SECURITY ON THE INTERNET
REPORT ON INFORMATION AND INTERNET SECURITY

Group Information Security I February 2013

LIFE IS FOR SHARING.

SECURITY ON THE INTERNET
MANAGEMENT SUMMARY

For the fourth time now, Deutsche Telekom is publishing its "Security on the Internet" report, with which it provides information about potential threats on the Internet every six months. The last few months have been primarily dominated by discussion of malware codes such as Duqu, Flame and Gauss, which have demonstrated a very high level of technical sophistication in many cases. The MD5 collision attacks in the Flame malware are one such example.

Another prominent malware, Red October, was revealed at the beginning of 2013, and experts have stated that it was first created in 2007. How can highly complex malware with more than 10 different components manage to infect government computers across the world and remain undetected for almost six years?

Red October provides a striking demonstration of the importance of effective patch management – especially on normal office PCs. All previously identified entry points (exploited vulnerabilities) for Red October malware have been made known and security updates made available.

Of course, update procedures are complex and must be processed correctly. As a rule of thumb, every IT system ought to have its software brought up-to-date within a few hours. That's the only way to close entry points such as vulnerable versions of Java or Adobe Flash Player effectively.

On top of this, according to Kaspersky the IT security industry faces the challenge of analyzing and recognizing more than 200,000 new malware codes every day. Trends in the last few weeks show that malware codes are increasingly beginning to bypass automatic analysis systems such as virus scanners (see "Security Updates").

A further trend can be observed in the exploitation of vulnerabilities within the programming language Java. This is a worthwhile target for attackers due to Java's widespread use. At least two flaws have been massively exploited in order to infect computer systems through so-called drive-by attacks in the last 12 months. The Red October malware also includes an attack code (exploit) for a Java interface. It is interesting to note that the most recently exploited Java vulnerability (CVE-2013-0422) had obviously been used on a few occasions weeks before its actual discovery in commercial attack toolkits.

This can be explained by the fact that certain developers of corresponding attack toolkits apparently sometimes go so far as to buy information about vulnerabilities in order to include them in their respective toolkits. This shows how the potential threat and the commercialization of attackers have further developed. With this report, we're making a contribution to the explanation and adaptation of today's security models.

I hope you enjoy reading this report.

Yours,

Thomas Tschersich

In-house expertise: This report is published twice a year, and is available in both German and English on DT's corporate website: www.telekom.com/security.

CONTENTS

SECURITY ON THE INTERNET
SECURITY UPDATES

"Red October" malware

Kaspersky first reported on the "Red October" campaign in mid-January 2013. It was an attempt to spy on targeted diplomats, governments and organizations close to governments that began in 2007. Unlike other prominent malware codes from the last few years (Gauss, Flame), Red October did not use any zero-day vulnerabilities, instead targeting vulnerabilities in Microsoft Word and Java that have only now become known.

The campaign stands out due to the fact that the malware code remained undetected for almost six years, as well as due to the high number of modules that exist and the fact that, with over 60 servers, the Command and Control (C&C) infrastructure displays a very high level of complexity. The method of contaminating selected smartphones indirectly through synchronization with an infected PC is equally sophisticated.

Ruby on Rails (RoR) vulnerabilities

RoR has become one of the most popular platforms for Web-developers. Several vulnerabilities that could be used to execute arbitrary commands with the privileges of the RoR application (3.0.x and 2.3.x) were identified in January 2013. The recently discovered vulnerabilities are based on hackers making requests from the Internet that are then incorrectly handled and lead to the vulnerability (code execution) in the YAML backend.

Furthermore, security experts took a close look at RoR's approved user administrator access system at the end of 2012. Depending on which authentication model is used, a secret key is set up, which RoR applications save in the secret_token.rb file. This key exists once for each application. Many developers had saved all of their open-source RoR application source codes in public repositories like Github. Several users of these RoR applications have never changed the key, which meant that just by knowing the content of the secret_token.rb file, the security model of the application was compromised.

MySQL

Various vulnerabilities in the MySQL database software that could, depending on the operating system, also have resulted in execution of code being sent over the network. The imminent threat of attacks from the Internet is usually considered low, because databases are typically built in protected zones (so-called militarized zones, MZ). Nevertheless, a security update should be made available as soon as possible in such cases.

APT / New York Times / Washington Post

In January 2013 several large American media companies announced that they had been spied upon by hackers, who were presumed to be Chinese, over a long period of time. In February, similar reports were made by companies such as ThyssenKrupp and EADS. In the case of the New York Times, 45 malware codes were found installed on computers. However, virus scanners found just one file. This ultimately demonstrates the fact that computer users should not rely on anti-virus software alone: It is important to establish further defensive measures (logfile analysis, SIEM, etc.). Malware codes are now often designed with one target or purpose of attack in mind, which means detection without heuristics or behavior-based approaches is often impossible.

SECURITY ON THE INTERNET
SECURITY UPDATES

Java vulnerabilities

After the frequent exploitation of Adobe Flash/PDF as vectors of attack in the last few years, hackers began to focus on Java in 2012. One vulnerability was exploited for the infection of over 600,000 Mac OS X computers at the beginning of 2012 ("Flashback" malware code). As a result of this incident, Apple was heavily criticized for its slow update policy for Java.

In the fourth quarter of 2012 and at the beginning of 2013, several vulnerabilities within Java that had been exploited through visits to infected websites ("drive-by" attacks) were identified. The vulnerabilities forced Oracle to create updates at short notice. Detailed analyses showed that the vulnerabilities had already been in use as part of various underground toolkits for several weeks.

Bug bounty programs

As a result of the Java vulnerabilities, a new phenomenon was identified. At least one author of a well-known underground toolkit had used a modification of the popular idea of bug bounty programs. The author bought up unpublished vulnerabilities until they were no longer available in order to make his toolkit offer exclusive.

Vulnerable smartphones

A vulnerability exists that makes it possible to execute arbitrary code with core permission on popular smartphones that are based on Exynos 4210 and 4412 CPUs, such as the Samsung Galaxy SIII. This grants users access to extended privileges on the phone. But malware codes are also able to execute system-wide procedures and misuse the smartphone for undesired purposes. The device's security concept is thereby compromised. Samsung has already released a fix for the vulnerability, but other producers that also use these CPUs are affected too. This being said, no Trojans with this functionality – aside from Proof of Concept codes – were available in early 2013.

