VULNERABILITIES IN CORPORATE INFOSYSTEMS: THREATS GROW FASTER THAN SECURITY

Eugeny Gnedin, Eugenia Potseluevskaya

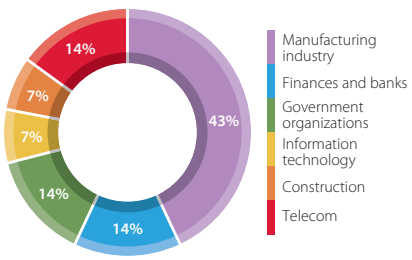
In 2013, many large companies witnessed a drop in their information security levels — in relation to both internal and external attacks. These days, attackers need to only have novice skills to carry out successful attacks, with fewer vulnerabilities required as compared to 2011 & 2012. One reason for threats becoming more numerous can be attributed to the fact that significantly fewer of the systems incorporated timely security updates. Unfortunately, conventional security practices (use of encryption and antivirus software, improvement of user awareness, etc.) alone are not enough to reverse this downward trend.

In 2013, Positive Technologies reached such conclusions after comparing recent penetration test results with that from a similar research survey conducted in 2011 and 2012. During testing, we simulate attacker's actions both from the Internet and from organizations' intranets. This approach allows us to assess a system's actual security level and discover flaws in protection mechanisms including ones that could be missed by using other audit methods.

Source Data

We selected 14 systems including major government and commercial companies from around the world. The majority of the systems analyzed were from the Manufacturing industry. We investigated a series of systems that were geographically distributed, (36%) including those with numerous branches in different cities and countries.

Industrial control systems (ICS) were a common aim of penetration testing in 2013, since their operation is critical and attacks against them are growing in number.



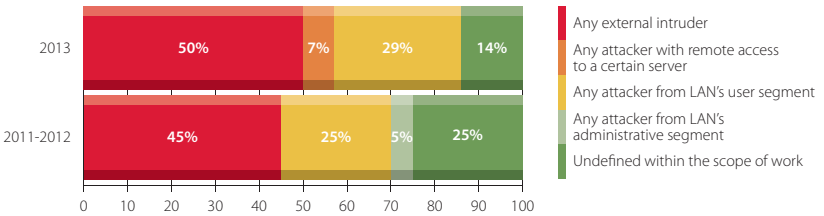
Systems tested by industry

Overall Results

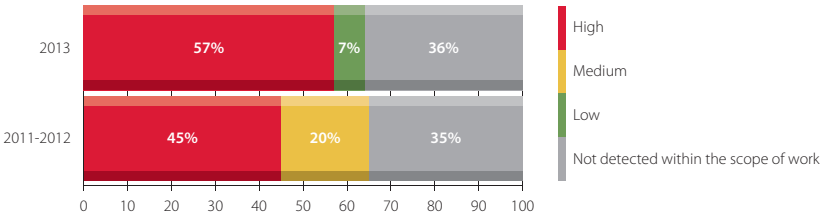
In 2013, **86% of the systems** tested appeared to be exposed to vulnerabilities that could allow an attacker to gain **full control** over critical resources (Active Directory, ERP systems, email systems, network equipment control systems, etc.). Half of the systems studied allowed an outside intruder to gain full control over critical resources. In almost one of every three systems (29%), attackers needed access only to a user segment in an intranet to get control over such resources.

93% of the systems we tested **included critical vulnerabilities** related to configuration flaws. This percentage is much worse than that from 2011 and 2012: during that period, 75% of the systems assessed contained critical configuration flaws.

More than half **(57%)** of the systems analyzed in 2013 had critical vulnerabilities since they used **out-of-date software and OS versions.** This percentage is worse compared to 45% of systems found in 2012. The average age of the most outdated patch is 32 months. One of the systems was detected to contain a nine-year-old vulnerability (as of 2004), which made a DoS attack against Windows possible (CVE-2004-0790).



Minimum privileges required to gain full control over critical resources



Systems compared by the maximum severity of vulnerabilities caused by the lack of security updates

Positive Technologies' Specialists Showed New Attack Scenarios against ICS

A report on ICS security and a contest called Choo Choo Pwn provided by the specialists of Positive Technologies were among the most remarkable events at Power of Community 2013 held in Seoul.

Choo Choo Pwn is an up-to-date large-scale railway model, whose components (trains, railroad crossing gates, and traffic lights) are controlled by an ICS based on three SCADA systems. More than 30 information security specialists tried their hand at hacking the model.

