CIRCL
Computer Incident
Response Center
Luxembourg

TREND REPORT 2011

A PERSPECTIVE ON COMPUTER SECURITY INCIDENTS IN LUXEMBOURG

The period covered by the report is between October 1, 2010 and December 31, 2011

CIRCL
Computer Incident Response Center Luxembourg

41, avenue de la Gare · L-1611 Luxembourg
Grand-Duchy of Luxembourg

ABSTRACT

This trend report covers the activities performed by CIRCL (Computer Incident Response Center Luxembourg), the national CERT of the Grand Duchy of Luxembourg. In addition to the factual information regarding CIRCL activities, security trends and lessons learned from incident handling have been summarized to highlight ways to improve security at the national and international level.

CONTENTS

SCOPE

This annual report covers the activities of the national CERT (CIRCL: Computer Incident Response Center Luxembourg) operated by SMILE GIE [1]. CIRCL operates under the auspices of, and with authority delegated by, the Grand Duchy of Luxembourg (Ministry of the Economy and Foreign Trade) [2].

The statistics mentioned in this report were collected using CIRCL-internal tools. The information and statistics collected from the incidents were anonymized for this report. When the anonymization was not feasible, information was not included in this annual report.

CIRCL

CIRCL [3] is the national security incident handling team for the Grand Duchy of Luxembourg covering the national infrastructure of Luxembourg established in May 2008. The constituency of CIRCL covers the .lu TLD, Internet Public ASN and IP addresses located/originated and/or operating in/from the Grand Duchy of Luxembourg. As handling security incidents is a cooperative process, CIRCL coordinates incident handling between international and local CSIRT/CERT partners.

CIRCL cooperates at a national and international level on the operational aspects of network and system security including research and development projects. CIRCL provides a large scope of incident-handling services and a majority of them are freely accessible to companies and other organizations within Luxembourg.

[1] Security made in Lëtzebuerg - Groupement d'Intérêt Economique (SMILE GIE) is a joint venture between several public entities of the Grand Duchy of Luxembourg. Its mission is to create, finance, manage and promote services and initiatives related to information security. SMILE powers CASES, the information security portal of the Ministry of the Economy and Foreign Trade, as well as CIRCL, the national CERT for Luxembourg (Computer Emergency Response Team).

[2] http://www.circl.lu/files/letter-circl.pdf

[3] Computer Incident Response Center Luxembourg

TIMELINE

May 2008	CIRCL (Computer Incident Response Center Luxembourg) is founded
October 2008	CIRCL is listed on trusted introducer (the trusted backbone of the Security and Incident Response Team community in Europe).
September 2010	CIRCL is officially hosted by SMILE GIE
October 2010	CIRCL is staffed with a team of five operators with an addition of two existing operators from the Ministry of Economy and Foreign Trade
October 2010	Dedicated incident-handling infrastructure activated
December 2010	285 events were processed in 3 months
February 2011	CIRCL receives the official mandate to operate as the national CERT of the Grand Duchy of Luxembourg
April 2011	CIRCL infrastructure extended to IPv6 and CIRCL becomes a RIPE member
June 2011	CIRCL becomes an accredited CERT from trusted introducer
September 2011	CIRCL initiates the CERT.LU initiative in collaboration with the 2 other CERTs in Luxembourg
December 2011	4 737 events are processed and more than 361 technical investigations are conducted in 15 months

PART I

INCIDENTS OVERVIEW AND SECURITY THREAT TRENDS

EXECUTIVE SUMMARY

The attack surface in Luxembourg (at the same rate as other countries around the world [4]) steadily increased over the past years, especially due to the continuous integration of network-connected devices. These opportunities have been used in 2011 by different kinds of attackers.

Three main groups have been identified: mainly cybercriminals, government-supported attackers and cyberactivists.

In this report, we use the following definitions:

Cybercriminals refers to criminals abusing a computer and/or a network to get a direct financial benefit from their actions.

Government-supported attackers refers to attacks abusing a computer and/or a network to get information for the benefit of the sponsoring government.

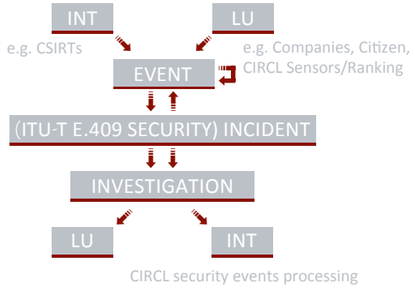
Cyberactivists refers to attackers abusing a computer and/or a network to directly support their social or political objectives.

