank transactions, and so on. Consider how ESET Senior Malware Researcher Aleksandr Matrosov describes Win32/Festi, one of the three most active spam botnets worldwide in May of 2012:

“Thanks to plugin modules Win32/Festi is capable of being used for distributed denial of service (DDoS) attacks. The malware's kernel-mode driver implements backdoor functionality and is capable of updating configuration data from the C&C (command and control server) and downloading additional dedicated plugins.”

One further trend now emerging is the standardization of code

so that it can be deployed on different botnets. Consider the art of "html injection" or webinject, which can be used to insert rogue form fields in an otherwise legitimate web page, thereby harvesting additional data from the target. In his most recent post about Win32/Gataka, ESET's Boutin notes:

"In one campaign we have followed, Win32/Gataka botnet operators make use of advanced webinject configuration that can be used by different types of malware...People specializing in writing webinject configuration files are able to sell their work to a larger customer-base and are not tied to a particular type of malware. By allowing the script itself to communicate with the control panel, it is easier to implement compatibility with a wide range of information stealing malware."

So, we are now seeing the cumulative effects of these industrial factors of standardization, specialization, modularity, division of labor, and markets. Better malware can now be deployed faster, and evolved faster to evade detection and improve profitability. Consider the current plague of ransomware that presents victims with a fake FBI demand for money. The design of the ransom page is of a higher quality than the average scam. The way the malware takes over the victim's PC is very effective. The malware delivery mechanism is hard to avoid. The malware itself is difficult to remove. The overall scheme has been tested and improved over time through deployment in multiple countries. The result is, until the perpetrators are apprehended, a profitable and relatively low-risk criminal activity. We are likely to see more of the same as criminals exploit the benefits of industrialized malware.

Threatsense 2012 – the sequel

The malware that some people are calling Dorifel or XDocCrypt (ESET detects it as Win32/Quervar.C and has a cleaner for it here), had enormous impact this month, mostly in the Netherlands. It has some very interesting characteristics and a fascinating resemblance to Win32/Induc, as a technical analysis by Róbert Lipovský makes clear: Quervar – Induc.C reincarnate?.

However, it turns out that it is being used for scamming purposes that even its authors may not have anticipated. Indian support scammers are using it to convince potential victims in the Netherlands that they need to let the scammer 'clean' or 'protect' their systems. For a price, as always…

In fact, I was contacted in a somewhat similar vein a few days ago by a lady with an Indian accent (yes, yet another): she told me that there is a virus wreaking havoc in the UK and that she would help me to protect my system from it. For a price, no doubt. However, she was unable to tell me anything about this supposed virus, and when I told her (quite truthfully as it happened) that I wasn't using a Windows machine, she told me she was unable to 'help' me and rang off while I was still telling her not to confuse helping me with helping herself to my money.

She gave her name as Anna, but I'm not sure if she was the same 'Anna' who contacted me earlier in the month, claiming that my PC had been sending error messages to her in Uttar Pradesh and trying to prove to me that she knew something about my system using the CLSID gambit. She put the phone down when she realized I wasn't buying it and was trying to get her to tell me what she thought the ASSOC program really does.

These scammers almost certainly have no real connection or knowledge of Quervar or other real malware. (Or even PC technology in general: Anna II was totally confused by the enforced departure from her script, when I told her I was using

a Mac at that time, and had to ask her supervisor for advice on what to tell me.) What we're seeing here is more akin to the gambit blogged here in July by Righard Zwienenberg – Scareware on the Piggy-Back of ACAD/Medre.A – where the threat (rather than the actuality) of real malware is used to sell an ineffective solution. (I won't revisit the use by certain security vendors of spurious claims about spurious malware to sell legitimate AV by somewhat unethical means, infuriating though I find it: see Scareware and Legitimate Marketing.)

This may just be a new twist like the misuse of the VERIFY utility that also crossed my radar this month: Misusing VERIFY (and other support scam tricks). But it suggests the possibility of very specific geographical targeting, mapping the prospective victims to the region where the impact of the malware is (at present, anyway) likely to be greatest.

But it's not all bad news.

When a support scammer tries to get you to hand over your credit card details in exchange for a fraudulent virus removal and system protection 'service', an important part of the scam involves persuading you to give them remote access to your system.

According to reports from the UK, the scammers often use the logmein.com remote access service (I see reports of Team Viewer being used, too), but in the US, they make use – more often than not – of ammyy.com. In fact, the scam is often referred to in the US as the ammyy scam, though I haven't seen indications that Ammyy LLC is directly implicated in the fraudulent use of its service.