SSL certificate authority gives out incorrect certificates

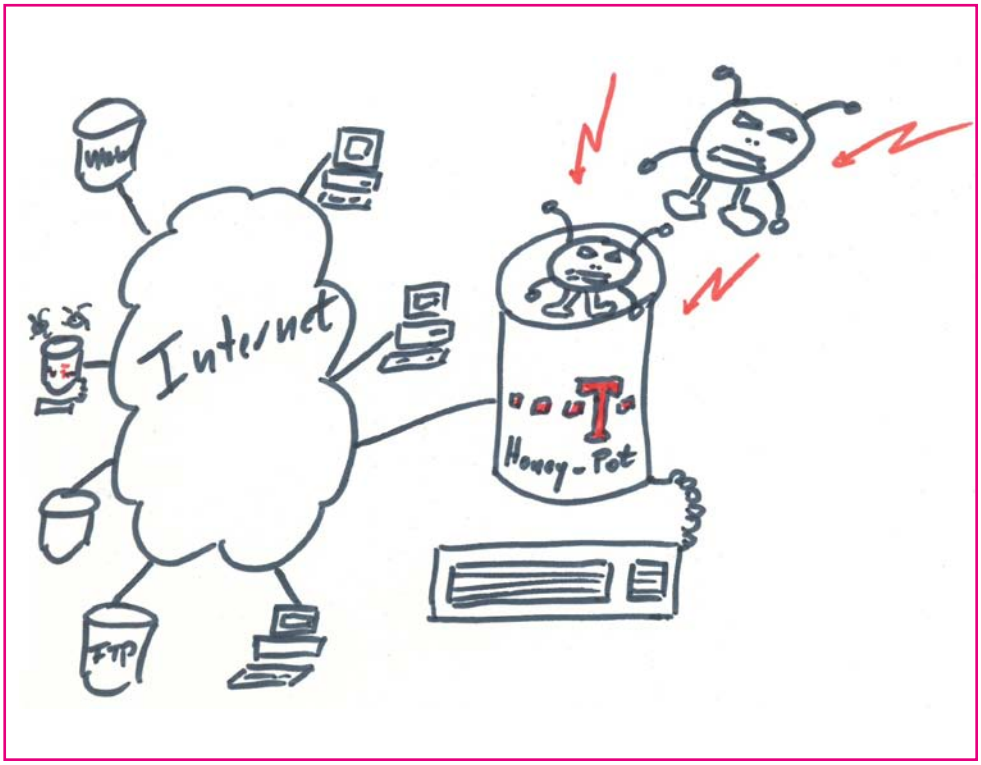
Due to a mistake, the Turkish SSL certificate provider Turktrust provided two subordinate certification authority (SubCA) certificates through which it was possible to issue valid certificates arbitrarily. Google discovered this at the end of 2012 when a certificate for *.google.com that had been provided through these SubCAs was identified. Google reacted promptly and withdrew all trust in the SubCA certificates. Even though in this case the certificate had not been created through a hacker attack, as was the case with Comodo and DigiNotar, the incident once again demonstrates the weaknesses in the trustworthiness of certificate-based SSL infrastructure.

SECURITY ON THE INTERNET

EARLY WARNING SYSTEMS: WHAT THEY ARE AND HOW THEY WORK

The early warning system at Deutsche Telekom offers a perspective on security on the Internet, independent of security providers. The information that is currently available on the Internet regarding this topic mainly comes from individual security providers and can sometimes differ considerably. In the area of monitoring the volume of unsolicited e-mail (SPAM) and the rankings of the respective countries of origin in particular, there are sometimes discrepancies with the data that Deutsche Telekom has generated from its own sources (primarily Abuse input channels).

The goal is to combine our own knowledge with that of these providers in order to offer Deutsche Telekom customers the best possible protection from online threats. It also helps us to know where there is a possible need for change in the current security systems or security standards at an early stage.



Therefore, the general rule is: The higher the number of sources of information involved, the more effective the early warning systems are and the more damage can be avoided to our systems, the connected partner systems and the customers' systems.

We have observed the strict legal regulations concerning data privacy, security, as well as confidentiality from as early on as the development phase of the so-called honeypot infrastructure, which aims to attract attacks. The graphic illustrates how different data sources and system components work together.

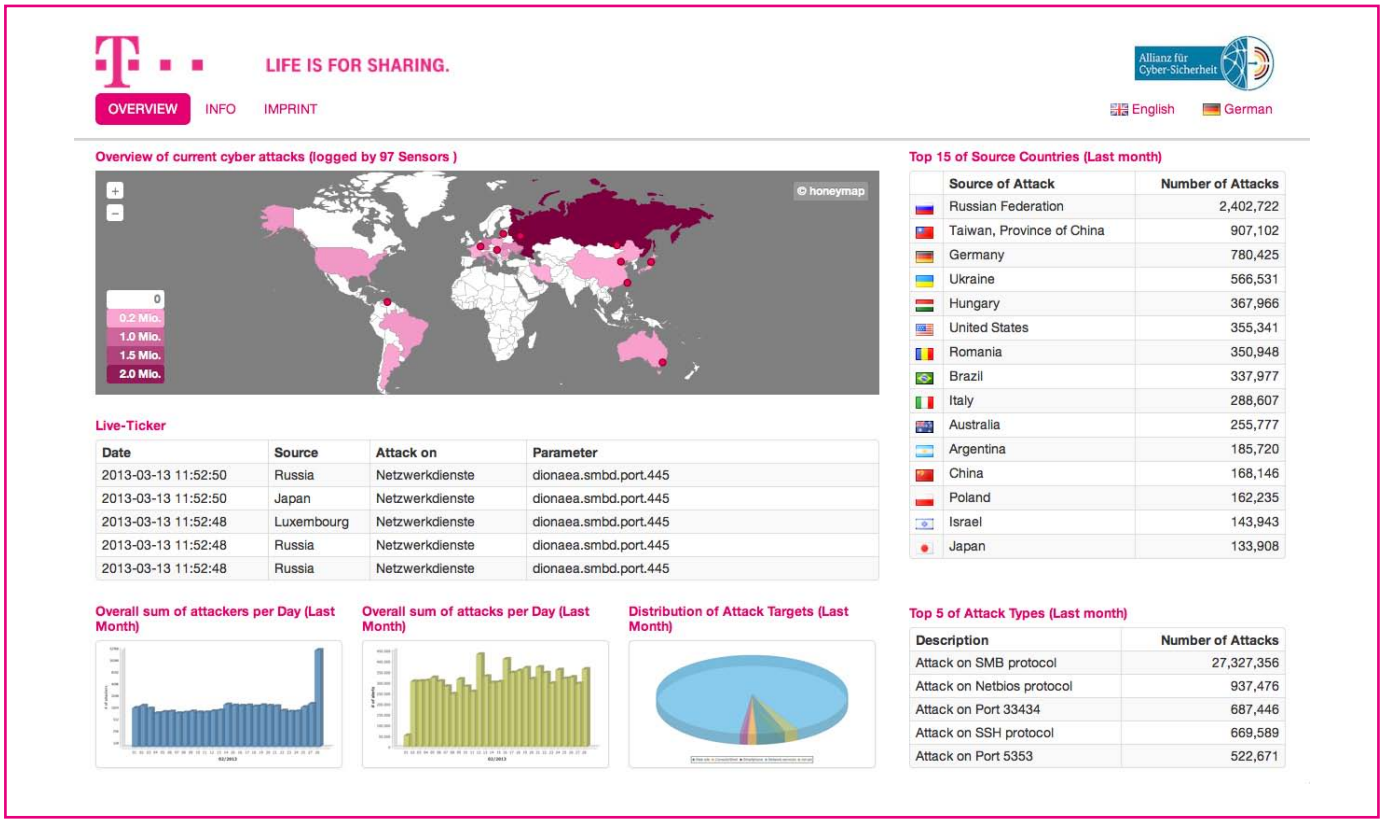
Deutsche Telekom uses a variety of data sources for its early warning system to get an overview of security on the Internet. The four most important elements are:

- Honeypot systems (for the simulation of Web applications, SSH and databases among other things)
- Web application firewall systems
- External indications (Abuse/suspected misuse of Deutsche Telekom services)
- CERT (Cyber Emergency Response Team) information sources

▶ Page 6

SECURITY ON THE INTERNET

▶ Continued from page 5 – Early warning systems: What they are and how they work



Visible and usable honeypot data

To obtain an even faster, more up-to-date overview of the security situation, Deutsche Telekom will publish a new website contributing to the German government's cyber-alliance at CeBIT 2013.

The website www.sicherheitstacho.eu will function on all modern browser platforms without prior registration.

The following data will be shown on the website:

Overview of current cyber attacks

The map of the world presented here provides a visual display of the attacks on the sensor network (honeypots) at a specific time. Countries are also color-coded based on the number of successful attacks.

Top 5 countries of origin for attacks in the previous month

This table includes the above color-coding system and ranks the top 5 countries of origin for the previous month.

Distribution of attack targets (for the previous month)

This table describes the attacks that have been identified by the distributed sensor network according to the target of the attack (Technology).

Total number of attackers per day (for the previous month)

This graphic shows the total number of attackers per day distributed across the previous month.

Total number of attacks per day (for the previous month)

In addition to the figures for the number of attackers per day, this graphic shows the number of attacks (alerts) per day distributed across the previous month.

Distribution of attack targets (for the previous month)

This graphic shows the attacks that have been identified by the distributed sensor network according to the target of the attack (technology).

SECURITY ON THE INTERNET
AN OVERVIEW OF HONEYPOT SYSTEMS

Honeypots are a software that simulates vulnerabilities in applications without putting the host system at risk.

A honeypot is usually an application (or a component like a Web application firewall in logging mode), which diverts hackers from their actual goal or locks them into specially prepared areas where they are unable to do any damage. This function can be compared to actual pots of honey, used in nature to keep wild bears away from human victims.

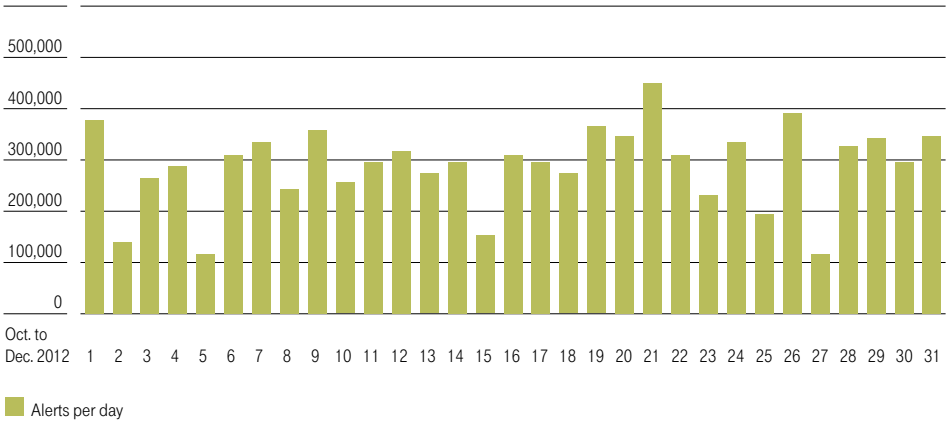
Honeypots have been known in the IT world for more than 10 years, however those that operate at the Web-application level are more recent – they were only introduced during the past five years. The first honeypot approach was implemented by US astronomer Clifford Stoll and recorded in his book "The Cuckoo's Egg" (1986). In this particular case, the idea was to detain Europe-based hackers who used dialup connections for their attacks in the system long enough to allow a trace from the USA back to Hannover.

Deutsche Telekom set up this kind of systems for the first time in April 2010. Initially, it was only designed to make inferences to attacks on DT Web applications possible. DT now uses the data for a variety of purposes, including supplying information to end-customers and other Internet service providers (ISPs).

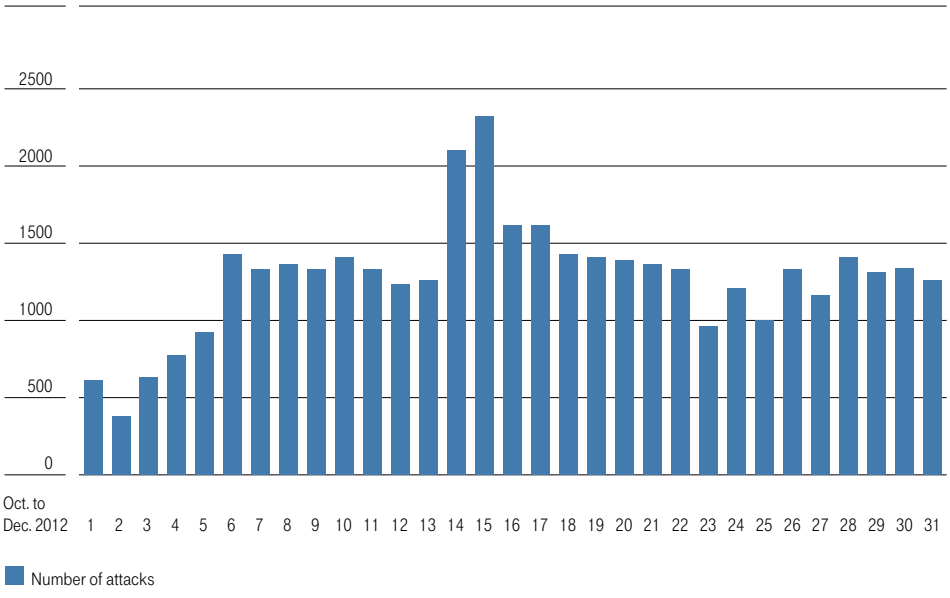
Honeypots are of a fundamentally reactive nature. Client-side honeypots are the only exception, as they visit websites autonomously, access data and can thereby recognize so-called "drive-by attacks".