When delivering the report "Techniques of Attacking Real SCADA & ICS Systems", Alexander Timorin, Yury Goltsev, and Ilya Karpov shared the latest results, they obtained while analyzing security of industrial protocols used by SCADA systems, and their vast experience in auditing information systems of critical infrastructure elements. Sergey Gordeychik and Alexey Moskvin spoke about a new technology they implemented to analyze source code, which allowed them to automate vulnerability search, detection of bugging devices and undocumented features in applications.

Security Perimeter Flaws

In 2013, any external intruder acting from the Internet could access internal hosts of **91% of the systems** tested (as opposed to 74% in 2011 & 2012). A malicious user could obtain full control over the company's whole infrastructure in 55% of the cases.

On average, only **two vulnerabilities** had to be exploited to penetrate a perimeter (previously, three vulnerabilities were required). Even novice hackers could conduct attacks in 82% of the cases.

Weak password protection triggered 40% of intranet breaches. This vulnerability is the most widely spread as it was in 2011 & 2012. It was found on the network perimeter of 82% of the systems, every one of which had dictionary passwords in web applications as well. 67% of the companies used dictionary passwords for privileged accounts.

Vulnerabilities connected with the availability **of server and network hardware control interfaces** from external networks (SSH, Telnet, RDP, web interfaces) were commonplace. Moreover, the percentage of vulnerabilities triggered by the **absence of relevant security updates** on network perimeter hosts grew significantly in 2013 to 64%.

The intranet of every third system could be accessed through **web application vulnerabilities.** Such vulnerabilities as Unrestricted File Upload and SQL Injection were common for 55% of the systems. All in all, web application vulnerabilities were detected in 93% of the systems.

Intranet Security Flaws

The security level of intranets also declined as compared to levels in 2011-2012. During that period, 84% of systems allowed attackers to obtain maximum privileges that could be used to control critical intranet resources. However, in 2013, we found that this was possible for **all of the systems** studied (though a number of the systems required attackers to have very high qualifications and to exploit unknown vulnerabilities). 17% of the systems required an insider to have high qualifications to access critical resources; **half** the systems studied could be attacked by **any** unqualified internal user. On average, an attacker needs to exploit **five vulnerabilities** to obtain control over critical resources if access to an intranet is provided (as opposed to seven vulnerabilities required in 2011 & 2012).

According to our 2013 study, the most common vulnerabilities are caused by the use of **dictionary passwords (92%).** The administrators of half of the systems with weak passwords used numeric passwords with less than 10 figures; the most frequently used was **123456** (discovered in one third of system). 36% of the systems used the password "cisco" for network equipment.

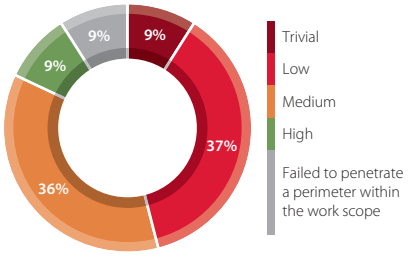
In addition to weak passwords, **security flaws in service protocols** (DHCP, STP, ARP, CDP, DTP) and **storing unencrypted sensitive data** are still quite commonplace. As compared to the data from 2011-2012, the following flaws have undergone certain changes:

— Service protocol protection flaws, which result in hijacking and redirecting network traffic — dropped by 25% (from 92% to 67%).

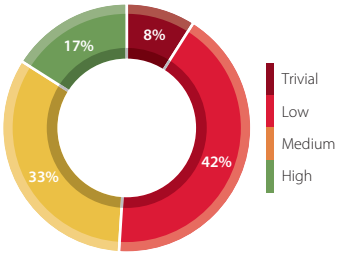
— Use of poorly protected data transfer protocols — dropped by 33% (from 75% to 42%).

— Use of weak encryption algorithms — dropped by 25% (from 42% to 17%).