The incidents reported and analyzed this year show an expansion in their numbers, complexity and level of impact. A large proportion of incidents could have been avoided, or at least limited, by adequate protection measures and/or by a proper level of regular maintenance.

[4] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_ en_xg.pdf

OVERALL INCIDENT STATISTICS

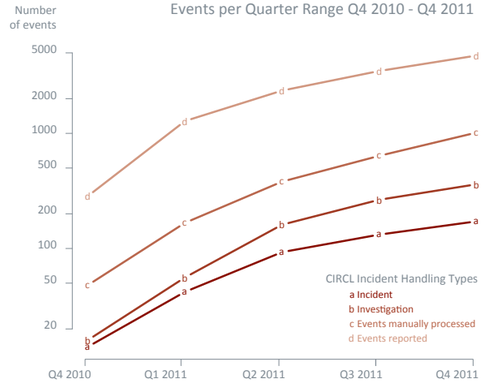
The CIRCL work-flow is described in the adjoining figure. CIRCL receives event notifications from monitoring infrastructure (e.g. Honeypots), international CSIRT partners, organizations or companies based in Luxembourg. If the event notification received, could or has been threatening an infrastructure in Luxembourg, a CIRCL operator classifies it as a security incident (as defined by the ITU). Those incidents are then handled by CIRCL for technical investigation. Some incidents can generate much more technical investigations to analyze the incident and coordinate with the victims.



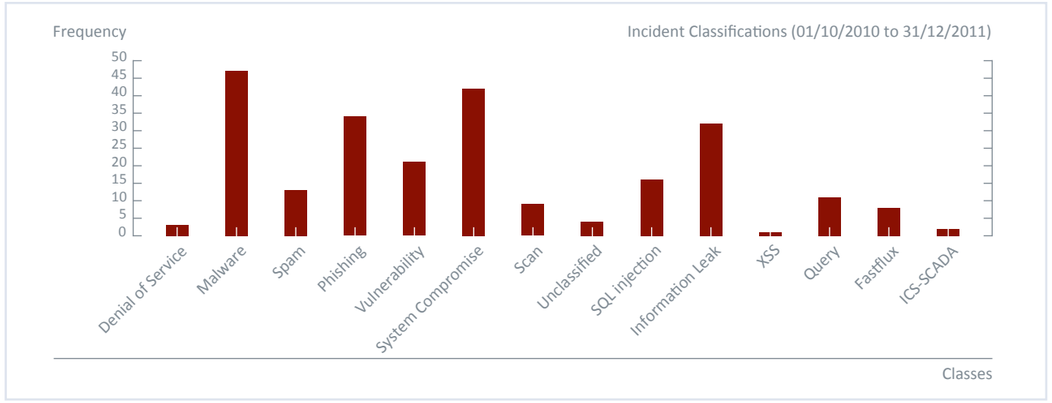
Statistics are compiled from the ticketing system operated by CIRCL to manage security events received over a one-year period (from last quarter 2010 until the last quarter 2011). An event can be an automatic security event reported by an internal CIRCL tool (e.g. high activity against a honeypot for an ASN located in Luxembourg), an event reported by third party CSIRTs at an international level, or reported by organizations operating or established in Luxembourg.

Reported events (labeled d on the graph) are then classified and manually processed for analysis (labeled c on the graph). An event becomes an incident (security incident in the ITU E.409 definition and labeled a on the graph) when an aspect of information security could be or has been threatened in Luxembourg. For those incidents, CIRCL carries out a technical analysis and coordination to limit their impact in the very short term, called an investigation (labeled b on the graph).

As you can clearly see, the number of reported events slightly increased during the year. This can be explained by multiple factors, but two major ones are:



- the exchange of information among CSIRT teams and automatic reporting systems improved in the past months;
- an increase of attacks (and especially their discovery and reporting) is another key factor for the increase of reported security events.