▶ Page 8

Alerts per day October to December 2012



Number of attacks October to December 2012



SECURITY ON THE INTERNET

▶ Continued from page 7 – An overview of honeypot systems

Deutsche Telekom currently operates over 92 honeypot systems, the majority of which are Web application honeypots. The Deutsche Telekom Group is also constantly expanding the systems in its international networks and systems, to identify new forms of hacking attacks on broader levels, and to guard against them.

Due to the general statistical information from the honeypots, it is not possible to make a definitive statement about the extent to which the production infrastructure, including websites like www.musicload.de for example, is being attacked. In order to get a practical, relevant picture, Deutsche Telekom is increasingly supplementing the early warning system with data points on production servers (Web application firewalls, which deliver sensitive data to the correlation engine when in logging mode). Some administration portals for end-customers are currently being included, for example.

Honeypot systems for Web applications

The honeypots (excluding the Web-application-firewall modules) are isolated from Deutsche Telekom's real infrastructure, so that in the event of an attack, these honeypots cannot become a threat to this infrastructure. The Deutsche Telekom Group's Web-honeypot systems are self-learning, which means that they identify unknown attacks using heuristic methods, analyze them and integrate their patterns into the systems' own recognition process.

The Deutsche Telekom Group's honeypot systems registered a total of 32,767 individual attackers from January 1 to February 11, 2013. By definition, each attacker can carry out one or more attacks. The total number of individually simulated vulnerabilities was 1,023,980 as of February 6, 2013 (compared to just 816,270 vulnerabilities in September 2012).

Analyses of the most frequently attacked applications have shifted only marginally as a result of the broader honeypot spectrum. With Web applications, we continue to see a very high number of automated attacks against simulated Wordpress and Typo3 systems. No new trends have been observed with regard to hackers' defensive measures against honeypots.

With so-called Remote Code Execution attacks in the PHP field in particular, the level of masking or coding of the malware remains conspicuously high. In the past, hackers used just one PHP command for encoding, whereas they're now using several codes consecutively.

REMOTE CODE EXECUTION/REMOTE FILE INCLUSION (RFI)

Remote Code Execution (RCE) / Remote File Inclusion (RFI) refers to attacks in which the targeted system executes a code that was sent by the attacker. In the case of Web applications, a PHP code is often executed, which the hacker has sent along or referenced directly.

In December 2012, the case of Remote Code Execution within Ruby on Rails (ROR) applications emerged in addition to traditional PHP Remote Code Execution (see also the details at the beginning of the report).

We have known about some of these security gaps since May 2010, and appropriate updates have long been available. Since the attacks are still being carried out, it seems likely that unpatched online systems with outdated software versions can still be targeted today. Our findings indicate that the attacks on these vulnerabilities were extensively automated.

The most common attack methods in this area are the same as last quarter and again reflect typical attack patterns (manual and automated):

- SQL Injection
- PHP Code Injection/Execution
- Remote File Inclusion

None of the attacks observed in the last quarter are of a new kind, and they can easily be hindered by implementing strict input validation procedures. Current trends show that despite the availability of best practices on the topic of input validation, attacks based on missing input validation are still among the most common forms of attack.

11,201 malware programs were registered by the honeypot systems in 2011. Only 427 malware programs were registered in 2012, which shows that the rate of increase in new malware programs has significantly leveled out.

▶ Page 9

SECURITY ON THE INTERNET

▶ Continued from page 8 – An overview of honeypot systems

Attacks differentiated by country

Country	Number of attacks October to December 2012
Russian Federation (RU)	3,501,921
Romania (RO)	2,192,024
Taiwan (TW)	1,463,875
Ukraine (UA)	1,374,210
Australia (AU)	743,606

Secure Shell Honeypot systems (SSH)

Since December 2010, Deutsche Telekom has been operating several Secure Shell honeypots (SSH) in addition to the established Web application honeypot systems. These honeypots simulate SSH servers and make it possible to record the course of an attack while collecting the employed malware and authentication information for later analysis. These are "low interaction" honeypots, which have limited functionality yet are able to deliver very good results when it comes to automated attacks.

According to our findings to date, many attacks are being conducted according to the brute force principle, which means that all possible combinations of usernames and passwords are attempted. We know this from the failed logins, which show us, depending on the tool used, the exact combinations and sequences of usernames and passwords employed.

It is also worth mentioning that almost every successful hacker conducts a check to find out whether the server they have taken over is equipped with a sufficient broadband connection. The speed is usually measured by downloading service packs of Microsoft products because these have sufficient length to allow for speed tests.

Deutsche Telekom has also observed that the first hackers could "successfully" penetrate a SSH honeypot using a standard password with eight digits after four hours.

The previous analysis shows that we have primarily seen dictionary-based brute force attacks on the basis of machine-generated passwords (e.g. AAAAA, AAAAB, AAAAC). In the SSH honeypots, connection disruptions are repeatedly being observed, although it's not clear whether these are indicative of targeted attacks on the SSH implementation or "just" of mistakes made by the hackers.

The malware uploaded after a successful attack can be classified into the following categories:

- Programs that make it possible to access administrator rights (so-called exploits, local privilege escalation).
- Scan programs to identify other vulnerable systems online.
- Programs to attack authentication mechanisms (brute force attack programs).

Please note: After the password on one SSH honeypot was changed to a far more complex one, there were only two individual successful hacks within two months. From this, we learned that most brute force attacks were based on existing password lists and that the hackers execute no, or at least significantly fewer, successful brute force attacks against passwords of 12 characters.

Mobile honeypots

In addition to the traditional honeypots described previously, which generate data from the fixed network (data centers, virtual servers and systems on DSL connections), Deutsche Telekom also decided to operate honeypots that simulate the iOS (iPhone, iPad) and Android operating systems.

The goal was to develop honeypots that simulate iOS/Android-based smartphones in mobile access networks and record any attacks on these devices.

This new, adapted form of existing honeypots, based on the "Kippo" OpenSource software among other things, is fully functional and shows that systematic brute force attacks against open systems in mobile networks are now routine.

In addition to the SSH honeypot Kippo, Deutsche Telekom also utilizes the "honeytrap" OpenSource software in order to recognize generic attacks in mobile networks. However, observations to date clearly show that most of the attacks follow the same pattern in all access networks.