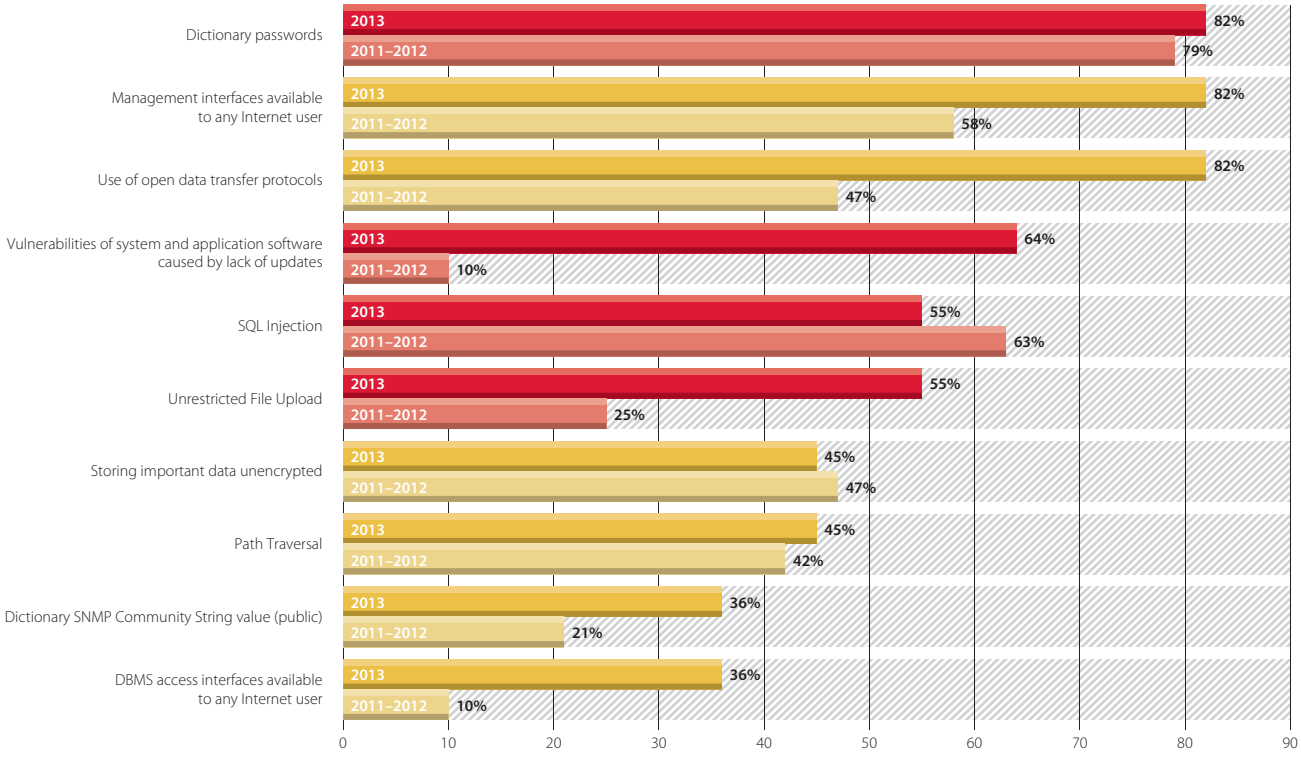
— **Insufficient antivirus protection** — increased by 35% (from 15% to 50%). Curiously enough, the level of antivirus protection improved in 2013 (i.e. antivirus software is installed and databases are updated in time); however, antivirus programs usually lack self-protection features or they appear disabled, and privileged users can disable protection, all of which reduces antivirus efficiency.



Perimeter penetration difficulty (attacker's skills)