Going into a more detailed view, we classified the incidents into respective categories. Those categories are “Denial of Service”, “Malware”, “Spam”, “Phishing”, “Vulnerability”, “System Compromise”, “Scan”, “Unclassified”, “SQL injection”, “Information Leak”, “Cross-Site Scripting (XSS)”, “Query”, “Fastflux”, “ICS-SCADA”. Even if such classification is subjective, malware is still one of the highest scorers when dealing with incidents. Malware plays a key role in the malicious activities of the attacker. Attackers know that their Malware is analyzed and reversed by CSIRTs and A/V vendors. So attackers invest a lot of resources into the obfuscation and complexity of these malware.

It’s a major issue to keep ahead in the analysis of such components. As described below, Web threats are still very active due to their scale and how easy they are to exploit. The classification does not report the time invested in analyses, and a malware analysis can take much more time than a phishing case handling. According to a survey [5], ICS-SCADA incidents are increasing and we did indeed observe in our constituency and elsewhere, some incidents. According to the Microsoft Security Intelligence Report volume eleven [6], the infection trends score for Luxembourg decreased from 8 (1Q2010) to 3.8 (2Q2011) regarding the infected personal computers.

[5] http://cryptocomb.org/2011-Leverett-industrial.pdf

[6] http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_Regional_Threat_Assessments_English.pdf

THREATS

In the technical analysis of the incidents processed by CIRCL, we have seen many different threats towards or originating from Luxembourg with a clear tendency towards the following threats:

WEB THREATS

The abuse of unsecured web infrastructure to host malicious content (from phishing to desktop infection) is still a very active threat especially in that the number of vulnerable services has progressed due to the wide accessibility of software packages (e.g. CMS, Blogging systems or CRM software). These services are usually abused to host two types of malicious content:

- direct phishing content (or HTTP redirect to phishing content);
- click fraud or exploit kits targeting end-user browsers.

For the purpose of exploiting vulnerable end-users’ PCs via “exploit kits”, attackers tend to favor unsecured websites with a large audience, or target website services (e.g. advertising servers) which display content on other websites. This tendency shows the importance of improving the security of hosted services along with the clients accessing them. Such threats are regularly used by cybercriminals to infect new target computers while keeping the origin of the attacks difficult to detect (e.g. cybercriminals use more and more complex VPN infrastructure to hide their traces). The main issue with such unsecured web infrastructures is that they are providing continuous ground for infecting new systems. In Luxembourg, this threat is quite present (as web-based services are largely used) and could be addressed by some preventive and reactive actions.

Another issue with the large attack surface of web applications is that cyberactivists often use these as a protesting platform while putting in danger the information and services hosted on such platforms.

MALICIOUS DOCUMENTS AND SOCIAL ENGINEERING

In the incidents analyzed during 2011, targeted attacks increased as well. Those targeted attacks regularly used malicious documents while abusing the confidence of the user when they read, access or run those documents. The success rate of such attacks is quite high due to the regular use of zero-day attacks against well-known software (e.g. from true-type font parsing to RTF parsers) along with their capacity to abuse user confidence. Those techniques are regularly used by cybercriminals (in some cases the cybercriminals seem to be State-sponsored) to perform more complex attacks.

What about “Advanced Persistent Threats”?

Organizations are nowadays facing two threats, that are basically the same: RAT and APT. RAT is an acronym for ‘Remote Administration Tool’, which allows somebody to take control of a machine remotely with or without the consent of the user.

Such a tool might be legitimately installed and used by the

IT Helpdesk of a company, but it is also widely deployed by a lot of different malware variants to control computer systems to perform actions without the consent of the user. They are also used to observe the activity of a user or to access his private electronic data. The infection by a RAT can be in the scope of a targeted attack, but it is more usual to discover it along with "standard" malware. APT, which stands for 'Advanced Persistent Threat', is similar to RAT, but the difference lies in the sophistication of the malware code and the way it is used to target companies. Due to increased complexity and sophistication, the invested manpower in such malware is much higher.

It is used specifically in targeted campaigns to lower the danger of detection where it could be found.

As for our definition, RAT is widely used and "bundled" with lots of malware variants. The sophistication of an APT is much beyond that of a RAT, and due to more sophisticated infection and exfiltration methods, it is less often detected and can persist for a much longer time.

Nowadays, the terminology "Advanced Persistent Threat" is often misused to mention a common infection using malware with some level of remote administration capabilities.

MISCONFIGURED ICS SYSTEMS

In 2011, CIRCL had to analyze and coordinate a few incidents regarding Industrial Control Systems (e.g. HVAC control system, facility control system, etc).