Deutsche Telekom has made this technology of the honeypot system for mobile networks available to its partners worldwide. ▶ Page 10

SECURITY ON THE INTERNET

▶ Continued from page 9 – An overview of honeypot systems

Database honeypots

Database honeypots do not represent a fundamentally new class of honeypot. The first honeypots of this kind have been available since 2006. The initial focus was on the emulation of Microsoft SQL servers, because this server type was easy to attack due to far-reaching access opportunities on the file system in cases of faulty configuration, and because a default account (q.v.) was well known.

In 2011, the well-known "Dianoea" OpenSource project expanded an emulation of MySQL databases. Deutsche Telekom established its first MySQL database honeypots based on this in the first quarter of 2012, and developed its own, additional solution in the course of the year.

The experiences of 2012 show that the MySQL honeypots are only attacked in an intermittent and sporadic way, but that the individual attacks here display a considerable volume, with more than 500 login attempts.

The MySQL honeypots are used in two different operating modes:
1. Denial of every login attempt (goal: To collect access data).
2. Acceptance of every login attempt (goal: To record and analyze hackers' actions after login).

Outlook: Client honeypots

One of the variations that Deutsche Telekom has not yet covered is client-side honeypots. Automatisms that cyclically visit websites through Web-browser automation and then analyze changes in the data system in order to recognize so-called "drive-by attacks" are often discussed in this context.

Previously observed OpenSource solutions based on wrappers for Javascript engines have not proven productive to use.

A malware code analysis can then be carried out on the basis of the well-known scan service Virustotal, as well as on the basis of the well-known sandbox solutions. This kind of drive-by attack recognition could also be applied in the context of the activities of the Computer Emergency Response Team (CERT). A detailed study of these honeypot technologies and of the market environment is planned for the coming months.

SSH:
Secure Shell or SSH refers to both a network protocol and to corresponding programs that are used to establish a secure connection to a remote system on the basis of an SSH protocol.

SMTP:
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

iOS:
iOS (known as iPhone OS before June 2010) is the operating system for the mobile end-device from Apple.

MySQL:
MySQL is an OpenSource database that is the main component for many projects. The producer of the database was taken over by Oracle, which is still further developing the free OpenSource database MySQL today.

MALWARE:
Malware, sometimes called malicious code, usually refers to programs that execute malicious functions without the knowledge of the user. Strictly speaking, this includes Trojans, viruses and worms.

SECURITY ON THE INTERNET
HANDLING ABUSE: EXAMINATION OF EXTERNAL REPORTS AND COMPLAINTS

The Abuse team acts as the point of contact for individuals and customers who want to report the abuse of Internet services offered by Deutsche Telekom. The focus is currently on the German business, because the IP addresses used for DSL dial-in to the Internet here, among other things, are saved for seven days to combat abuse.

Examples of abuse of Deutsche Telekom services include:
- Receiving/sending unwanted e-mails, for example containing advertising content (spam)
- Receiving/sending e-mails containing viruses Trojans and worms
- Hacker attacks on computers (port scans or similar)
- Suspected abuse of account information
- Criminal content on customer websites
- Phishing sites from Deutsche Telekom Internet portals or those of companies generally

It should be noted that in particular, the sending of e-mails with attached viruses or Trojans has decreased significantly in recent years. The trend for customer infections through visiting contaminated websites ("drive-by") is clearly visible in the statistical evidence.

External reports submitted to the Abuse team are classified into three main categories:

1. Spam via IP
   The "Spam via IP" category refers to unwanted e-mails containing advertising content (spam) being sent directly to other online systems by bypassing the regular T-Online mail servers.

2. Hosting/websites
   The "Hosting/Websites" category includes e-mail complaints about hosting spam (sending spam via websites) and criminal content on customer websites. Due to a significant increase in criminal website creations since May 2011, the amount of spam sent via these websites has also grown significantly.

3. Reports on hacked customer accounts
   Last year, the "Hacking/Port scan" area was also included here. Customers' reports on suspected port scans were recorded in this category. The category has now been changed to include complaints about compromised customer accounts, for example those based on reports from the Shadow Server Foundation.

ABUSE DEPARTMENTS AND TEAM:
Internet Service Providers' Abuse departments handle (customer) complaints and help customers whose computers are infected with malicious codes such as spam-bots.

Reports submitted to the Abuse team are generally first checked for their relevance and accuracy. The team then informs affected customers about the incident/procedure. This can be information about a probable infection of the customer's computer with a virus or a Trojan, for example, or a report of port scans coming from an infected computer system. The customer is advised to remove the malware with current anti-virus software as soon as possible, and is accordingly provided with examples and resources for security software. If the customer does not respond and their computer continues to attack other online systems with things like spam, the Abuse team may initiate further measures. As a last resort, individual services like e-mail dispatch may be blocked in this case.

The Deutsche Telekom Abuse team depends on external input to identify computers affected by abuse or infection and inform the customers.

The main external partners are:

- Shadowserver Foundation
- Scomp Service (AOL)
- Abusix Global Reporting Project
- NetCologne
- Uceprotect
- 1&1 / United Internet
- Junk Email Filter
- Trend Micro
- Gossler
- SpamVZ
- Hotmail freemail provider

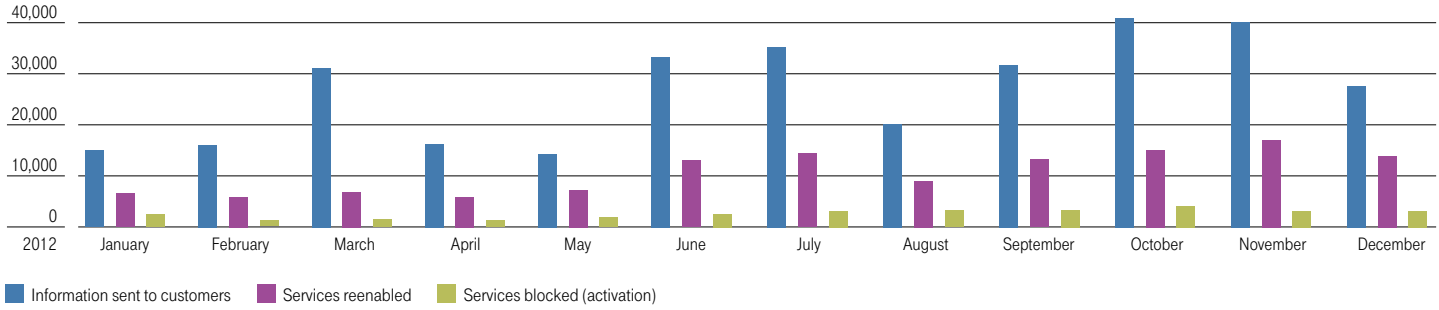
The honeypot infrastructure also provides data to the Abuse team. At 12,000 notifications per year, the current volume is at a negligible level. Significantly higher volumes of data are expected to result from the further expansion of the honeypot infrastructure.

