

# ENISA Threat Landscape, Mid-year 2013

In theory, the process of risk management is an ongoing iterative process. However, practical observations show that iteration is often neglected in risk management. There are always “good reasons” to avoid iteration of existing assessments: shift of focus, budget cuts, planning cycles, changing strategic priorities, reorganisations, to name but a few. This is unfortunate because iteration is the only path to maturity improvement: it enhances available knowledge, leads to better assessments, to corrective measures and improves the quality of subsequent assessments. All in all, it helps in understanding reality and smoothly adapting mitigation strategies. In the dynamic cyber security ecosystem this is THE key capability. *Bertolt Brecht* understood this long before information technology, risk and threat analysis:

*“Taught only by reality can reality be changed”*

With this in mind, ENISA presents in this short paper a first “taste” of current developments related to the Threat Landscape 2013. The objectives of this short report are the following:

- *To get better*: Improve our assessment capabilities with regard to emerging trends in cyber security by validating 2012's assessed threat trends<sup>1</sup>;
- *To reflect the reality*: Deliver a consolidated view of the current threat landscape while at the same time providing the grounds for observed deviations;
- *To flag new developments*: Inform the public as early as possible about developments from our on-going information collection. The collected information comes mainly from reports published during 2013 and covers the 1<sup>st</sup> half of 2013.




























The reality check of 2012's assessment is depicted in Figure 1. The notation used for this reality check is the following:

- The prioritization of threats has been taken “as is” from the 2012 assessment.
- Changes in trends - indicated through the arrows - are commented on in the accompanying text.
- We then briefly comment on important issues identified in 2013 regarding the top threats along with references to relevant sources.

An updated prioritization, detailed analysis of threats, trends, threat agents and attack vectors will be delivered in the full ENISA Threat Landscape report to be published before the end of 2013.

---

<sup>1</sup> [https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA\\_Threat\\_Landscape/at\\_download/fullReport](https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport), accessed 22 August 2013.

Top Threats	Trends assessed in 2012	Current trends mid 2013	
1. Drive-by exploits			 <a href="#">Interesting developments</a>
2. Worms/Trojans			
3. Code Injection			 <a href="#">Interesting developments</a>
4. Exploit Kits			
5. Botnets			 <a href="#">Interesting developments</a>
6. Denial of Service			 <a href="#">A change has been identified</a>
7. Phishing			
8. Compromising Confidential Information			
9. Rogueware/ Scareware			 <a href="#">A change has been identified</a>
10. Spam			
11. Targeted Attacks			 <a href="#">Interesting developments</a>
12. Physical Theft/Loss/Damage			
13. Identity Theft			 <a href="#">Interesting developments</a>
14. Abuse of Information Leakage			
15. Search Engine Poisoning		<b>Unable to assess trend!</b>	 <a href="#">No much data found!</a>
16. Rogue Certificates			





Legend:  Declining,  Stable,  Increasing,  Warning

Figure 1 Overview of Trends assessed in 2012 vs. 2013 mid-year

## Changes in threat trends and interesting developments

Through the ongoing information collection and analysis exercise, ENISA has identified the following changes/interesting developments regarding the threats identified in 2012:

**Drive-by-exploits:** There is a shift from Botnets to malicious URLs as the preferred means to distribute malware<sup>2</sup>. An advantage of URLs as a distribution mechanism lies in the fact that URLs are not such an easy target for law enforcement takedowns. It has been reported that there is an increase in the rate of suspicious URLs compared with 2012<sup>3</sup>. Concluding, one can say that browser-based attacks still remain the most reported threats, whereas Java remains the most exploited software<sup>4,5</sup> for the materialization of this threat.

**Code Injection:** A notable issue with regard to this threat is attacks against popular Content Management Systems (CMSs). Due to their wide use, popular CMSs make up a considerable attack surface that has drawn the attention of cyber-criminals<sup>6,7</sup>. Although no important changes have been reported in 2013 regarding this threat, it is worth noting that cloud service provider networks are used increasingly to host tools for automated attacks<sup>8</sup>, thus implementing an important step in code injection attack vectors.

**Botnets:** Although there is a shift to URLs for malware infection (see Drive-by-exploits above), there are further interesting developments with regard to this threat. Although not new, an interesting aspect of botnet activity reported, is the use of botnet infrastructure to mine Bitcoins<sup>9</sup>. Another important development is the increased use of P2P botnets<sup>10</sup>. Such botnets are difficult (yet not impossible<sup>11</sup>) to locate and take down. Moreover, in Internet Census 2012<sup>12</sup> it has been demonstrated how easy is to create botnet infrastructures by misusing weaknesses in security of massively deployed devices. The Browser-Based botnets is yet another example on how easy is to create a very large botnet infrastructure<sup>13</sup>. Finally it is interesting to observe a rise in TOR-based botnets<sup>14</sup>, while more "traditional" botnet operations seem to be in decline, reportedly due the low interest in "traditional" botnet "business cases"<sup>15</sup>.