In the majority of incidents, the ICS systems were directly connected to the Internet without any protection measures. Considering the low level of security for the ICS systems, it seems quite probable that the skills required to compromise such systems are quite low. As those systems are often not monitored, incident analysis tends to be difficult as no trace is left behind. The threats against such equipment increases due to two main factors:

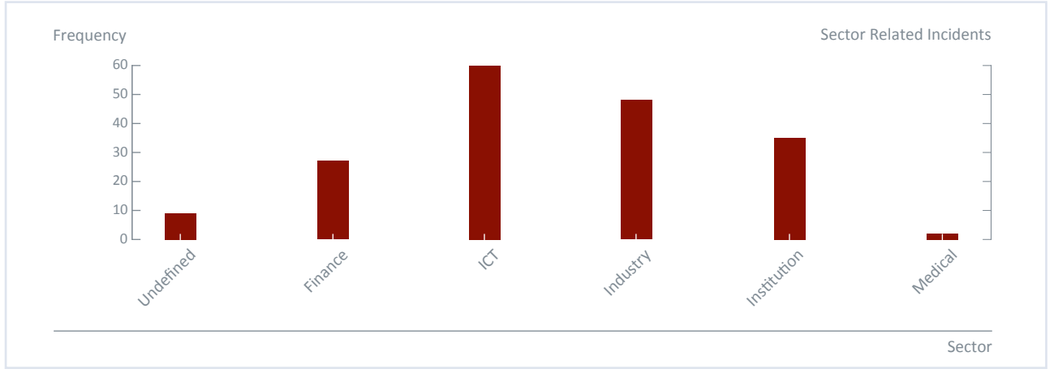
- convergence to the IP protocol (also bringing some benefits)
- operation of ICS systems that are often performed by teams outside the traditional IT security landscape who don't always know the basic security requirements for such a system.

In the future, security of industrial control systems must not be underestimated as they will become key components of our infrastructure while relying on their existing legacy infrastructure.

What is an ICS (industrial control system) or a SCADA (supervisory control and data acquisition) system?

Industrial control systems (ICS) refer to specific computer equipment used for the control of industrial– or facility–equipments. The term SCADA is regularly used as a synonym, highlighting both aspects: supervision and control. A majority of ICS equipments have these two functionalities and thus providing an increased level of opportunity to attackers.

PART II
IMPACTED ECONOMICAL SECTORS



As previously defined, CIRCL is the national CERT of Luxembourg. Hence, it is the national and international response center for incidents. CIRCL covers the rich variety of economical sectors in Luxembourg. In this report a coarse grained classification is selected in order to guarantee the anonymity of the victims in a given particular economical sector. Thus the following economic sectors have been selected, including the victims helped by CIRCL to solve their incidents: "unclassified [7]", "financial", "industry", "institution" and "medical". The incidents have been either reported by the victims themselves or by a third party. A third party could be either an aggrieved party or collaborating international CERT. Frequently, the owners of a given infrastructure are not aware of an incident. This is often the case where industrial or governmental espionage is executed. In this case, attackers use stealthy methods to subvert the targeted infrastructure aiming to maximize information ex-filtration.

The figure above shows the distribution of economical sectors in which CIRCL was active in helping the victims to assess and recover from their incidents. The explanations below show just the major trends and do not exhaustively enumerate all the different kinds of incidents.

Most incidents were observed in the ICT sector. This is mainly due to the reporting of international collaborating partners notifying CIRCL about incidents at ICT infrastructures related to Luxembourg. Another factor is that the ICT sector includes the Internet Service and Hosting Provider were the majority of Internet services are hosted. A total of 48 incidents have been reported to CIRCL related to the industry sector. These incidents were frequently related to ICT infrastructure dedicated to specialized industries and often aimed at industrial espionage. Luxembourg hosts many international institutions and 35 incidents have been reported in this sector.

[7] For the victims not falling into the other categories.

Leaked information regarding this sector reported by third parties dominated these incidents. As an example, the leaked information is found in drop zones from attackers or in reversed malware samples.