▶ Page 12

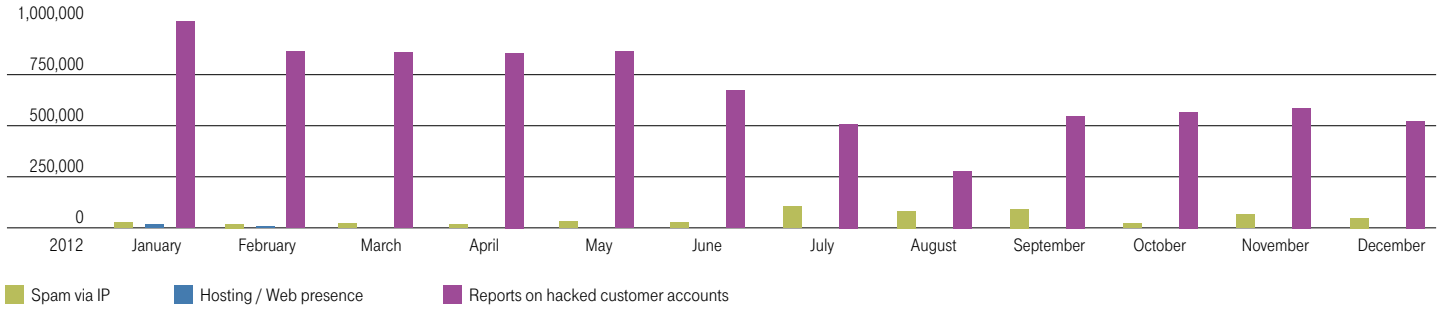
SECURITY ON THE INTERNET

▶ Continued from page 11 – Handling Abuse: Examination of external reports and complaints

Customers contacts



Complaint categories



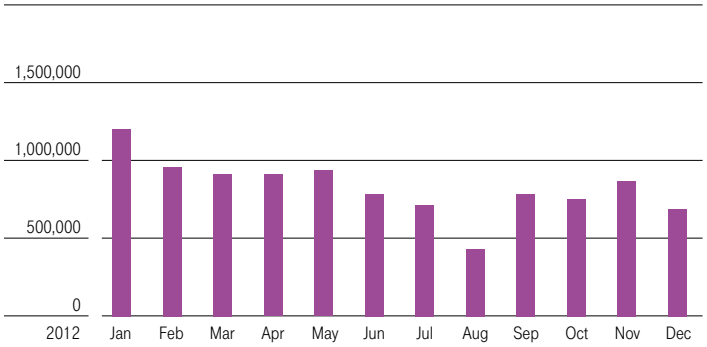
Abuse of Deutsche Telekom services

The total number of abuse reports submitted to Deutsche Telekom increased to 12.7 million in 2012. After an increase to 6,996,309 reports of abuse in the first six months of 2012 (compared with 3,278,947 in the third quarter of 2011 and 2,611,136 in the fourth quarter) only 5.8 million additional reports were submitted in the second half of the year.

In the first half of 2012, the Abuse team wrote to 137,237 Deutsche Telekom customers to inform them that their computers seemed to be infected with malware (compared with 162,517 in the second half of 2011). 200,003 customers were contacted in the second half of the year, which means that despite a 10-percent decrease in complaints submitted, 50 percent more customers were contacted.

In total, service limitations such as “port 25” blockings were established for 132,906 customers in 2012 (48,582 in the first six months). That puts the blocking measures carried out back on the same level as in 2011 (32,265 in the first quarter of 2011).

Incoming complaints



SECURITY ON THE INTERNET

DEUTSCHE TELEKOM CERT: CYBER EMERGENCY RESPONSE TEAM

The Deutsche Telekom Cyber Emergency Response Team (CERT) has the important task of protecting the Group and its customers from the dangers of the Internet. The Deutsche Telekom CERT is the central point of contact for employees, customers and citizens to report cyber-incidents, which are then processed by the CERT. In addition, the CERT establishes mechanisms for the early recognition of attacks on internally as well as externally accessible systems.

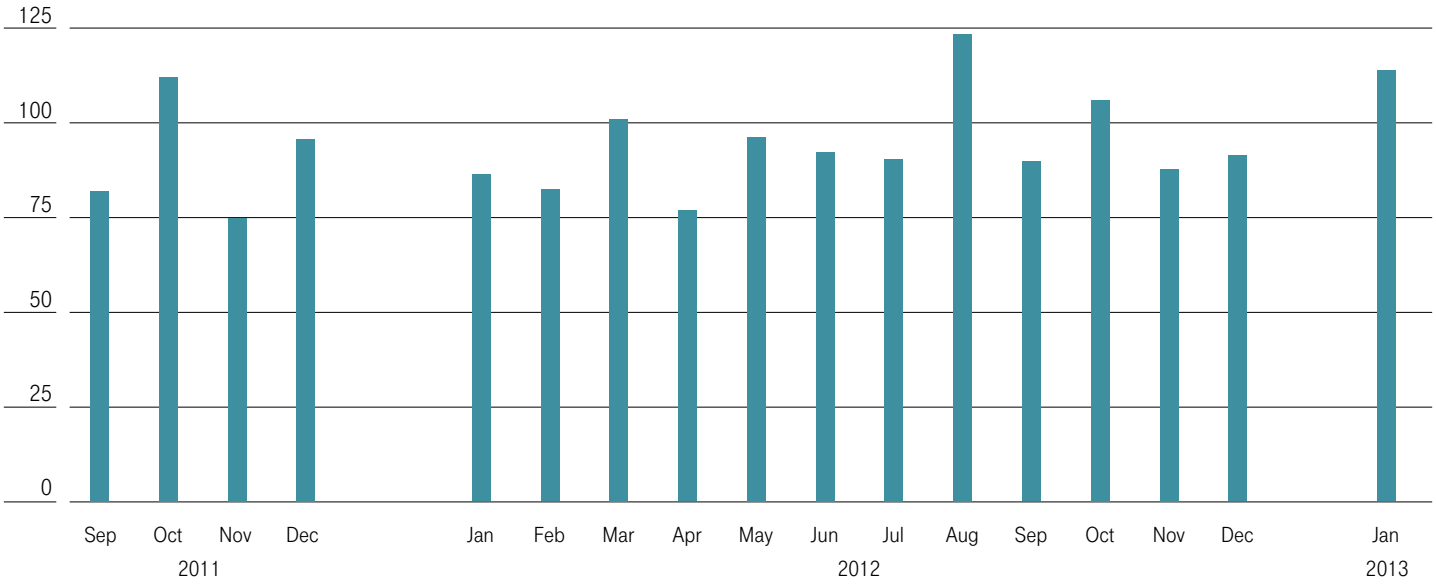
The tasks of the Deutsche Telekom CERT include:

- **Cyber-incident management:** Coordination and management of critical security incidents.
- **Strategic threat radar:** Identification and analysis of threats to the Group's current and future core technologies.
- **Advisory management:** Evaluation and distribution of security advisories and recommendations for action within the Group, as well as monitoring the implementation of critical security updates.
- **Security audits:** Inspection and analysis of security architecture, security processes and system landscapes in company areas that are exposed to a higher level of potential threat from the Internet.
- **Vulnerability scanning:** Regular execution of security scans on those portals and systems that are accessible via the Internet.

Furthermore, the Deutsche Telekom CERT is an international point of contact for topics of Internet security and cybercrime. In this field, projects and initiatives that improve security on the Internet are developed with relevant stakeholders including the German Federal Office for Information Security (BSI), the European Network and Information Security Agency (ENISA), the European Commission (EC) and the German Federal Criminal Police Office, as well as the inter-trade organizations GSM Association (GSMA), ETNO, ETSI and the Forum for Incident Response and Security Teams (FIRST). The Deutsche Telekom CERT is currently focused on advanced persistent threats (APT) in particular. In collaboration with the BSI, the Deutsche Telekom CERT has initiated a project that aims to identify suitable measures with respect to this. The results will be made publicly available.

▶ Page 14

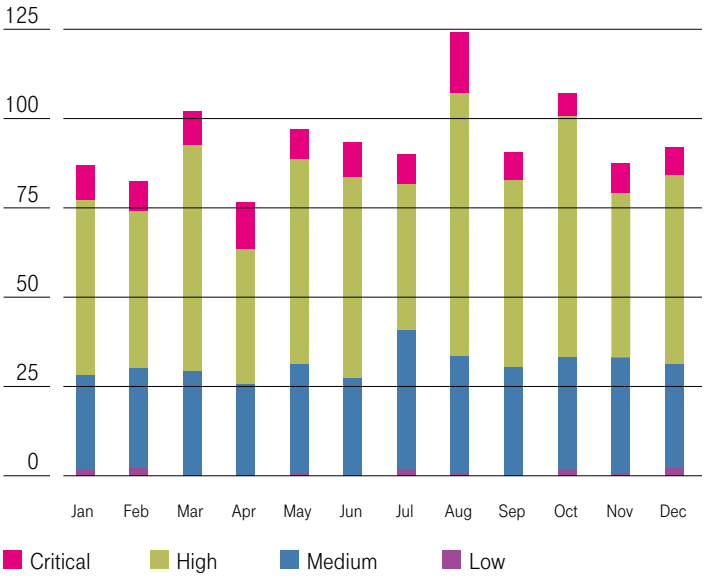
Advisories September 2011 to January 2013



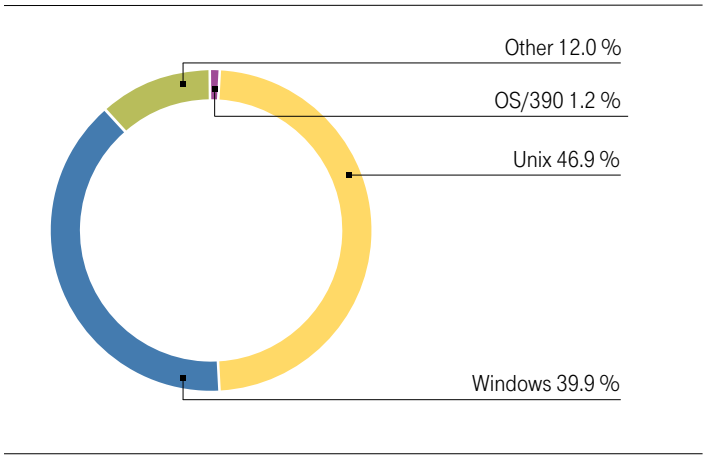
SECURITY ON THE INTERNET

▶ Continued from page 13 – Deutsche Telekom CERT: Cyber Emergency Response Team

Advisories 2012



Affected operating systems



Statistical information about vulnerabilities

The image above shows the distribution of security advisories over several months. From year to year, the numbers of security advisories published are as follows:

2010 1,137 security advisories
2011 1,174 security advisories
2012 1,120 security advisories

The evaluation of the security advisories concerning their level of criticality shows an essentially constant high proportion of advisories defined as “critical” or “high” level. Many of these advisories address vulnerabilities that could lead to Denial of Service attacks or so-called drive-by infections.

A look at the operating systems affected reveals hardly any observable difference to previous reports. Due to the high market penetration of Unix and Windows systems, both operating systems have almost the same share of vulnerabilities: In a direct comparison, the shares are 47 percent for Unix systems and 40 percent for Windows systems.

Cyber-incident management

The Deutsche Telekom CERT is responsible for international cyber-incident management through crisis and project management. The CERT assesses the criticality of incidents, involves experts from Group Information Security and other technical experts if necessary, and is responsible for reporting to the top Management and the Board.

When security incidents occur within the Deutsche Telekom Group, the CERT drafts in so-called information advisories – depending on necessity and the incidents’ respective criticality – to inform other parts of the Group about the security incident and to recommend measures that will prevent the incident from extending to other branches of the company. Security incidents can be reported by e-mailing cert@telekom.de or by phoning 0800 DTAG CERT.

Deutsche Telekom CERT strategic threat radar

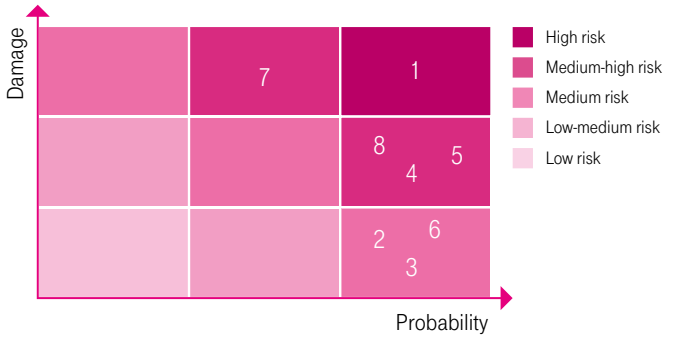
The Deutsche Telekom Group’s Board of Management needs to be put in a position to identify and assess threats with regard to their effects on business at an early stage. This allows for a timely planning of security measures. As part the strategic threat radar, innovative trends and future technologies are examined, as are technologies that are already in use.

▶ Page 15

SECURITY ON THE INTERNET

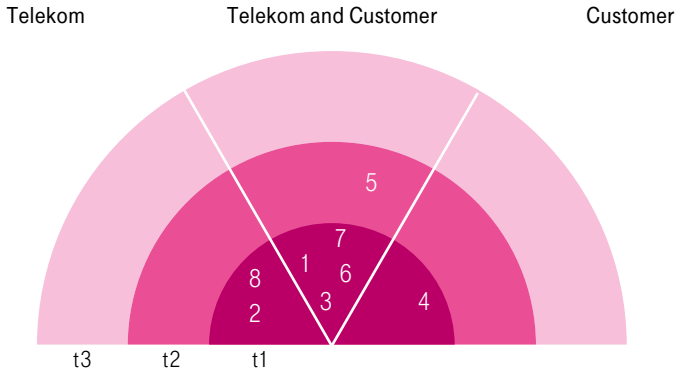
▶ Continued from page 14 – Deutsche Telekom CERT: Cyber Emergency Response Team

Risk portfolio



1 Advanced persistent threats
2 Spear phishing against DT
3 Mobile malware
4 Attacks on mobile banking
5 DoS on DNS
6 Attack on DSL router
7 Cloud recovery failure
8 Shitstorm

Threat radar



t1 Active utilization of known vulnerability
t2 Vulnerability exists and proven usability
t3 Vulnerability exists and theoretically usable

Key contents of the strategic threat radar:
The trend-scouting community is a new instrument of the strategic threat radar methodology. The idea is for security experts from the IT and network industries to communicate on an international scale. Deutsche Telekom is using a collaboration software that allows participants to identify and discuss technology trends and threats specifically for this purpose. The Deutsche Telekom CERT uses this community to take highly individual technologies and trends into account in their risk analysis as well.

Advanced persistent threats (APT):
APT refers to the combination of different tools and methods of attack such as social engineering, SQL Injection, (spear-)phishing, Trojans and botnets. By means of a persistent APT attack, the chain from the desktop to the production systems becomes compromised for a long period and company information is revealed. The number of affected businesses is constantly increasing. Theft and unauthorized publication of information, as well as impairment to the availability of services can cause massive damage to a company's reputation and lead to a loss of customers.
Security measure: Establishing a security framework of organizational and technical controls; identifying critical data and systems; implementing security requirements more strongly and supervising systems according to the criticality of these systems and data.

Spear-phishing (against Deutsche Telekom employees):
Spear-phishing is a phishing attack on a specific group of people or a single person, often connected with the goal of gaining access to or compromising company information.
Security measure: Raising awareness for this topic is crucial to the key functions of every company. A strict patch management for the systems that are most often attacked, such as Web browsers and add-ons (flash/macromedia), Office Suite, mail clients and operating systems. A further measure is network and data segmentation.

Mobile malware:
Malignant and fraudulent malware programs on mobile terminals, which are distributed over app stores without quality checks, can cause extensive damage. Mobile malware programs can build up botnets for smartphones, for example. Possible targets of attack are reachable from the Internet using infrastructure components.
Security measure: Installing anti-viruses and anti-malware onto mobile terminals as a standard configuration, user-awareness campaigns for identifying safe apps.

Attacks on mobile banking:
Several techniques to avoid the use of authentication procedures for mobile banking can be found on the Internet nowadays. We have pointed out the variations in different parts of this ▶ Page 16

SECURITY ON THE INTERNET

▶ Continued from page 15 – Deutsche Telekom CERT: Cyber Emergency Response Team

report. Examples are so-called "Zeus" Trojans on mobile end-devices (on Blackberry, Symbian, and Android), SpyEye (PC-based malware). The end-users are most at risk, as they are often involved in executing the malware program without realizing it.
Security measure: Implementing virus protection on smartphones; awareness programs about vectors of attack and protective measures in the banking sector, educational programs for customers.

DoS on DNS:
Mobile malware programs for smartphones construct mobile botnets. The targets of these attacks are network components that can be reached from the Internet.
Security measure: Strengthening applications and systems with direct Internet access, supported by security patch management, vulnerability and advisory management, patch-level scanning.

Attacks on DSL routers (Chuck Norris worm):
Routers that have been infected with malware like the Chuck Norris worm become part of a botnet. The malware affects weakly configured routers and DSL modems. The security threats install themselves by working out standard administration passwords. The large-scale exploitation of weak access configurations has been proven. Among other things, the DNS server inputs were manipulated.
Security measure: Intensified educational campaigns informing users that they should change the standard passwords and accounts on DSL routers and Internet access devices that are new from the factory.

Cloud recovery failure:
on cloud services. Threats to the cloud's availability and reliability through large-scale outages of cloud services. Well-respected cloud service providers suffered a momentous outage to their cloud services in 2011 and 2012, which led to a loss of data and service outages for their customers. The damage to availability and reliability caused a loss of reputation and a loss of customers.
Security measure: Separation of cloud-based data and duplication of critical data on server territory in different geographical locations. Continual checking of suitable backup and restore solutions, and concepts that should be supported by a suitable emergency response management in disaster recovery.

Shitstorm:
Shitstorms or waves of rebellion are an Internet phenomenon that produce a high volume of Internet entries that mix fact and fiction, correct and incorrect information. This information is picked up by public media and brought to the attention of the affected companies' management. The consequence of this is that due to considerable public pressure from the media based on false information, companies are forced to immediately invest massive resources into examining the problem and implementing communication measures. In doing so they are diverted from real, critical problems and relegate these to a lower priority level.
Security measure: Targeted, personal awareness measures should be implemented to advise on the risk of hasty action based on shitstorm information.

Invitation
The Deutsche Telekom CERT invites experts from all areas of the Deutsche Telekom Group to become trend scouts and contribute to updating the strategic threat radar and assessing potential threats. For more information, please contact cert@telekom.de directly.

Facts and figures for 2012

Number of honeypot systems operated by Deutsche Telekom	92
Total number of vulnerabilities simulated in honeypots	1,023,980
Number of individual malicious codes collected in the Web application honeypots	11,628
Number of reports of abuse submitted	12.7 million
Number of service blockings (for example e-mail)	132,906
Number of network access restrictions removed	33,693

SECURITY ON THE INTERNET

CONTACT

Abuse Team
Deutsche Telekom
Group Information Security
Abuse Team
T-Online-Allee 1
64295 Darmstadt, Germany
E-mail: Abuse@t-online.de

Deutsche Telekom CERT
Deutsche Telekom
Group Information Security
Landgrabenweg 151
53227 Bonn, Germany
E-mail: CERT@telekom.de

Editorial Office
Deutsche Telekom
Group Information Security
Friedrich-Ebert-Allee 140
53113 Bonn, Germany
E-mail: CERT@telekom.de

LIFE IS FOR SHARING.