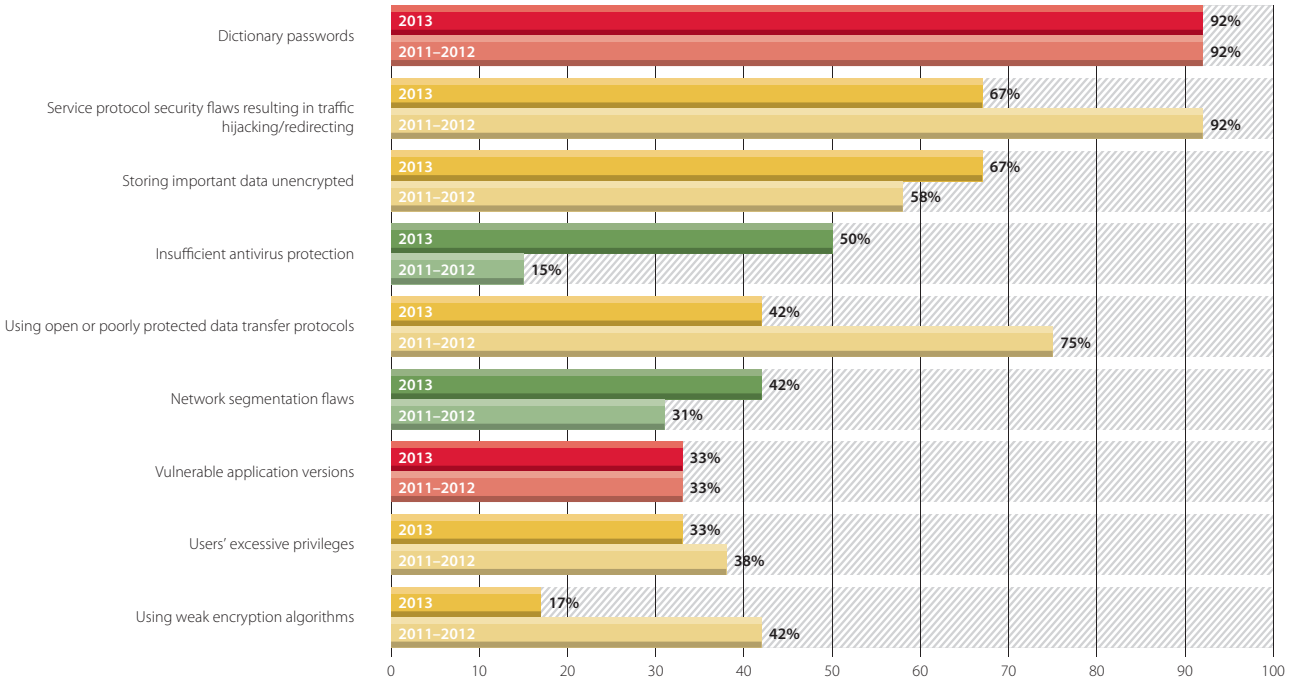


Accessibility of critical resources to an insider



Top 10 network perimeter vulnerabilities

POSITIVE TECHNOLOGIES



Common intranet vulnerabilities

Flaws in Security Awareness

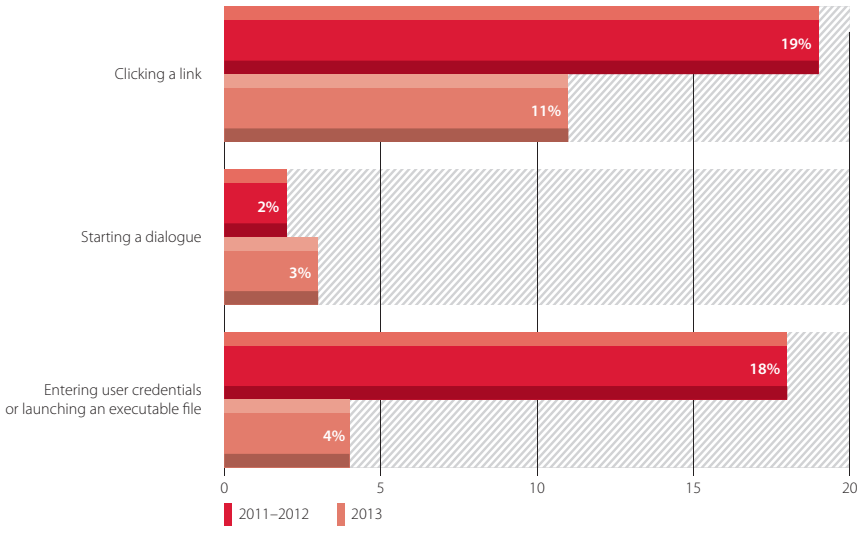
The scope of penetration testing conducted for a number of companies in 2013 included assessment of information security awareness. The analysis consisted of a series of attacks agreed with the customer, which emulated attackers' actions, and further tracking of staff responses. This report focuses on the results of the most widely spread testing tool — emailing with a file or a link to an external resource attached. We tracked any evidence of clicking the link, running the executable attached to the letter, entering credentials if a phishing attack was emulated, or attempts to communicate with the sender. As a rule, emailing was carried out on behalf of an organization's employee.

The results obtained indicate the **improvement of staff awareness** in information security as compared to the results from 2011-2012. The staff awareness level of every third system tested was assessed as satisfactory. The level of the same number of systems was evaluated as lower than medium and low.

The number of cases when users followed a link attached to an email dropped from 19% to 11% in 2013. As to entering credentials and running attached files, their number also dropped from 18% to 4%.

However, the number of users, who **started dialog with a potential attacker,** remained almost the same (3%). Such users' actions cannot cause workstation infection or loss of credentials directly, but interacting with an employee, a malicious user can obtain additional information to develop attacks against a necessary system.

A full version of penetration testing results statistics will be published on www.ptsecurity.com.



The number of recorded events to the total number of emails sent

Positive Technologies at 30C3: Disneyland for Hackers and New Threats for SCADA

The experts of Positive Technologies took part in Chaos Communication Congress, the largest hacker conference in Europe, with more than 9,000 participants, that took place in Hamburg on December 27-30, 2013.

Sergey Gordeychik and Gleb Gritsai from Positive Technologies presented their research of production system security describing the most dangerous vulnerabilities and attacks based on them. Alexander Timorin held a hands-on lab devoted to SCADA security, and Alexey Osipov spoke about DBMS vulnerabilities.

Yury Goltsev and Alexander Zaitsev organized a spectacular contest "The Labyrinth". Participants had an hour to pass a laser field and motion sensors, outwit artificial intelligence, break locks, clear a room of bugs, and deactivate a bomb.

POSITIVE TECHNOLOGIES