However, it seems that Ammyy is aware of the problem and is eager to disassociate itself from the scam. The company says:

"!!! If you receive a phone call claiming to be from 'Microsoft' or someone claiming to work on their behalf, telling you that you have a virus on your computer or some errors which they will help you to fix via Ammyy Admin, it is definitely a scam. "

The company also has advice for people caught out by scammers: firstly to turn off their internet connection and contact their bank to freeze their bank accounts – that may be overkill, but I can't say it isn't worth considering the possibility of your financial services having been compromised; secondly, to reboot and scan for viruses. Again, a sensible precaution, even if we haven't seen confirmed reports of out-and-out malicious software so far. And for people wondering how they can be sure the crooks can't regain access, this is a passage that many people will appreciate:

"…make sure Ammyy Admin Service isn't installed and doesn't run in automatic mode. For this go to main window of Ammyy Admin -> Ammyy -> Service -> Remove. Then restart your PC again."

The company also assures us that if you don't want to use Ammyy Admin, you don't have to uninstall it, just delete the .EXE.

Mobile Mugging: Phoning in the Attack

Róbert Lipovský

Once upon a time, criminal attacks on mobile phone users were mostly restricted to theft and mugging. That type of attack hasn't gone away, but in the age of the smartphone, there are plenty of other ways to skin a cat (or fleece a victim). Virtual mugging is alive and well and coming to a smartphone near

you.

We have seen a dramatic increase in the detections of mobile malware, especially on the Android platform, due to its popularity among users and therefore also among cybercriminals. Attached is a graph illustrating the number of detections of Android malware over the last 12 months – the increase from a few sporadic malware occurrences to a serious threat is quite obvious.

(See Annex – Image 2)

mTAN mADness

A real world scenario for a home user is when the user is attacked by a banking trojan. In order to overcome two-factor authentication implemented as mTANs (mobile Transaction Authentication Numbers) sent in SMS (text) messages, the criminals employ the mobile components of banking trojans. The scenario would go like this:

1. User's computer gets infected by banking trojan through drive-by-download

2. The banking trojan is activated when the user types in his bank's website address

3. It inserts an HTML element in the bank's website asking for the user's mobile phone type (e.g. Symbian, Android, etc.) and telephone number under the false pretense of a new security certificate

4. The user gets an SMS with a download link for the make-believe certificate, which is, in fact, the mobile malware component, and installs it

5. The banking trojan on the desktop computer makes a bank transfer to the criminal's bank account, without the user's knowledge

6. The bank sends an authentication SMS to the user's phone, which is forwarded to the attacker by the mobile component. The mobile malware can also mute the phone ringtone sound, and delete the message, so the user won't be aware of what just happened

7. Now that the attacker has the mTAN for authentication, he can proceed to mug the victim.

A business scenario would involve sensitive data from the mobile device (such as contact details or emails) being sent to the attacker.

Top mobile threats

In terms of "threat level" or "seriousness", the abovementioned examples would get top positions. In terms of the most prevalent threats (i.e. the ones that are mostly responsible for the rise in the statistics), simple SMS trojans and mobile adware / PUAs are at the top. An SMS trojan usually contains a hard-coded premium-rate number, to which it silently sends SMS messages, which results in a high telephone bill for the victim, and profit for the attacker. Mobile greyware (i.e. adware and various PUAs – potentially unwanted applications) are a totally different story. As we all know, a lot of free mobile applications are ad supported. But a few of these advertisement networks go a little too far with their unfair practices, collect too much information from the mobile device, make unsolicited changes to the phone (e.g. browser homepage, application shortcuts, etc), display annoying popups, and so on.

The simple and free steps for protecting oneself are actually very similar to PC advice. With PC's we advise people to "think before you click": with phones, the advice is to think before you install an application, as most mobile malware isn't so devilishly sophisticated as to use exploits for installation without the user's content, but rather employs social engineering, masquerades as another popular legitimate app, and so on. A smartphone user should always carefully consider whether the installed application really requires all the permissions that it asks for.

For business users, the advice would extend to employing group mobile policies, banning the installation of applications from unofficial app stores (or, even more strictly, only allowing certain apps from a whitelist to be installed), etcetera.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 4.62%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://blog.eset.com/?p=94 ; http://blog.eset.com/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

2. HTML/ScrInject.B

Previous Ranking: 2
Percentage Detected: 3.55%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

3. Win32/Conficker

Previous Ranking: 3
Percentage Detected: 3.06%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This

threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://blog.eset.com/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

4. Win32/Sirefef

Previous Ranking: 4
Percentage Detected: 2.75%

Win32/Sirefef.A is a trojan that redirects results of online search engines to web sites that contain adware.