<sup>2</sup> <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf>, accessed 22 August 2013.

<sup>3</sup> [http://www.securelist.com/en/analysis/204792292/IT\\_Threat\\_Evolution\\_Q1\\_2013](http://www.securelist.com/en/analysis/204792292/IT_Threat_Evolution_Q1_2013), accessed 22 August 2013.

<sup>4</sup> [http://www.kaspersky.com/about/news/virus/2012/Oracle\\_Java\\_surpasses\\_Adobe\\_Reader\\_as\\_the\\_most\\_frequently\\_exploited\\_software](http://www.kaspersky.com/about/news/virus/2012/Oracle_Java_surpasses_Adobe_Reader_as_the_most_frequently_exploited_software), accessed 22 August 2013.

<sup>5</sup> <http://globenewswire.com/news-release/2013/07/18/561078/10041006/en/Bit9-Research-Shows-Java-is-Most-Targeted-Endpoint-Technology-for-Cyber-Attacks-Widely-Deployed-Older-Versions-Represent-Greatest-Risk.html>, accessed 22 August 2013.

<sup>6</sup> <http://www.h-online.com/open/news/item/CMSs-mostly-vulnerable-through-addons-says-German-security-agency-1894431.html>, accessed 22 August 2013.

<sup>7</sup> <http://securitywatch.pcmag.com/security/310350-wordpress-joomla-sites-under-brute-force-password-attack>, accessed 22 August 2013.

<sup>8</sup> <http://www.firehost.com/company/newsroom/press-releases/firehost-report-suggests-commodity-cloud-providers-are-bolstering-botnet-agility>, accessed 22 August 2013.

<sup>9</sup> [http://www.fortinet.com/press\\_releases/2013/fortiguard\\_threat\\_landscape\\_research\\_team\\_reports.html](http://www.fortinet.com/press_releases/2013/fortiguard_threat_landscape_research_team_reports.html), accessed 22 August 2013.

<sup>10</sup> <http://www.csoonline.com/article/734485/malware-increasingly-uses-p2p-communications-researchers-say?page=1>, accessed 22 August 2013.

<sup>11</sup> <https://threatpost.com/peer-to-peer-botnets-resilient-to-takedown-attempts>, accessed 22 August 2013.

<sup>12</sup> <http://internetcensus2012.bitbucket.org/paper.html>, accessed 22 August 2013.

<sup>13</sup> <http://www.itworld.com/security/366872/black-hat-ad-networks-lay-path-million-strong-browser-botnet>, accessed 22 August 2013.

<sup>14</sup> <http://www.welivesecurity.com/2013/07/24/the-rise-of-tor-based-botnets/>, accessed 22 August 2013.

<sup>15</sup> <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf>, accessed 22 August 2013.

**Denial of Service:** After the Spamhaus<sup>16</sup> attack, DNS reflection attacks have gained in popularity<sup>17,18</sup>. Attackers seem to have adopted the DNS reflection technique to launch amplification attacks, an old technique that has made a come-back. Moreover, attack bandwidths achieved have reached impressive levels: the rate of 2-10Gbps attacks has doubled<sup>19</sup> and the level of 300Gbps attack was reached in 2013<sup>20</sup>.

**Rogueware/Scareware:** In 2013 there was an increase in rogueware/scareware reported. Despite recent law enforcement advances<sup>21</sup>, the reports analysed provide strong evidence that there is an increase in ransomware threat. One reason for the growth is the expansion of ransomware and fake Antivirus distribution to mobile platforms, such as Android<sup>22,23</sup>. In all cases, the availability of anonymous payment services to channel illegal profits obtained from this threat is a key enabler for this kind of fraud<sup>24</sup>.

**Targeted Attacks:** In first half of 2013, targeted attacks demonstrated their effectiveness in achieving their objectives. In particular, cyber espionage attacks reached a dimension that went far beyond expectations<sup>25</sup>. Again, the proliferation of mobile devices delivers a wide exploitation surface for this kind of threats<sup>26</sup>. It is worth mentioning that mobile spyware applications might become strong tools for APTs targeting Bring Your Own Device environments<sup>27</sup>.

**Identity Theft:** This threat led to some of the most successful attacks by abusing SMS-forwarders to achieve significant financial fraud<sup>28</sup>. These attacks were based on known financial trojans (e.g. Zeus, SpyEye, Citadel<sup>29</sup>) that have been implemented on mobile platforms and attack 2-factor authentication<sup>30</sup>. A significant source for applying this threat remains social media<sup>31</sup>. It is worth mentioning that an increase in malicious browser extensions has been registered, aimed at taking over social network accounts<sup>32</sup>.