In the finance sector, phishing-related incidents have often been encountered along with malware, targeting financial applications. Even though CIRCL does not have the PSF (Profession du Secteur Financier) status, 27 incidents have been reported to CIRCL in this sector. There might be some discrepancies between the figures of CSSF and CIRCL. An important proportion of those phishing were targeting financial organization outside Luxembourg even if the phishing website is based in Luxembourg. Another point to take into consideration is the scope reduction defined by CSSF. However, this reduction [8] might introduce some risks because no distinction between phishing attacks against the financial player sectors' and its customers is made. In order to illustrate this subtle difference, the following example is presented.

An attacker sets up a fake online banking site aiming to get the user credentials from the customer of a financial sectors company. In this case, the infrastructure operating the phishing server is out of the control of the targeted financial company.

However, if spear-phishing is used, dedicated users of a financial organization receive a document with a malicious payload targeting a range of word processors. The action of opening these documents triggers the deployment of espionage tools targeting financial internal information that is leaked to the attackers. In this case, the incident happens on the local infrastructure under the control of the victim.

The unclassified incidents target economical sectors where the victims can be easily identified and they are not discussed in this report. In the medical sector two incidents have been observed centered on information leak of personal data.

[8] http://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf11_504eng.pdf

PART III

LESSONS LEARNED

Most of the incidents CIRCL was involved in were incidents touching information technology infrastructures where these infrastructures were partially compromised by attackers. They either hijacked services or infected systems and controlled parts of the infrastructure besides the legitimate operators. The observed attackers were very dynamic and often do not follow traditional managerial approaches such as a project-oriented approach. In addition, they tend to ignore procedures and do not bother about established policies and regulations. Furthermore, attackers are often aware of the behavior of their adversaries. Their high flexibility and the fact of having well prepared the subverting of the underlying infrastructure gives the attackers a temporal advantage and puts the legitimate operators in a defensive position.

In order to confront these kinds of attackers, a state-of-the-art crisis management approach is not suited in order to efficiently reconquer the compromised infrastructure. Crisis management [9] approaches often assume that the adversarial strike is over and that the goal is to recover from the created damage. Due to the strategic interests of intruders in compromised information technology infrastructures this hypothesis does not hold. First, attackers are often constantly active on the infrastructure, frequently increasing the damage during the time dedicated for crisis management. Second, attackers often notice the actions of their adversaries due to a frequently observed tedious preparation phase. Attackers are often not satisfied with the observation but they use their strategic advantage to react appropriately. A hierarchical top-down crisis management approach gives an additional advantage to attackers. They operate at infrastructure level and hardly on organizational level. Hence, it is essential to have, from the beginning of the observation of the incident, people in the response team capable of taking immediate actions on the infrastructure. Such as taking recovered traces left by the attackers or the left-overs from a take-down of parts of the infected infrastructure. The more time is needed for doing these actions, the more time attackers have to hide their tracks.

A traditional procedural crisis management approach also gives an advantage to attackers due to their cumbersome and exhaustive nature. Attackers that have prepared their strike well, have often carefully designed complex tools enabling their hijacking of the targeted infrastructure and the analysis of these tools consume de-facto a lot of time. The current paradigm of evidence collection, evidence analysis, reaction is a good approach but often inadequately implemented for efficiently handling incidents. First, during an incident the evidence is not visible at first glance.

A common use case is the discovery of an unknown malicious program. While following the evidence collection, evidence analysis and reaction paradigm, the unknown malicious program is collected, then analyzed and a detailed report is written. The report is analyzed and a reaction is taken. During analysis of the malicious program, the analyst often notices that

[9] Different definitions of crisis management exist. In this document, crisis management means a top-down approach compared to incident-handling where it's more bottom-up.

additional evidence needs to be collected. Therefore, an incremental approach is a better solution, where direct communication, including decision taking, between the analyst and the members of the response team capable of taking immediate actions on the infrastructure is possible. The direct feedback of the analyst enables the response team to collect additional evidence in order to complete the overall picture of the attack.

Second, attackers often prefer to leave volatile traces. A real world example is attacking tools residing only in memory. The analysis results must be communicated quickly to assure related, volatile, evidences can be collected in time. The optimal approach would be to pro actively collect a maximum of potential evidence at the beginning of the incident even though not all data results in evidence. From an effective incident-handling approach, the collection of additional data is an advantage which is often conflicting with existing privacy regulations.

Therefore, during an incident it is essential that the runtime of the evidence collection, evidence analysis and reaction is very small in order to be effective.

The worst case of an incident situation is if the operational response team having access to their infrastructure has no strategy when dealing with this case. This often results in wrong decisions such as switching off compromised systems without having first saved volatile evidence. A lesser worst-case scenario is if there are procedures in case of an incident. However, procedures could be a two-edged sword. It could be out of date and too complicated so that it is not taken into account by operational people. The best situation is if operational people have a very basic procedure which is easy to remember and was already experienced in real life, at least as a test.

A generalized lesson learned for a particular incident is to avoid such incidents in the future. The common approach of only buying security services, such as penetration tests or security audits, is just a partial solution to security problems. CIRCL has observed incidents where their impacts could have been limited by appropriate and regular log analysis. Predecessors have retroactively observed system logs. If more time and resources had been allocated to operational people, they could have noticed it and might have taken defensive actions in advance.

[10] "Expectations for Computer Security Incident Response"
[11] http://www.circl.lu/services/
[12] http://pgp.circl.lu/

PART IV

SERVICES AND COLLABORATION

SERVICES PROVIDED BY CIRCL

CIRCL, as the national CERT in the Grand Duchy of Luxembourg, is providing multiple services to its constituency as well as to the community at large. The mission of CIRCL is described in its RFC 2350 [10] formatted document. Beside the traditional incident response services, we provide specialized services to improve security or support incident handling in Luxembourg and abroad.

Incident coordination

Incident coordination is a service freely accessible to all companies or organizations based in the Grand Duchy of Luxembourg. It includes:

- online reporting;
- incident identification, analysis and response;
- technical investigation (e.g. security vulnerability/ incident matching, malware analysis, network or system forensic, etc);
- vulnerability handling and responsible vulnerability disclosure on incident reporter's request;
- national/international CSIRT cooperation.

Incident handling for CIRCL members

In addition to the standard CERT services, we provide additional services to our members [11].

This service extends the standard incident coordination services along with:

- access to the CIRCL SNP platform providing insights about the Internet assets of the member and the related security events reported;
- one day on-site intervention in Luxembourg for incident handling.

ONLINE TOOLS PROVIDED & OPERATED BY CIRCL

CIRCL operates and develops tools that are accessible publicly to improve security or incident handling.

OpenPGP Public Key Server

CIRCL operates an OpenPGP key server [12] located in Luxembourg to support the use of PGP. PGP is commonly used among the CSIRT community to securely communicate among partners. The PGP keyserver is part of the international SKS network and the SKS server pool. It contains more than 3 millions PGP keys with an average of 400 new keys per day.

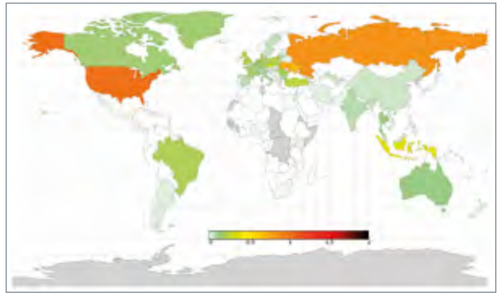
Passive DNS

Passive DNS [13] is a technique to collect only valid answers from caching/recursive nameservers and authoritative nameservers. The technique permits the reconstruction of a view of the public data available in the worldwide DNS. In security, the system is used to detect malicious or hijacked domains. CIRCL developed and operates a passive DNS to trace the evolution of the domains.

A well-known domain [14] that has hijacked for a short period of time in September 2011.

BGP Ranking

A key element in Internet is the BGP protocol, each Internet Service Provider (ISP) has a unique identifier called an Autonomous System Number. CIRCL supports and maintains a system called BGP Ranking [15] to analyze the proportion of malicious activities per Internet Service Provider (ISP). BGP Ranking uses publicly available data to rank each of the ISPs and provides a score from the most to the least malicious activities per ISP. This information permits the improvement of the classification when analyzing large sets of IP addresses (e.g. from an incident) or rank-specific domain names.



An overview of the malicious activities per country from BGP Ranking.

[13] http://pdns.circl.lu/
[14] http://itigloo.com/2011/09/04/the-register-hacked/
[15] http://bgpranking.circl.lu/

SOFTWARE DEVELOPED & PUBLISHED BY CIRCL

During and after each incident, we create tools to ease or improve the incident-handling process. As CIRCL resources are limited (five employees dedicated to the handling of security incidents), CIRCL improved the process of incident-handling by automating some parts of incident handling or improving its early-warning systems. Some of the tools developed by CIRCL are publicly available [16] to citizens and especially to the overall security community, such as the followings tools:

- nfdump-tools - a tool for analysis of large datasets of network flows;
- pe32-cert-dump - a tool to dump and extract certificate from PE binary files;
- vt-tools - to automate queries against VirusTotal public and private interfaces;
- bgp-ranking and bgp-ranking-API - to calculate the trust in an ISP and provide a unified interface to query their ranking value;
- traceroute-circl - a tool to improve lookup of internet ressources for security contact and location.

Some other tools related to critical security handling, like malware analysis or detection, are not publicly available to keep ahead of the attackers. These are internally shared among preferred partners, CSIRTS or trusted groups when this can be a benefit to the global security community.

CONFERENCES, PRESENTATIONS & COLLABORATION

CIRCL attends conferences to share information about its current activities or research projects with the objective to create new collaborations. The list below includes the conferences where we contributed with presentations or/and papers.

- 4GHCon [17] - 2-4 December 2011 - CIRCL gave a presentation about “Large-scale Netflow Indexing”
- OWASP Benelux 2011 - 1-2 December - CIRCL gave a presentation about “Dynamic malware analysis”
- CERT Verbund Arbeitstreffen - 29-30 October - CIRCL presented “SSL/TLS vulnerability status in Luxembourg”
- 34th TF-CSIRT Meeting [18] in Luxembourg - 22-23 September 2011 - CIRCL talked about “Ranking Internet resources to find suspicious activities”
- hack.lu - 19-22 September 2011 CIRCL - co-organized the event
- 5th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2011) 13-17 June, 2011, Nancy France[19] - CIRCL gave a training “Using Distributed Computing Techniques and Tools to Help Network Forensics”
- Belnet Security Conference - 5 May 2011 in Brussels[20] - CIRCL spoke about “Design and Implementation of a Fast and Scalable Ranking Scheme for Internet Resources”

[16] https://github.com/CIRCL
[17] http://www.4gh-con.org/program.html
[18] http://www.terena.org/activities/tf-csirt/meeting34/
[19] http://www.aims-conference.org/2011/
[20] https://www.belnet.be/en/news/programme-bsc

- CIRCL gave courses at Lycée Technique des Arts et Métiers (LTAM) on “Network Forensics”, “Customized Embedded Devices for Security Services” and “Logging & Security”.
- 2011 FIRST Symposium, Barcelona 1-3 February 2011 CIRCL spoke about “Fast and Scalable Ranking Scheme for Internet Resources” [21]
- CIRCL co-organized hack.lu 2010 - an international security conference

CIRCL is actively collaborating with other CSIRTs at national and international levels on different research projects (e.g. Malware analysis, network forensic project, etc) beside incident handling. As Luxembourg is a major player in the economic world, incident handling is not limited to its borders. There is a strong relationship with the Benelux CSIRTs and the pan-European CSIRTs.

PART V
CONCLUSION

The diversity of attacks shows the complexity and the attack surface in day-to-day life. During our investigations, interesting facts were revealed as described in the lessons learned part. One of the more interesting facts is the gap between the procedures (e.g. security policies) and their application. Operational security is the key element for adequate application of the procedures but most important are the detection and handling of the incidents in a fast and efficient way. Log management and analysis deserves more attention especially because initial infections are usually detected by regular manual log analysis. As the detection of such anomalies cannot be easily automated, we recommend the investment of more resources and training into information security human resources.

Attackers show a high level of flexibility. Incident management should keep this in mind. When handling information security incidents, attackers usually benefit from latency when dealing with non-operational incident management. An adequate incident management should also include direct operational security that leads to limiting the attacker’s actions. In other words, to be better prepared for an incident, you should include your staff which is directly involved in security operations and ensure really sound procedures and practices. These steps can be introduced by testing the overall incident management from the collection of evidence up to their analysis/remediation with real concrete data.

[21] http://www.terena.org/activities/tf-csirt/meeting34/dulaunoy-ranking.pdf

CIRCL

Computer Incident
Response Center
Luxembourg

41, avenue de la Gare · L-1611 Luxembourg
Tel.: (+352) 247 88 444 · e-mail : info@circl.lu

www.circl.lu