5. HTML/Iframe.B

Previous Ranking: 11
Percentage Detected: 2.66%

Type of infiltration: Virus

HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

6. JS/Iframe

Previous Ranking: 9
Percentage Detected: 2.04%

JS/Iframe.AS is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

7. Win32/Dorkbot

Previous Ranking: 5
Percentage Detected: 1.49%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX.
The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

8. Win32/Qhost

Previous Ranking: 21
Percentage Detected: 1.45%

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker.

9. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 7
Percentage Detected: 1.36%

It is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

10. Win32/Sality

Previous Ranking: 6
Percentage Detected: 1.21%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

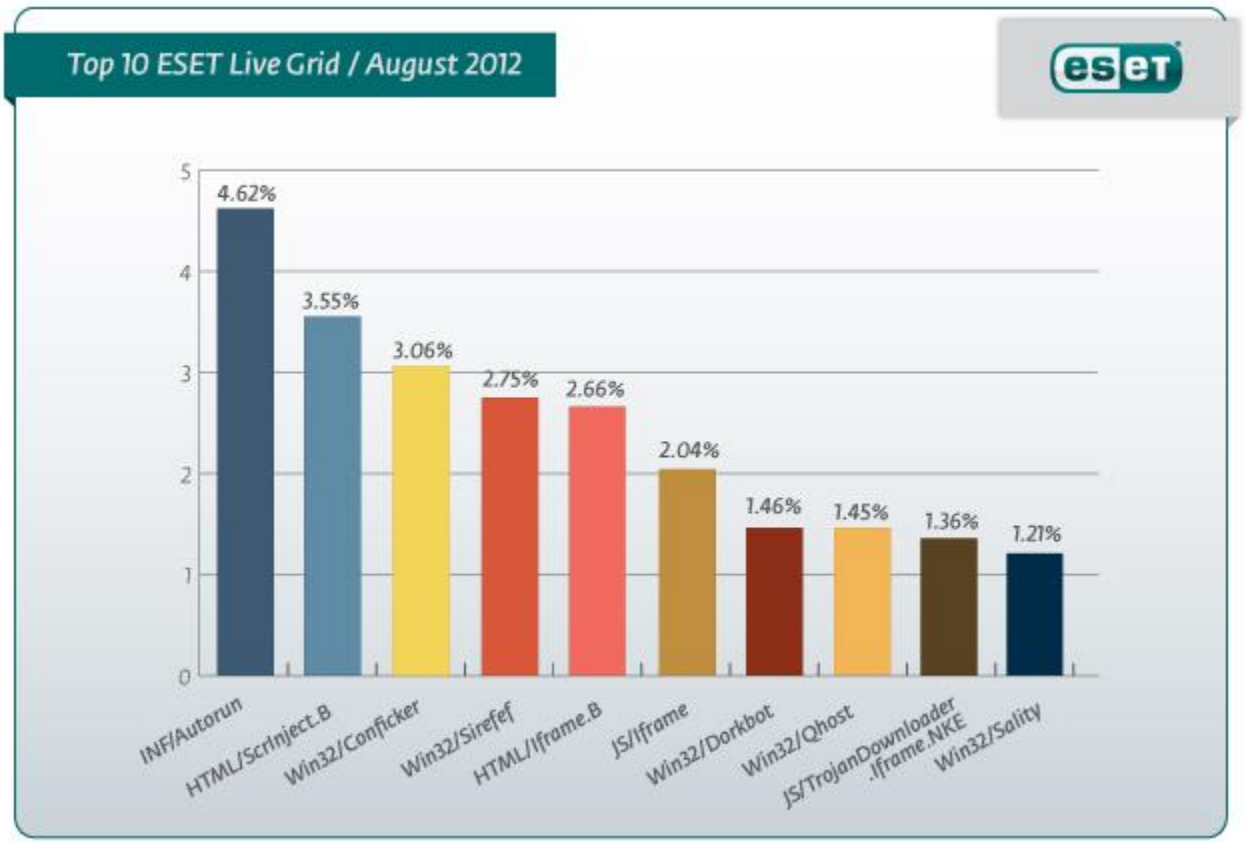
It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature:

http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

Top Ten Threats at a Glance (graph)

Analysis of ESET Live Grid, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 4.62% of the total, was scored by the INF/Autorun class of threat.