**Search Engine Poisoning:** In the first half of this year not many references to this threat have been found. One reference about better defence levels against this threat stated that the relevant defences of Google<sup>33</sup> seemed to reduce this threat. As with many other threats, Search Engine Poisoning has also gone mobile: some reports on malicious mobile apps performing Search Engine

<sup>16</sup> [http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability/at\\_download/fullReport](http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability/at_download/fullReport), accessed 22 August 2013.

<sup>17</sup> <http://www.akamai.com/stateoftheinternet/>, accessed 22 August 2013.

<sup>18</sup> <https://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q2/pr.html>, accessed 22 August 2013.

<sup>19</sup> <http://www.arboretworks.com/corporate/blog/4922-q2-key-findings-from-atlas>, accessed 22 August 2013.

<sup>20</sup> <http://www.arboretworks.com/corporate/blog/4813-putting-the-spamhouse-ddos-attack-in-perspective>, accessed 22 August 2013.

<sup>21</sup> <https://www.europol.europa.eu/content/police-dismantle-prolific-ransomware-cybercriminal-network>, accessed 22 August 2013.

<sup>22</sup> <http://www.symantec.com/connect/blogs/fakeav-holds-android-phones-ransom>, accessed 22 August 2013.

<sup>23</sup> <https://www.infoworld.com/t/mobile-security/ransomware-android-it-was-only-matter-of-time-221285>, accessed 22 August 2013.

<sup>24</sup> <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf>, accessed 22 August 2013.

<sup>25</sup> [https://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons/at\\_download/fullReport](https://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons/at_download/fullReport), accessed 22 August 2013.

<sup>26</sup> <https://www.securelist.com/en/blog/208194186/>, accessed 22 August 2013.

<sup>27</sup> <http://www.kindsight.net/sites/default/files/Kindsight-Q2-2013-Malware-Report.pdf>, accessed 22 August 2013.

<sup>28</sup> [http://www.cs.stevens.edu/~spock/Eurograbber\\_White\\_Paper.pdf](http://www.cs.stevens.edu/~spock/Eurograbber_White_Paper.pdf), accessed 22 August 2013.

<sup>29</sup> <http://www.mcafee.com/us/resources/white-papers/wp-citadel-trojan.pdf>, accessed 22 August 2013.

<sup>30</sup> <http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf>, accessed 22 August 2013.

<sup>31</sup> <http://bits.blogs.nytimes.com/2013/06/03/malware-that-drains-your-bank-account-thriving-on-facebook/>, accessed 22 August 2013.

<sup>32</sup> [https://www.symantec.com/content/en/us/enterprise/other\\_resources/b-intelligence\\_report\\_05-2013.en-us.pdf](https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_05-2013.en-us.pdf), accessed 22 August 2013.

<sup>33</sup> <https://www.bluecoat.com/security-blog/2013-04-05/search-engine-poisoning-brief-update>, accessed 22 August 2013.

Optimization poisoning have been found<sup>34, 35</sup>. As ENISA sees this threat as an important part of malicious code attack vectors, we will continue observing developments in this area.

### Concluding remarks

When we look at 2013 and beyond, the following developments regarding the threat landscape can be observed:

- Cyber-criminals increasingly use advanced methods to implement attack vectors that are non-traceable and difficult to take down. An important role in this play: anonymization technologies and the use of distributed technologies for more “resilient” infrastructures, such as P2P.
- It is clear that mobile technology is, and will increasingly become, exploited by cyber-criminals. Threats of all kinds that were encountered in the more traditional arena of IT will prevail on mobile devices and the services available on these platforms. The proliferation of mobile devices will lead to an amplification of abuse based on knowledge/attack vectors targeting to social media.
- The consumerization of malware, cyber-hacking tools and services, together with the availability of digital currencies and anonymous payment services, will open up new avenues for cyber-fraud and criminal activity.
- There is a real possibility of large impact events when attacks combining the above threats are successfully launched. A characteristic impact from such attacks is described in the risk of digital wildfires that was assessed in the beginning of 2013<sup>36</sup>.
- As reported by ENISA<sup>37</sup>, cyber-attacks are the 6<sup>th</sup> most important cause of outages in telecommunication infrastructures, with an impact on considerable numbers of users in this sector. Taking into account incidents<sup>16</sup> of the first half of this year, and also developments in the denial of service threat, we see an increase of infrastructure threats in 2013. When additional sectors and assets are being considered, the impact of cyber-attacks will be better analysed and understood.

<sup>34</sup> [https://www.symantec.com/content/en/us/enterprise/other\\_resources/b-istr\\_appendices\\_v18\\_2012\\_221284438.en-us.pdf](https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v18_2012_221284438.en-us.pdf), accessed 22 August 2013.

<sup>35</sup> <http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf>, accessed 22 August 2013.

<sup>36</sup> <http://forumblog.org/2013/04/digital-wildfires-fast-flaring-easily-doused/>, accessed 22 August 2013.

<sup>37</sup> [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012/at\\_download/fullReport](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012/at_download/fullReport), accessed 22 August 2013.