Annex

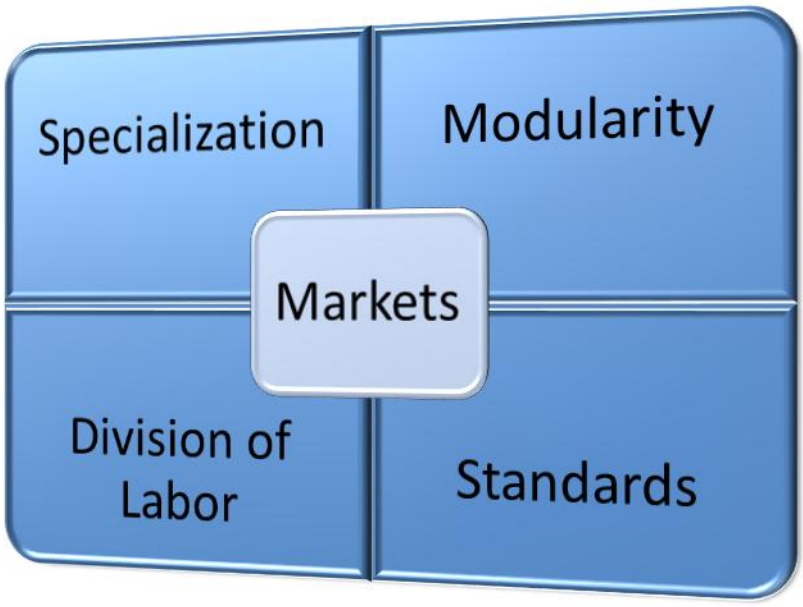


Image 1

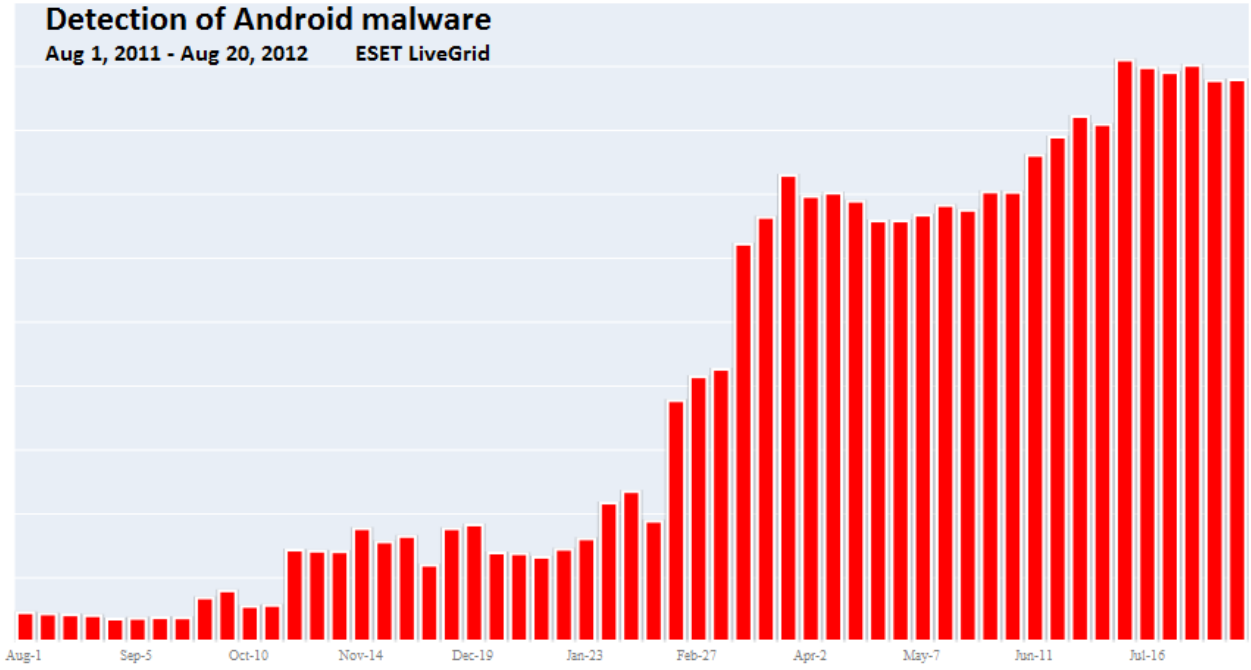


Image 2

About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- ESET Blog
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation