MODERN OPERATING SYSTEMS

LECTURE 9

AUTHOR: DR. ZVEREVA OLGA M.

AGENDA

- ✓ TERMS AND DEFINITIONS
- ✓ MAIN THREATS
- ✓ MALICIOUS SOFTWARE
- ✓ SECURITY CONCEPTS
- ✓ SECURITY CONCEPT REALIZATION IN WINDOWS

COMPUTER SECURITY

- **COMPUTER SECURITY, CYBERSECURITY** OR **INFORMATION TECHNOLOGY SECURITY** (**IT SECURITY**) IS THE PROTECTION OF COMPUTER SYSTEMS FROM THEFT OR DAMAGE TO THEIR HARDWARE, SOFTWARE OR ELECTRONIC DATA, AS WELL AS FROM DISRUPTION OR MISDIRECTION OF THE SERVICES THEY PROVIDE [WIKIPEDIA]
- **THE TERM COMPUTER SYSTEM SECURITY** MEANS THE PROTECTION OF RESOURCES (INCLUDING DATA AND PROGRAMS) FROM UNAUTHORIZED DISCLOSURE, MODIFICATION OR DESTRUCTION.

CIA TRIAD

Confidentiality
Integrity
Availability

SECURE INFORMATION SYSTEM MUST HAVE THE FOLLOWING CHARACTERISTICS:

- **DATA CONFIDENTIALITY** (PRIVACY): *A REQUIREMENT WHICH PURPOSE IS TO KEEP SENSITIVE INFORMATION FROM BEING DISCLOSED TO UNAUTHORIZED RECIPIENTS*. THE SECRETS MIGHT BE IMPORTANT FOR REASONS OF NATIONAL SECURITY (NUCLEAR WEAPONS DATA), LAW ENFORCEMENT (THE IDENTITIES OF UNDERCOVER DRUG AGENTS), COMPETITIVE ADVANTAGE (MANUFACTURING COSTS OR BIDDING PLANS), OR PERSONAL PRIVACY (CREDIT HISTORIES)
- **DATA INTEGRITY**: *IS A REQUIREMENT MEANT TO ENSURE THAT INFORMATION AND PROGRAMS ARE CHANGED ONLY IN A SPECIFIED AND AUTHORIZED MANNER*. IT MAY BE IMPORTANT TO KEEP DATA CONSISTENT, OR TO ALLOW DATA TO BE CHANGED ONLY IN AN APPROVED MANNER. IT MAY ALSO BE NECESSARY TO SPECIFY THE DEGREE OF THE ACCURACY OF DATA.
- **DATA AVAILABILITY**: *IS A REQUIREMENT INTENDED TO ENSURE THAT SYSTEMS WORK PROMPTLY AND SERVICE IS NOT DENIED TO AUTHORIZED USERS*. FROM AN OPERATIONAL STANDPOINT, THIS REQUIREMENT REFERS TO ADEQUATE RESPONSE TIME AND/OR GUARANTEED BANDWIDTH. FROM A SECURITY STANDPOINT, IT REPRESENTS THE ABILITY TO PROTECT AGAINST AND RECOVER FROM A DAMAGING EVENT

MAIN TERMS AND DEFINITIONS

- **VULNERABILITY** *IS A WEAKNESS IN DESIGN, IMPLEMENTATION, OPERATION OR INTERNAL CONTROL*. MOST OF THE VULNERABILITIES THAT HAVE BEEN DISCOVERED ARE DOCUMENTED IN “THE COMMON VULNERABILITIES AND EXPOSURES (CVE) DATABASE”.
- **THREAT** *IS A POSSIBLE DANGER THAT MIGHT EXPLOIT A VULNERABILITY TO BREACH SECURITY AND THEREFORE CAUSE POSSIBLE HARM*. A THREAT CAN BE:
  - ✓ EITHER "INTENTIONAL" (I.E. HACKING: AN INDIVIDUAL CRACKER OR A CRIMINAL ORGANIZATION)
  - ✓ OR "ACCIDENTAL" (E.G. ACTIONS OF A NON QUALIFIED USER, OR SOFTWARE WORKING IN AN INCORRECT WAY, OR EVEN THE POSSIBILITY OF A NATURAL DISASTER SUCH AS AN EARTHQUAKE, A FIRE, OR A TORNADO)
- **RISK** *IS THE POTENTIAL OF A SIGNIFICANT IMPACT RESULTING FROM THE EXPLOIT OF A VULNERABILITY*.
- **ATTACK** IS ANY ATTEMPT TO EXPOSE, ALTER, DISABLE, DESTROY, STEAL OR GAIN UNAUTHORIZED ACCESS TO OR MAKE UNAUTHORIZED USE OF AN ASSET (OR IT IS A REALIZED THREAT)

ATTACKS

- In May 2000, the *Internet Engineering Task Force* defined attack in RFC 2828 (Internet Security Glossary) as:

  “*an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.”*

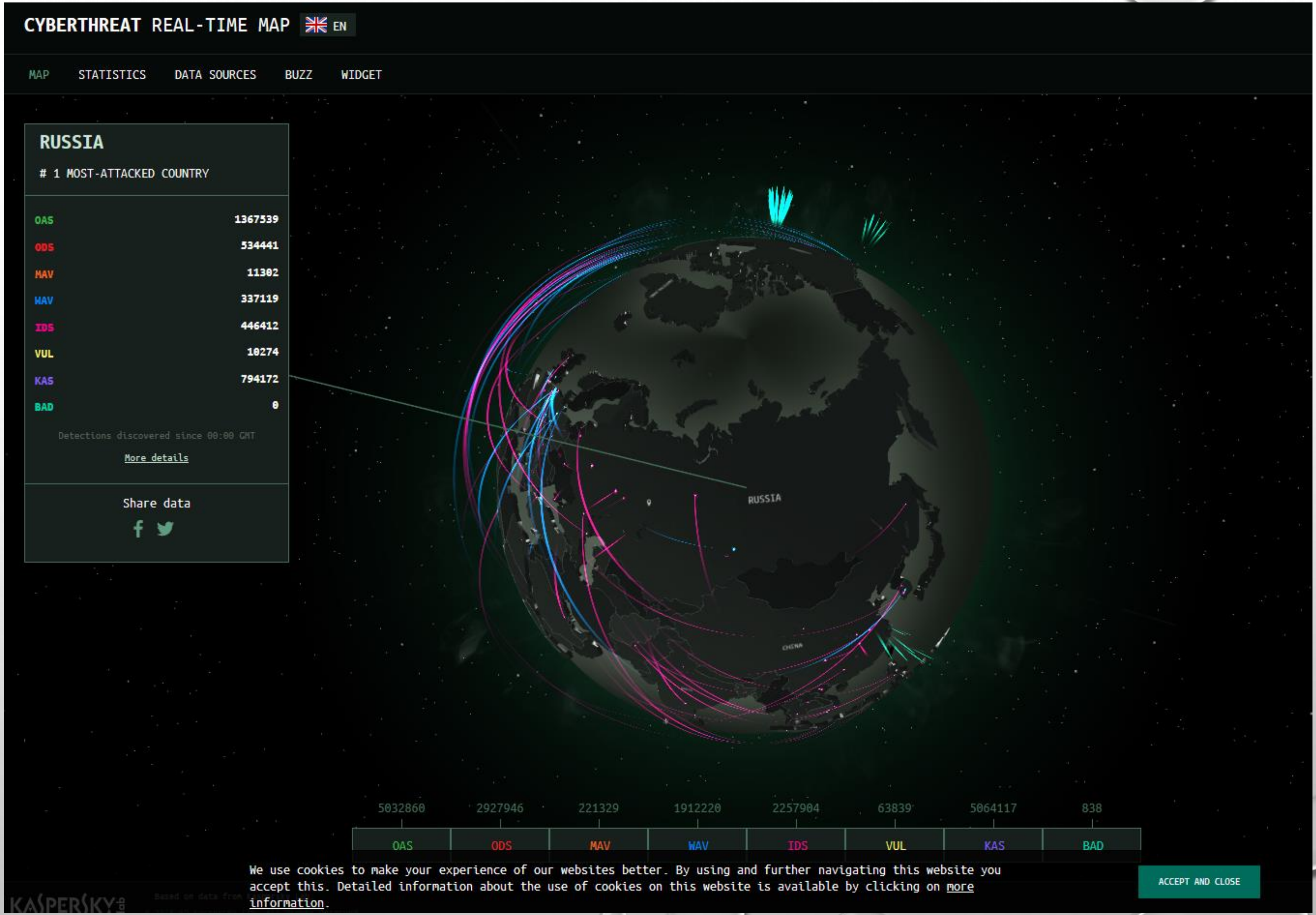
- CNSS Instruction No. 4009 dated 26 April 2010 by Committee on National Security Systems of USA defines an attack as:

  “Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.”

- CNSS Instruction No. 4009 define a *cyber attack* as:

  “An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.”

- *Attacks try to violate one or several characteristics of a safe system: confidentiality, integrity, or availability*



RUSSIA

1 MOST-ATTACKED COUNTRY

OAS	1367539
ODS	534441
MAV	11302
WAV	337119
IDS	446412
VUL	10274
KAS	794172
BAD	0

Detections discovered since 00:00 GMT

More details

Share data

OAS	ODS	MAV	WAV	IDS	VUL	KAS	BAD
5032860	2927946	221329	1912220	2257904	63839	5064117	838

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

https://cybermap.kaspersky.com/

IMPORTANT QUESTIONS

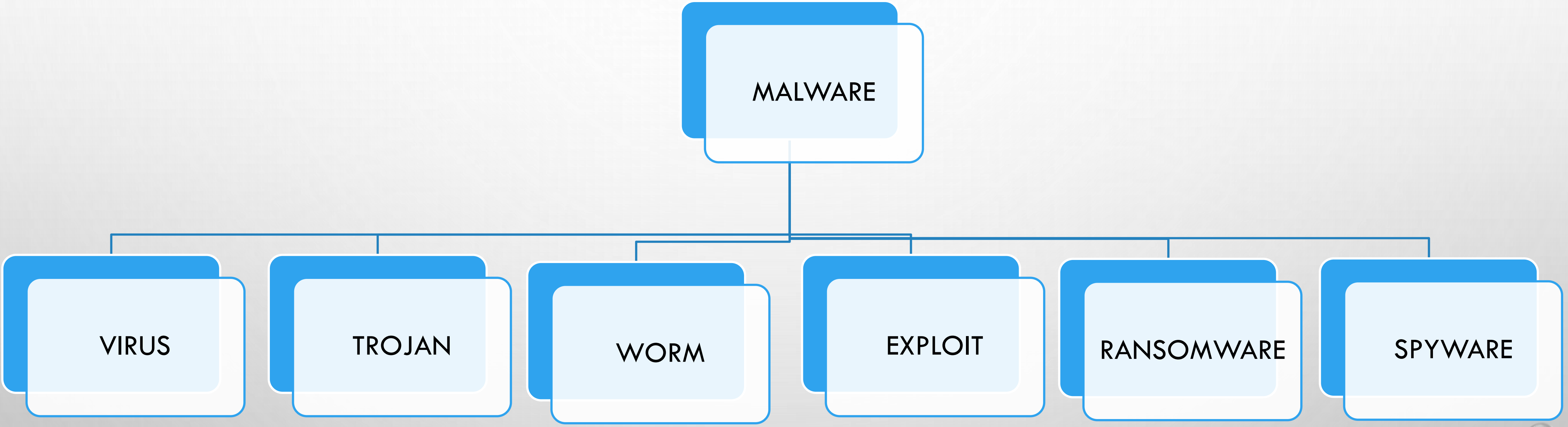
- **WHO ARE ATTACKERS?**
  - ✓ IN SECURITY LITERATURE, PEOPLE WHO TRY TO GAIN UNAUTHORIZED ACCESS TO INFORMATION SYSTEMS, WHETHER FOR COMMERCIAL OR NON-COMMERCIAL PURPOSES, ARE KNOWN AS INTRUDERS, GENERALLY REFERRED AS HACKERS OR CRACKERS.
  - ✓ THEY ACT IN TWO DIFFERENT WAYS: PASSIVE AND ACTIVE.
  - ✓ THE FORMER JUST WANTS TO READ FILES OR DATA FOR WHICH THEY ARE NOT PERMITTED, WHILE THE LATTER IS MORE DANGEROUS, WANTING TO MAKE UNAUTHORIZED CHANGES TO DATA.
- **WHAT ARE THE THREATS?**
  - ✓ INSIDER ATTACKS
  - ✓ OUTSIDER ATTACKS

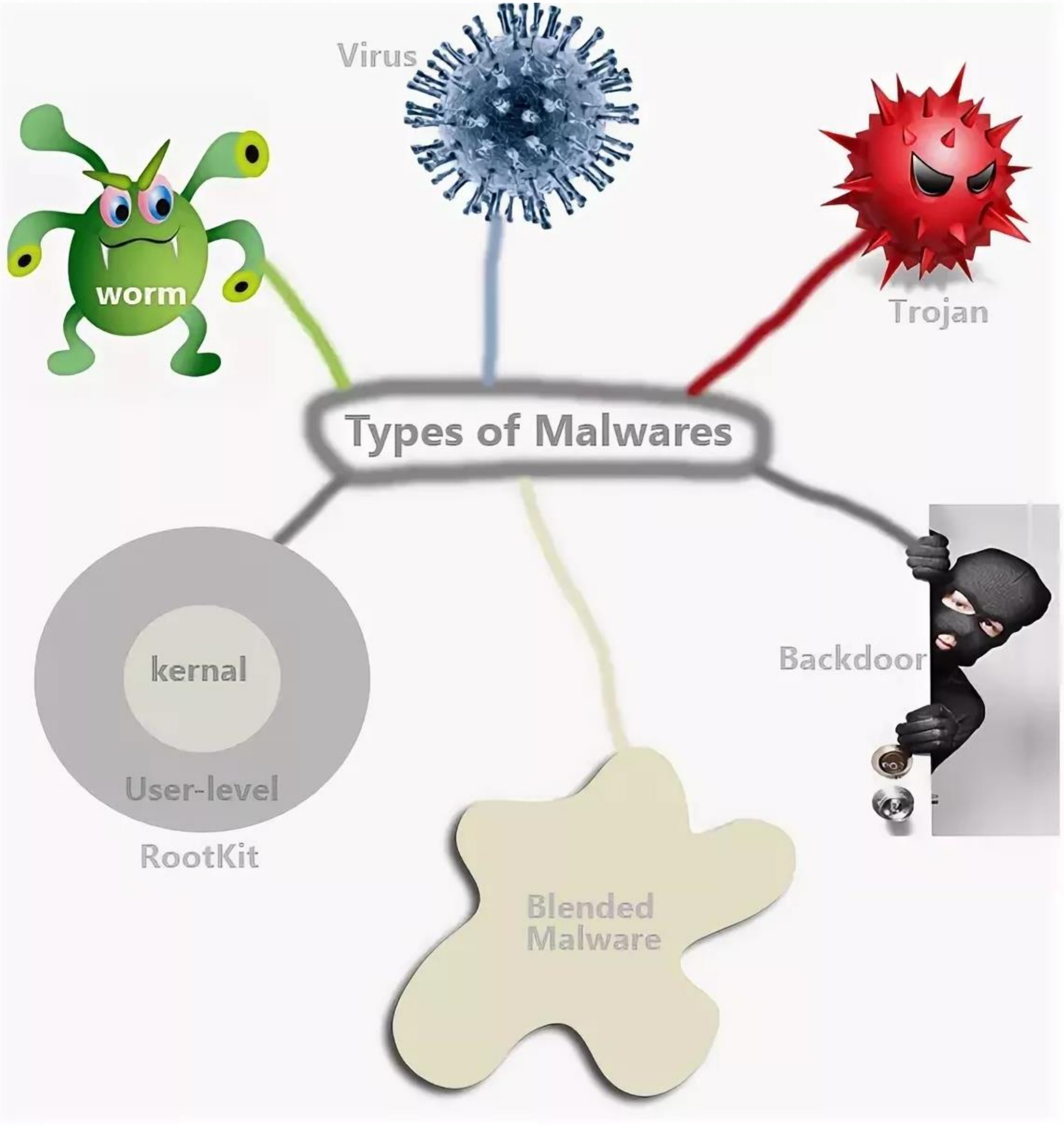
MALICIOUS SOFTWARE

- ➢ MALWARE IS A TERM USED TO DESCRIBE MALICIOUS APPLICATIONS AND CODE THAT CAN CAUSE DAMAGE AND DISRUPT NORMAL USE OF DEVICES.
- ➢ MALWARE CAN ALLOW UNAUTHORIZED ACCESS, USE SYSTEM RESOURCES, STEAL PASSWORDS, LOCK YOU OUT OF YOUR COMPUTER AND ASK FOR RANSOM, AND MORE.
- ➢ MALWARE DOES THE DAMAGE AFTER IT IS IMPLANTED OR INTRODUCED IN SOME WAY INTO A TARGET'S COMPUTER AND CAN TAKE THE FORM OF EXECUTABLE CODE, SCRIPTS, ACTIVE CONTENT, AND OTHER SOFTWARE.

HTTPS://WWW.YOUTUBE.COM/WATCH?TIME_CONTINUE=20&V=N8MBZU0X2NQ

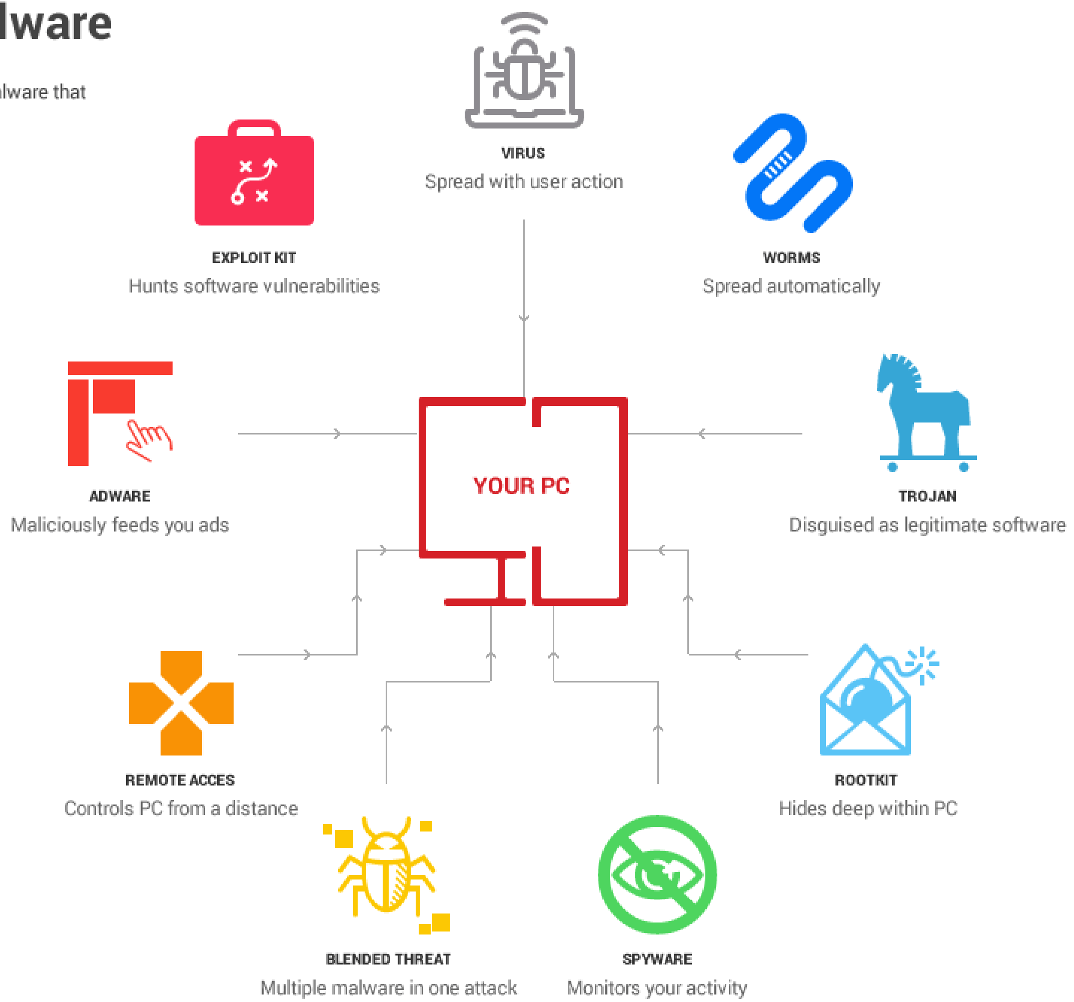
CLASSIFICATION ACCORDING TO KASPERSKY




Virus
worm
Trojan
Types of Malwares
kernal
User-level
RootKit
Backdoor
Blended
Malware

Types of malware

These are the main types of malware that can be found across the web.



EXPLOIT KIT
Hunts software vulnerabilities

VIRUS
Spread with user action

WORMS
Spread automatically

ADWARE
Maliciously feeds you ads

YOUR PC

TROJAN
Disguised as legitimate software

REMOTE ACCES
Controls PC from a distance

ROOTKIT
Hides deep within PC

BLENDED THREAT
Multiple malware in one attack

SPYWARE
Monitors your activity

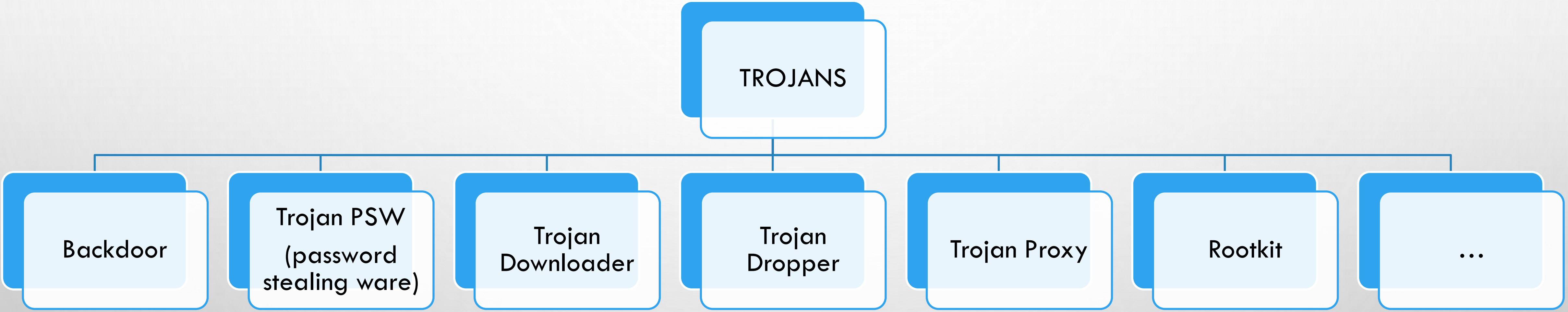
HEIMDAL

VIRUSES

- A COMPUTER VIRUS IS SOFTWARE USUALLY HIDDEN WITHIN ANOTHER SEEMINGLY HARMLESS PROGRAM THAT **CAN PRODUCE COPIES OF ITSELF** AND **INSERT THEM** INTO OTHER PROGRAMS OR FILES (INFECT THEM) AND THAT USUALLY PERFORMS A HARMFUL ACTION (SUCH AS DESTROYING DATA)
- VIRUS WRITERS USE **SOCIAL ENGINEERING** DECEPTIONS AND EXPLOIT DETAILED KNOWLEDGE OF **SECURITY VULNERABILITIES** TO INITIALLY INFECT SYSTEMS AND TO SPREAD THE VIRUS. THE VAST MAJORITY OF VIRUSES TARGET SYSTEMS RUNNING MICROSOFT WINDOWS, EMPLOYING A VARIETY OF MECHANISMS TO INFECT NEW HOSTS, AND OFTEN USING COMPLEX ANTI-DETECTION/STEALTH STRATEGIES TO EVADE ANTIVIRUS SOFTWARE.
- **MOTIVES FOR CREATING VIRUSES** CAN INCLUDE SEEKING PROFIT (E.G., WITH RANSOMWARE), DESIRE TO SEND A POLITICAL MESSAGE, PERSONAL AMUSEMENT, TO DEMONSTRATE THAT A VULNERABILITY EXISTS IN SOFTWARE, FOR SABOTAGE AND DENIAL OF SERVICE, OR SIMPLY BECAUSE THEY WISH TO EXPLORE CYBERSECURITY ISSUES, ARTIFICIAL LIFE AND EVOLUTIONARY ALGORITHMS.
- COMPUTER VIRUSES INFECT A VARIETY OF DIFFERENT SUBSYSTEMS ON THEIR HOST COMPUTERS AND SOFTWARE. ONE MANNER OF **CLASSIFYING VIRUSES IS TO ANALYZE PLACE OF INFECTION** - WHETHER THEY RESIDE IN BINARY EXECUTABLES (SUCH AS .EXE OR .COM FILES), DATA FILES (SUCH AS MICROSOFT WORD DOCUMENTS OR PDF FILES), OR IN THE BOOT SECTOR OF THE HOST'S HARD DRIVE (OR SOME COMBINATION OF ALL OF THESE)

TROJAN HORSES

- A **TROJAN HORSE,** OR **TROJAN,** IS ANY MALICIOUS COMPUTER PROGRAM WHICH **MISLEADS** USERS OF ITS TRUE INTENT.
- IT IS OFTEN DISGUISED AS LEGITIMATE SOFTWARE
- THE TERM IS DERIVED FROM THE ANCIENT GREEK STORY OF THE DECEPTIVE WOODEN HORSE THAT LED TO THE FALL OF THE CITY OF TROY.
- TROJANS CAN BE EMPLOYED BY CYBER-THIEVES AND HACKERS TRYING TO GAIN ACCESS TO USERS' SYSTEMS.
- USERS ARE TYPICALLY TRICKED BY SOME FORM OF **SOCIAL ENGINEERING** INTO LOADING AND EXECUTING TROJANS ON THEIR SYSTEMS.
- ONCE ACTIVATED, TROJANS CAN ENABLE CYBER-CRIMINALS TO SPY ON YOU, STEAL YOUR SENSITIVE DATA, AND GAIN BACKDOOR ACCESS TO YOUR SYSTEM.


TROJANS
Backdoor
Trojan PSW (password stealing ware)
Trojan Downloader
Trojan Dropper
Trojan Proxy
Rootkit
…

TROJANS

- A **BACKDOOR** GIVES MALICIOUS USERS REMOTE CONTROL OVER THE INFECTED COMPUTER. THEY ENABLE THE AUTHOR TO DO ANYTHING THEY WISH ON THE INFECTED COMPUTER – INCLUDING SENDING, RECEIVING, LAUNCHING AND DELETING FILES, DISPLAYING DATA AND REBOOTING THE COMPUTER. BACKDOOR TROJANS ARE OFTEN USED TO UNITE A GROUP OF VICTIM COMPUTERS TO FORM A BOTNET OR ZOMBIE NETWORK THAT CAN BE USED FOR CRIMINAL PURPOSES.
- **PSW TROJANS**: THIS FAMILY OF TROJANS STEALS PASSWORDS, NORMALLY SYSTEM PASSWORDS FROM VICTIM MACHINES. THEY SEARCH FOR SYSTEM FILES WHICH CONTAIN CONFIDENTIAL INFORMATION SUCH AS PASSWORDS AND INTERNET ACCESS TELEPHONE NUMBERS AND THEN SEND THIS INFORMATION TO AN EMAIL ADDRESS CODED INTO THE BODY OF THE TROJAN. IT WILL THEN BE RETRIEVED BY THE 'MASTER' OR USER OF THE ILLEGAL PROGRAM.
- A **TROJAN DOWNLOADER** IS A "DRIVE BY" MALWARE. A "DRIVE BY" DOWNLOADER IS INSTALLED ON A WEBSITE AND WHEN YOU ACCESS THIS WEBSITE YOUR COMPUTER WILL AUTOMATICALLY DOWNLOAD THE "TROJAN DOWNLOADER" THAT THEN IN TURN WILL DOWNLOAD TROJANS.

TROJANS

- **A ROOTKIT**: IS A CLANDESTINE COMPUTER PROGRAM DESIGNED TO PROVIDE CONTINUED PRIVILEGED ACCESS TO A COMPUTER WHILE ACTIVELY HIDING ITS PRESENCE.
- **A TROJAN DROPPER**: IS A PROGRAM THAT SAVES AND INSTALLS ANOTHER FILE (USUALLY A HARMFUL PROGRAM) ONTO A COMPUTER OR DEVICE. A TROJAN DROPPER AS A CARRIER OR DELIVERY VEHICLE FOR THE FILE THAT IS TO BE DROPPED, WHICH IS REFERRED TO AS THE DROPPER'S PAYLOAD. THE PAYLOAD IS USUALLY STORED IN THE DROPPER'S BODY AS A COMPRESSED FILE.
- **A TROJAN PROXY**: IS INTENDED FOR THE ATTACKER TO ACCESS VARIOUS INTERNET RESOURCES THROUGH A VICTIM COMPUTER. SUCH MALWARE IS USUALLY USED TO SEND SPAM.

TROJANS

- **A TROJAN-RANSOM** : CAN MODIFY DATA ON YOUR COMPUTER – SO THAT YOUR COMPUTER DOESN'T RUN CORRECTLY OR YOU CAN NO LONGER USE SPECIFIC DATA. THE CRIMINAL WILL ONLY RESTORE YOUR COMPUTER'S PERFORMANCE OR UNBLOCK YOUR DATA, AFTER YOU HAVE PAID THEM THE RANSOM MONEY THAT THEY DEMAND.
- **A TROJAN-SPY** : CAN SPY ON HOW YOU'RE USING YOUR COMPUTER – FOR EXAMPLE, BY TRACKING THE DATA YOU ENTER VIA YOUR KEYBOARD, TAKING SCREEN SHOTS OR GETTING A LIST
- **A TROJAN-IM :** STEALS YOUR LOGINS AND PASSWORDS FOR INSTANT MESSAGING PROGRAMS – SUCH AS ICQ, MSN MESSENGER, AOL INSTANT MESSENGER, YAHOO PAGER, SKYPE AND MANY MORE OF RUNNING APPLICATIONS.

EXAMPLE OF TROJAN - DARKCOMET

- **DARKCOMET** IS A REMOTE ACCESS TROJAN (RAT) DEVELOPED BY JEAN-PIERRE LESUEUR, AN INDEPENDENT PROGRAMMER AND COMPUTER SECURITY CODER FROM FRANCE.
- ALTHOUGH THE RAT WAS DEVELOPED BACK IN 2008, IT BEGAN TO PROLIFERATE AT THE START OF 2012. THE PROGRAM WAS DISCONTINUED, PARTIALLY DUE TO ITS USE IN THE SYRIAN CIVIL WAR TO MONITOR ACTIVISTS BUT ALSO DUE TO ITS AUTHOR'S FEAR OF BEING ARRESTED FOR UNNAMED REASONS.
- AS OF AUGUST 2018, THE PROGRAM'S DEVELOPMENT "HAS CEASED INDEFINITELY", AND DOWNLOADS ARE NO LONGER OFFERED ON ITS OFFICIAL WEBSITE.
- DARKCOMET ALLOWS A USER TO CONTROL THE SYSTEM WITH A GRAPHICAL USER INTERFACE (GUI). IT HAS MANY FEATURES WHICH ALLOWS A USER TO USE IT AS ADMINISTRATIVE REMOTE HELP TOOL; HOWEVER, DARKCOMET **HAS MANY FEATURES WHICH CAN BE USED MALICIOUSLY**.
- DARKCOMET IS COMMONLY USED TO SPY ON THE VICTIMS BY TAKING SCREEN CAPTURES, KEY-LOGGING, OR PASSWORD STEALING.

SOCIAL ENGINEERING

- **SOCIAL ENGINEERING**, IN THE CONTEXT OF INFORMATION SECURITY, REFERS TO PSYCHOLOGICAL MANIPULATION OF PEOPLE INTO PERFORMING ACTIONS OR DIVULGING (MAKE KNOWN) CONFIDENTIAL INFORMATION.
- EAMPLES: A USER MIGHT BE DECEIVED INTO EXECUTING AN E-MAIL ATTACHMENT CAMOUFLAGED AS NOT SUSPICIOUS, (E.G., A ROUTINE FORM TO BE FILLED IN), OR BY CLICKING ON SOME FAKE ADVERTISEMENT ON SOCIAL MEDIA OR ANYWHERE ELSE.

COMPUTER WORMS

- A WORM DOES NOT NEED A HOST PROGRAM IN ORDER TO RUN, SELF-REPLICATE AND PROPAGATE.
- ONCE A WORM HAS MADE ITS WAY ONTO YOUR SYSTEM, USUALLY VIA A NETWORK CONNECTION OR AS A DOWNLOADED FILE, IT CAN THEN MAKE MULTIPLE COPIES OF ITSELF AND SPREAD VIA THE NETWORK OR INTERNET CONNECTION INFECTING ANY INADEQUATELY-PROTECTED COMPUTERS AND SERVERS ON THE NETWORK.
- BECAUSE EACH SUBSEQUENT COPY OF A NETWORK WORM CAN ALSO SELF-REPLICATE, INFECTIONS CAN SPREAD VERY RAPIDLY VIA THE INTERNET AND COMPUTER NETWORKS.

COMPUTER WORMS

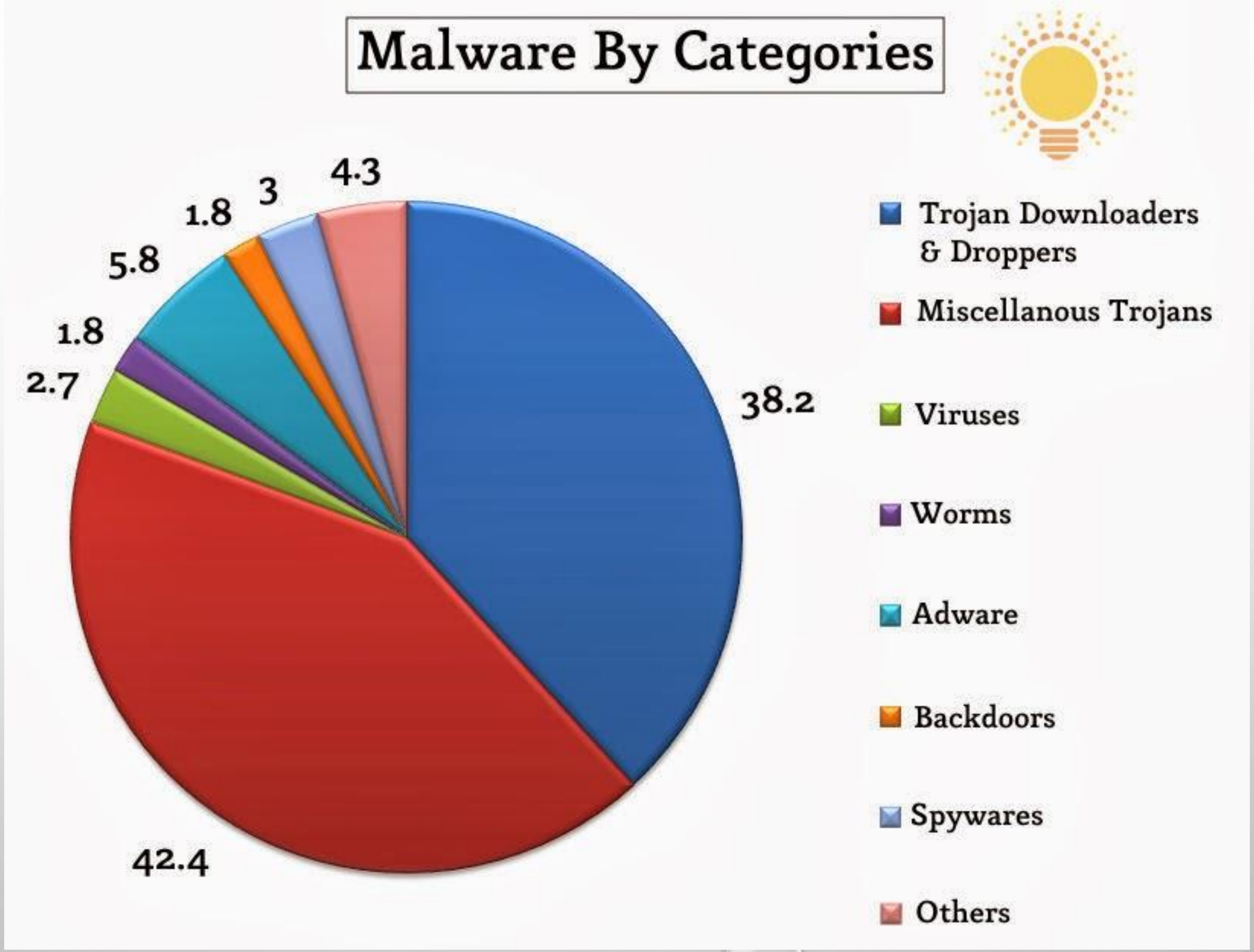
- MOST KNOWN COMPUTER WORMS ARE SPREAD IN ONE OF THE FOLLOWING WAYS:
  - ✓ FILES SENT AS EMAIL ATTACHMENTS
  - ✓ VIA A LINK TO A WEB OR FTP RESOURCE
  - ✓ VIA A LINK SENT IN AN ICQ OR IRC MESSAGE
  - ✓ VIA P2P (PEER-TO-PEER) FILE SHARING NETWORKS
  - ✓ SOME WORMS ARE SPREAD AS NETWORK PACKETS. THESE DIRECTLY PENETRATE THE COMPUTER MEMORY, AND THE WORM CODE IS THEN ACTIVATED.
- COMPUTER WORMS CAN EXPLOIT NETWORK CONFIGURATION ERRORS (FOR EXAMPLE, TO COPY THEMSELVES ONTO A FULLY ACCESSIBLE DISK) OR EXPLOIT LOOPHOLES IN OPERATING SYSTEM AND APPLICATION SECURITY. MANY WORMS WILL USE MORE THAN ONE METHOD IN ORDER TO SPREAD COPIES VIA NETWORKS.

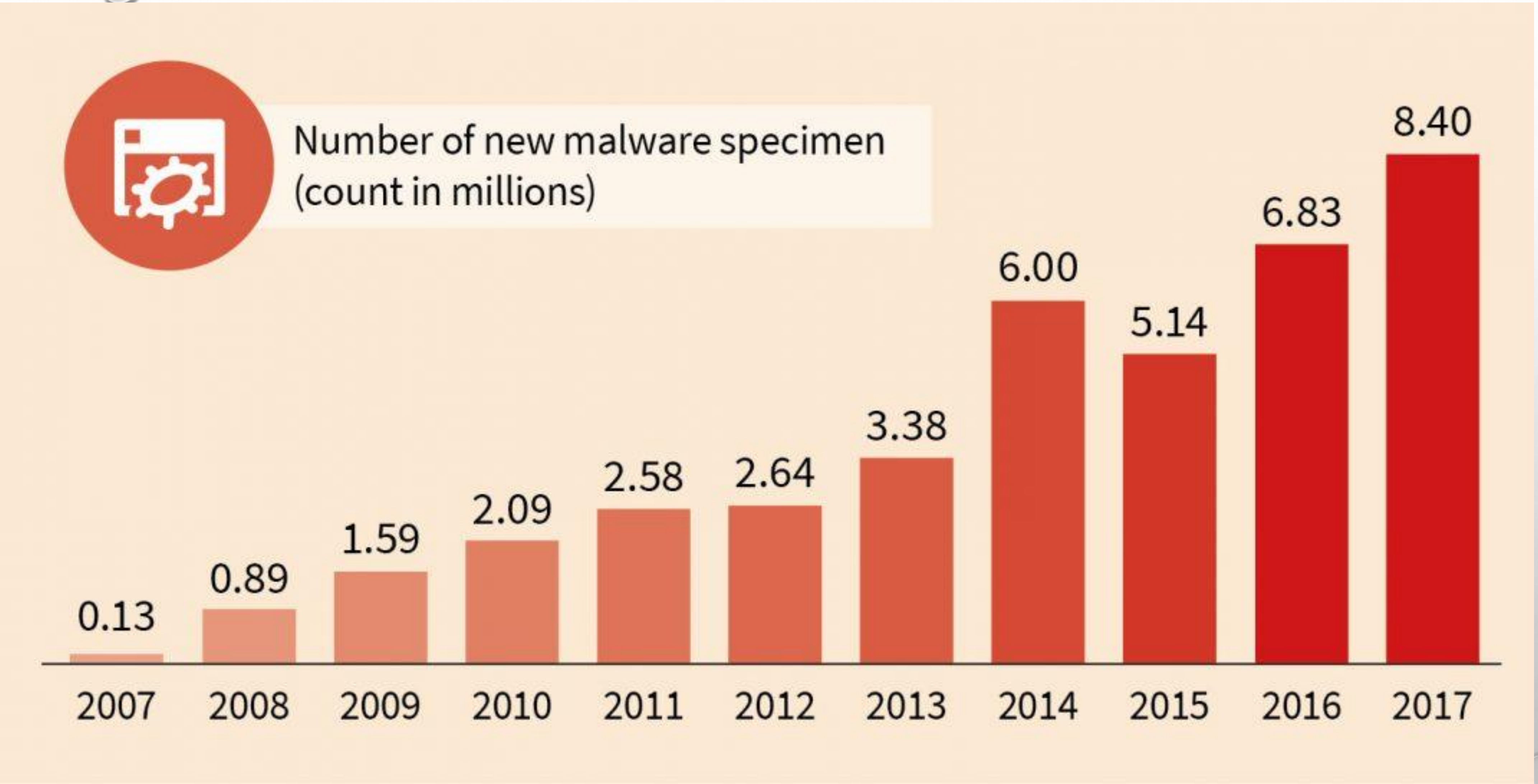
EXAMPLE OF A WORM ATTACK

- ON NOVEMBER 2, 1988, THE INTERNET WAS ATTACKED BY A SELF-REPLICATING PROGRAM CALLED A WORM THAT SPREAD WITHIN HOURS TO SOMEWHERE BETWEEN 2,000 AND 6,000 COMPUTER SYSTEMS—THE PRECISE NUMBER REMAINS UNCERTAIN. ONLY SYSTEMS (VAX AND SUN 3) RUNNING CERTAIN TYPES OF UNIX (VARIANTS OF BSD 4) WERE AFFECTED.
- THE INTERNET WORM WAS DEVELOPED AND LAUNCHED BY ROBERT T. MORRIS, JR., WHO AT THE TIME WAS A GRADUATE STUDENT AT CORNELL UNIVERSITY. MORRIS EXPLOITED SECURITY WEAKNESSES (IN THE FINGERD, RHOSTS, AND SENDMAIL PROGRAMS) IN THE AFFECTED VERSIONS OF UNIX. THE WORM PROGRAM ITSELF DID NOT CAUSE ANY DAMAGE TO THE SYSTEMS THAT IT ATTACKED
- ITS RAPID PROLIFERATION AND THE ENSUING CONFUSION CAUSED SEVERE DEGRADATION IN SERVICE AND SHUT DOWN SOME SYSTEMS AND NETWORK CONNECTIONS THROUGHOUT THE INTERNET FOR TWO OR THREE DAYS, AFFECTING SITES THAT WERE NOT DIRECTLY ATTACKED.

EXPLOIT

- AN **EXPLOIT** (FROM THE ENGLISH VERB *TO EXPLOIT*, MEANING "TO USE SOMETHING TO ONE’S OWN ADVANTAGE") IS A PIECE OF SOFTWARE, A CHUNK OF DATA, OR A SEQUENCE OF COMMANDS THAT TAKES ADVANTAGE OF A BUG OR VULNERABILITY TO CAUSE UNINTENDED OR UNANTICIPATED BEHAVIOR TO OCCUR ON COMPUTER SOFTWARE, HARDWARE, OR SOMETHING ELECTRONIC (USUALLY COMPUTERIZED).
- SUCH BEHAVIOR FREQUENTLY INCLUDES THINGS LIKE GAINING CONTROL OF A COMPUTER SYSTEM, ALLOWING PRIVILEGE ESCALATION, OR A DENIAL-OF-SERVICE (DOS OR RELATED DDOS) ATTACK.
- AN **EXPLOIT KIT** IS SIMPLY A COLLECTION OF EXPLOITS, WHICH IS A SIMPLE ONE-IN-ALL TOOL FOR MANAGING A VARIETY OF EXPLOITS ALTOGETHER. EXPLOIT KITS ACT AS A KIND OF REPOSITORY, AND MAKE IT EASY FOR USERS WITHOUT MUCH TECHNICAL KNOWLEDGE TO USE EXPLOITS.


Malware By Categories
4.3
3
1.8
5.8
1.8
2.7
38.2
42.4
🟦 Trojan Downloaders & Droppers
🟥 Miscellanous Trojans
🟩 Viruses
🟪 Worms
🟦 Adware
🟧 Backdoors
🟦 Spywares
🟥 Others


Number of new malware specimen
(count in millions)
0.13
0.89
1.59
2.09
2.58
2.64
3.38
6.00
5.14
6.83
8.40
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

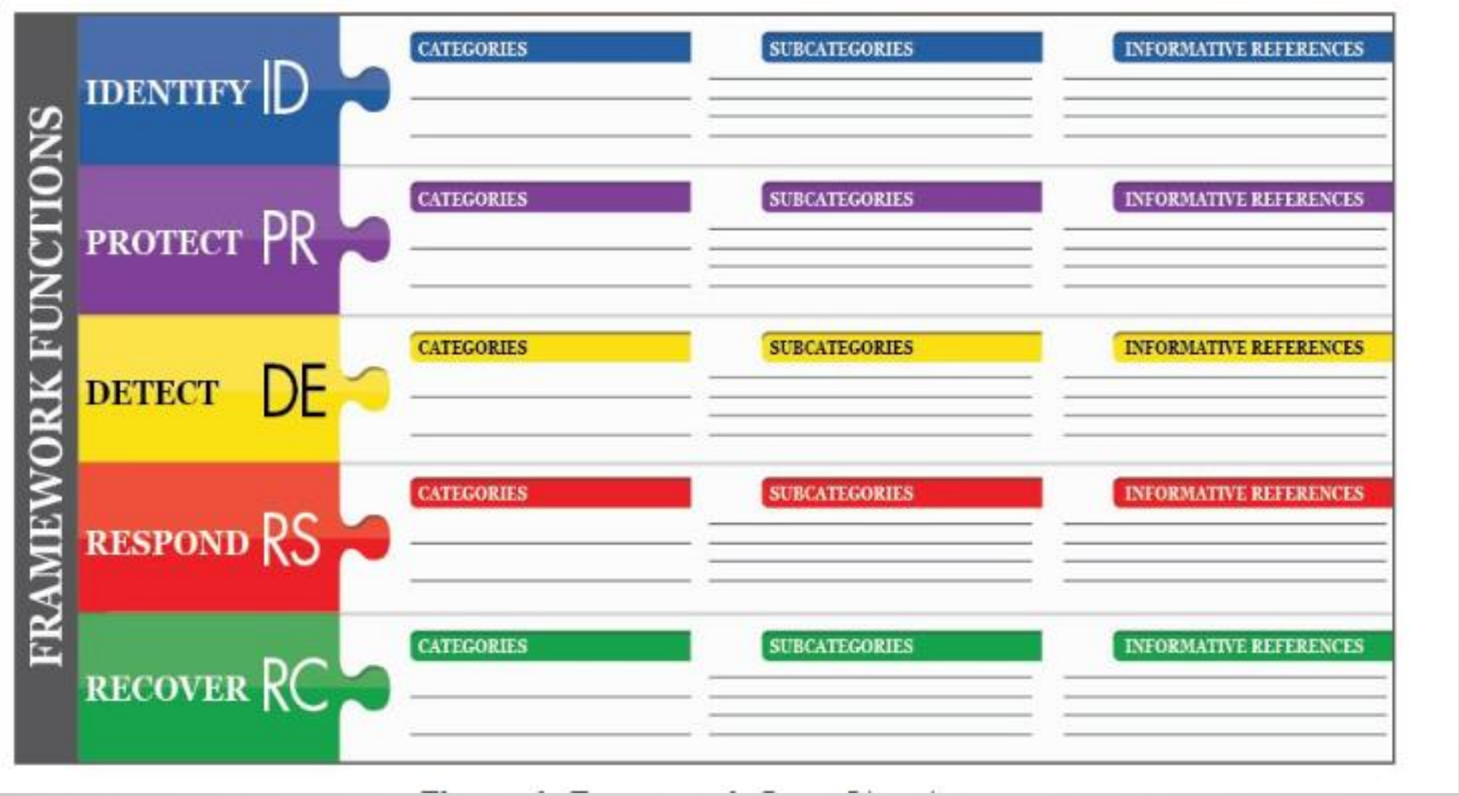
World Wide Web
VIRUS
World Wide Web
TROJAN
World Wide Web
ROOTKIT

5 MAIN ASPECTS OF CYBERSECURITY

U.S. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) FRAMEWORK ON CYBERSECURITY IDENTIFIES 5 ASPECTS OF SECURING ELECTRONIC INFORMATION:

- IDENTIFY THREATS
- PROTECT INFORMATION
- DETECT ATTACKS AND INTRUSIONS
- RESPOND TO ATTACKS AND INTRUSIONS
- RECOVER DATABASE AND INFORMATION SECURITY AND REBUILD DEFENSES AGAINST INTRUSION

FRAMEWORK CORE STRUCTURE



IDENTIFY

- **IDENTIFY** – DEVELOP AN ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK TO SYSTEMS, PEOPLE, ASSETS, DATA, AND CAPABILITIES.
- THE ACTIVITIES IN THE IDENTIFY FUNCTION ARE FOUNDATIONAL FOR EFFECTIVE USE OF THE FRAMEWORK.
- UNDERSTANDING THE **BUSINESS CONTEXT**, THE **RESOURCES** THAT SUPPORT CRITICAL FUNCTIONS, AND THE RELATED CYBERSECURITY **RISKS** ENABLES AN ORGANIZATION TO FOCUS AND PRIORITIZE ITS EFFORTS, CONSISTENT WITH ITS **RISK MANAGEMENT STRATEGY** AND **BUSINESS NEEDS**.
- EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: ASSET MANAGEMENT; BUSINESS ENVIRONMENT; GOVERNANCE; RISK ASSESSMENT; AND RISK MANAGEMENT STRATEGY.

PROTECT

- **PROTECT** – DEVELOP AND IMPLEMENT APPROPRIATE SAFEGUARDS TO ENSURE DELIVERY OF CRITICAL SERVICES.
- THE PROTECT FUNCTION SUPPORTS THE ABILITY TO LIMIT OR CONTAIN THE IMPACT OF A POTENTIAL CYBERSECURITY EVENT.
- EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: IDENTITY MANAGEMENT AND ACCESS CONTROL; AWARENESS AND TRAINING; DATA SECURITY; INFORMATION PROTECTION PROCESSES AND PROCEDURES; MAINTENANCE; AND PROTECTIVE TECHNOLOGY.

DETECT

- **DETECT** – DEVELOP AND IMPLEMENT APPROPRIATE ACTIVITIES TO IDENTIFY THE OCCURRENCE OF A CYBERSECURITY EVENT.
- THE DETECT FUNCTION ENABLES TIMELY DISCOVERY OF CYBERSECURITY EVENTS. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: *ANOMALIES AND EVENTS; SECURITY CONTINUOUS MONITORING; AND DETECTION PROCESSES*

RESPOND

- **RESPOND** – DEVELOP AND IMPLEMENT APPROPRIATE ACTIVITIES TO TAKE ACTION REGARDING A DETECTED CYBERSECURITY INCIDENT.
- THE RESPOND FUNCTION SUPPORTS THE ABILITY TO CONTAIN THE IMPACT OF A POTENTIAL CYBERSECURITY INCIDENT. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: RESPONSE PLANNING; COMMUNICATIONS; ANALYSIS; MITIGATION; AND IMPROVEMENTS.

RECOVER

- **RECOVER** – DEVELOP AND IMPLEMENT APPROPRIATE ACTIVITIES TO MAINTAIN PLANS FOR RESILIENCE AND TO RESTORE ANY CAPABILITIES OR SERVICES THAT WERE IMPAIRED DUE TO A CYBERSECURITY INCIDENT.
- THE RECOVER FUNCTION SUPPORTS TIMELY RECOVERY TO NORMAL OPERATIONS TO REDUCE THE IMPACT FROM A CYBERSECURITY INCIDENT. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: RECOVERY PLANNING; IMPROVEMENTS; AND COMMUNICATIONS.

SYSTEM APPROACH TO COMPUTER SECURITY

VARIOUS TYPE MEANS MUST BE USED:

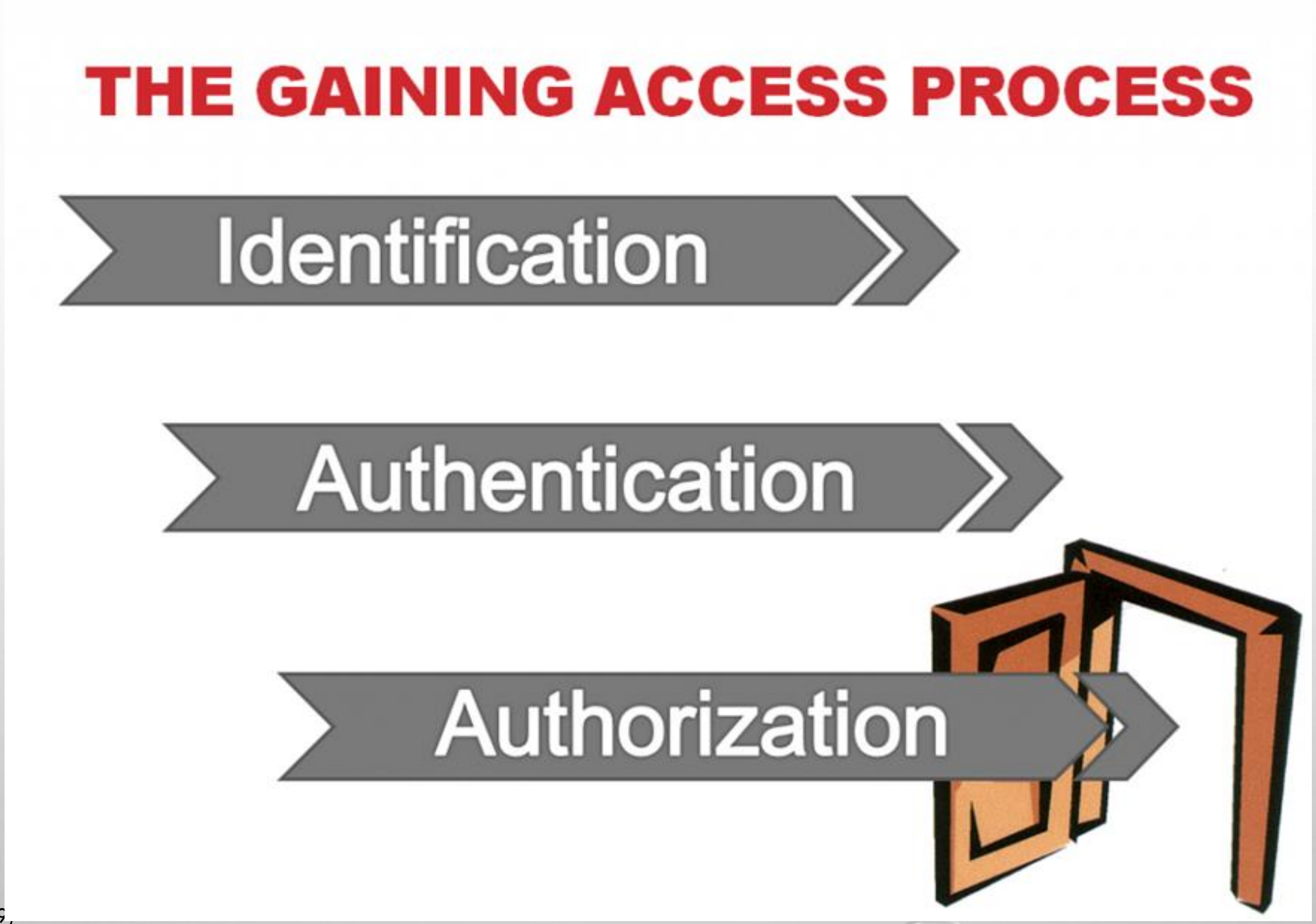
- MORAL ETHICAL
- LEGISLATIVE (LAW № 273)
- ADMINISTRATIVE
- PSYCHOLOGICAL (AGAINST SOCIAL ENGINEERING)
- PHYSICAL
- TECHNICAL

SECURITY POLICY

SECURITY POLICY IS A SET OF RULES, REGULATIONS, AND PRACTICES GOVERNING THE PROCESS OF PROTECTING (MAKING SECURE) A COMPUTER SYSTEM

MAIN FUNCTIONALITY OF THE OS SECURITY SUBSYSTEM

- ➢ SECURITY POLICY MANAGEMENT
- ➢ IDENTITY MANAGEMENT (IDENTIFICATION, AUTHENTICATION, AUTHORIZATION)
- ➢ ACCESS CONTROL
- ➢ AUDITING
- ➢ CRYPTOGRAPHIC FUNCTIONS (ENCRYPTING)
- ➢ MALWARE PROTECTION



THE GAINING ACCESS PROCESS

Identification

Authentication

Authorization

REGISTRATION

REGISTRATION IN A COMPUTER SYSTEM CONSISTS OF 3 FOLLOWING STAGES:

- IDENTIFICATION – DELIVERING USER'S DATA IN THE NECESSARY FORM (LOGIN+PASSWORD, FINGERPRINT, OR SOMETHING ELSE DICTATED BY THE SAFETY SYSTEM)
- AUTHENTICATION – CHECKING USER'S AUTHENTICITY (COMPARING DATA DELIVERED BY USER IN THE PREVIOUS STAGE WITH DATA STORED IN THE COMPUTER SYSTEM)
- AUTHORIZATION (IN CASE OF THE PREVIOUS STAGES WERE A SUCCESS) – PROVIDING THE USER WITH RIGHTS AND PRIVILEGES FOR THEIR WORK IN THE SYSTEM

WINDOWS SECURITY SUBSYSTEM

1. SECURITY POLICY MANAGEMENT

SECURITY POLICY MANAGEMENT

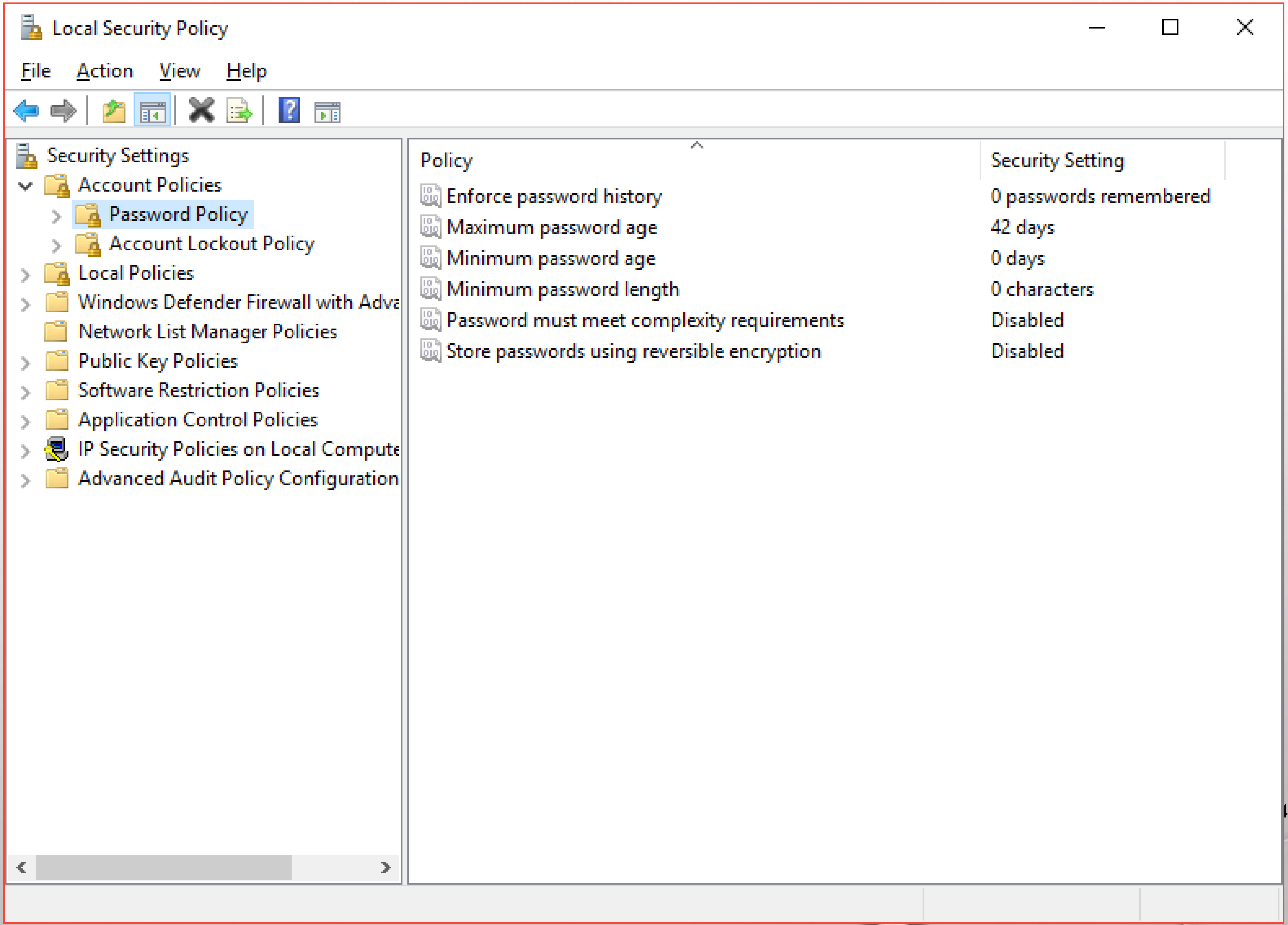
- THERE ARE SEVERAL INSTRUMENTS TO CONFIGURE SECURITY POLICY:
  - ✓ **THE LOCAL SECURITY POLICY SNAP-IN** (SECPOL.MSC, CONTROL PANEL\ADMINISTRATIVE TOOLS\LOCAL SECURITY POLICY) - MMC SNAP-IN DESIGNED TO MANAGE ONLY SECURITY POLICY SETTINGS
  - ✓ **SECURITY EDITOR COMMAND LINE TOOL** (SECEDIT.EXE) - CONFIGURES AND ANALYZES SYSTEM SECURITY BY COMPARING YOUR CURRENT CONFIGURATION TO SPECIFIED SECURITY TEMPLATES
  - ✓ **SECURITY CONFIGURATION MANAGER TOOL –** THIS TOOL SET ALLOWS YOU TO CREATE, APPLY, AND EDIT THE SECURITY FOR YOUR LOCAL DEVICE, ORGANIZATIONAL UNIT, OR DOMAIN.
  - ✓ **GROUP POLICY** (GPEDIT.MSC) - THE GROUP POLICY MANAGEMENT CONSOLE USES THE GROUP POLICY OBJECT EDITOR TO EXPOSE THE LOCAL SECURITY OPTIONS, WHICH CAN THEN BE INCORPORATED INTO GROUP POLICY OBJECTS FOR DISTRIBUTION THROUGHOUT THE DOMAIN. THE LOCAL GROUP POLICY EDITOR PERFORMS SIMILAR FUNCTIONS ON THE LOCAL DEVICE.
  - ✓ **SECURITY COMPLIANCE MANAGER -** IS A DOWNLOADABLE TOOL THAT HELPS YOU PLAN, DEPLOY, OPERATE, AND MANAGE YOUR SECURITY BASELINES FOR WINDOWS CLIENT AND SERVER OPERATING SYSTEMS, AND FOR MICROSOFT APPLICATIONS

USING THE LOCAL SECURITY POLICY SNAP-IN

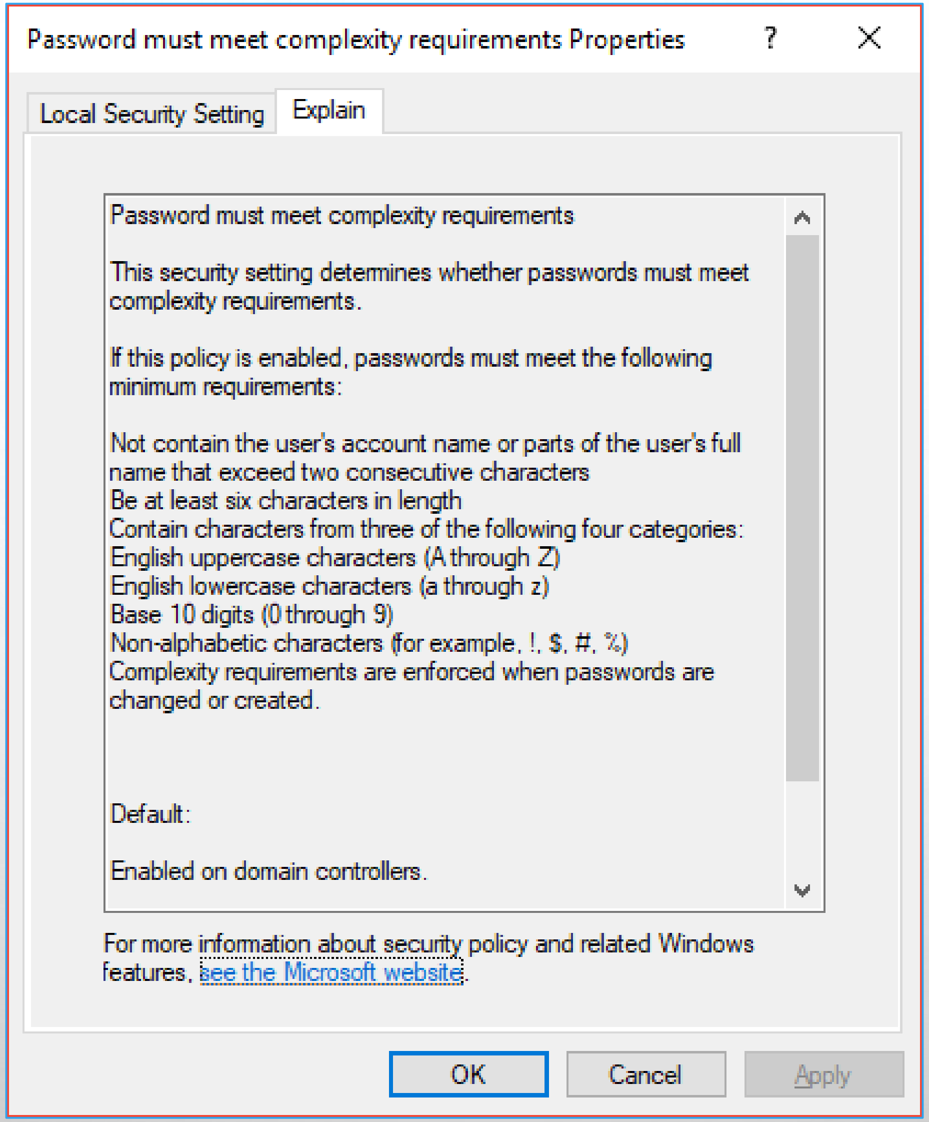
- THE LOCAL SECURITY POLICY SNAP-IN (SECPOL.MSC) RESTRICTS THE VIEW OF LOCAL POLICY OBJECTS TO THE FOLLOWING POLICIES AND FEATURES:
  - ✓ ACCOUNT POLICIES
  - ✓ LOCAL POLICIES
  - ✓ WINDOWS FIREWALL WITH ADVANCED SECURITY
  - ✓ NETWORK LIST MANAGER POLICIES
  - ✓ PUBLIC KEY POLICIES
  - ✓ SOFTWARE RESTRICTION POLICIES
  - ✓ APPLICATION CONTROL POLICIES
  - ✓ IP SECURITY POLICIES ON LOCAL COMPUTER
  - ✓ ADVANCED AUDIT POLICY CONFIGURATION
- POLICIES SET LOCALLY MIGHT BE OVERWRITTEN IF THE COMPUTER IS JOINED TO THE DOMAIN.
- THE LOCAL SECURITY POLICY SNAP-IN IS PART OF THE SECURITY CONFIGURATION MANAGER TOOL SET.

ACCOUNT POLICIES \ PASSWORD POLICY

1. If a password policy is set for the domain (in the domain controller), it overlaps the local ones
2. If it is necessary to make empty passwords impossible, it is necessary to set “Minimum password length” at least to 1 character
3. Maximum password length is set to 14 (other characters will be ignored)
4. The setting “Password must meet …” (see the next slide)


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled



Password must meet complexity requirements

This security setting determines whether passwords must meet complexity requirements.

If this policy is enabled, passwords must meet the following minimum requirements:

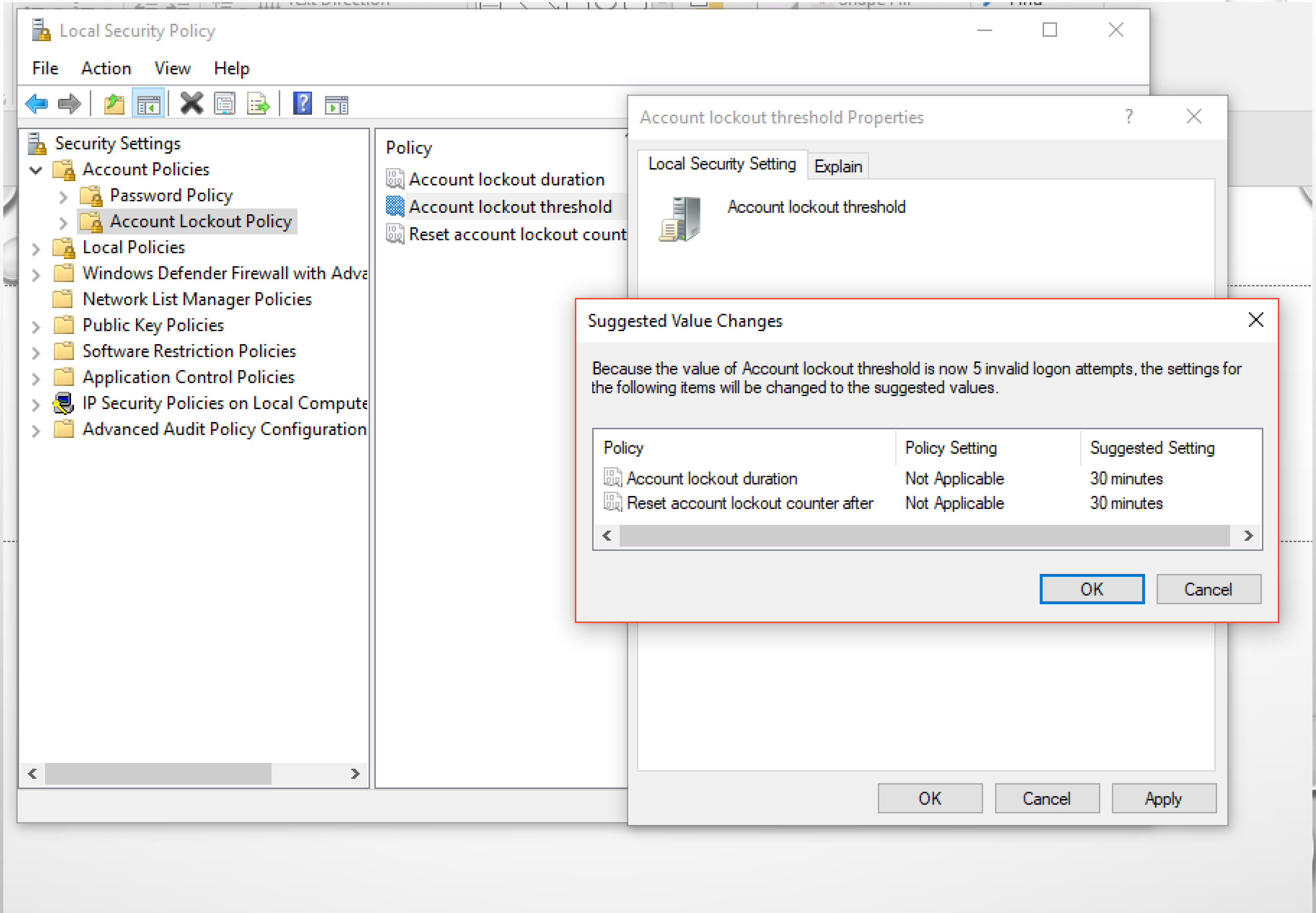
Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
Be at least six characters in length
Contain characters from three of the following four categories:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)
Complexity requirements are enforced when passwords are changed or created.

Default:

Enabled on domain controllers.

For more information about security policy and related Windows features, see the Microsoft website.

ACCOUNT POLICIES \ ACCOUNT LOCKOUT POLICY



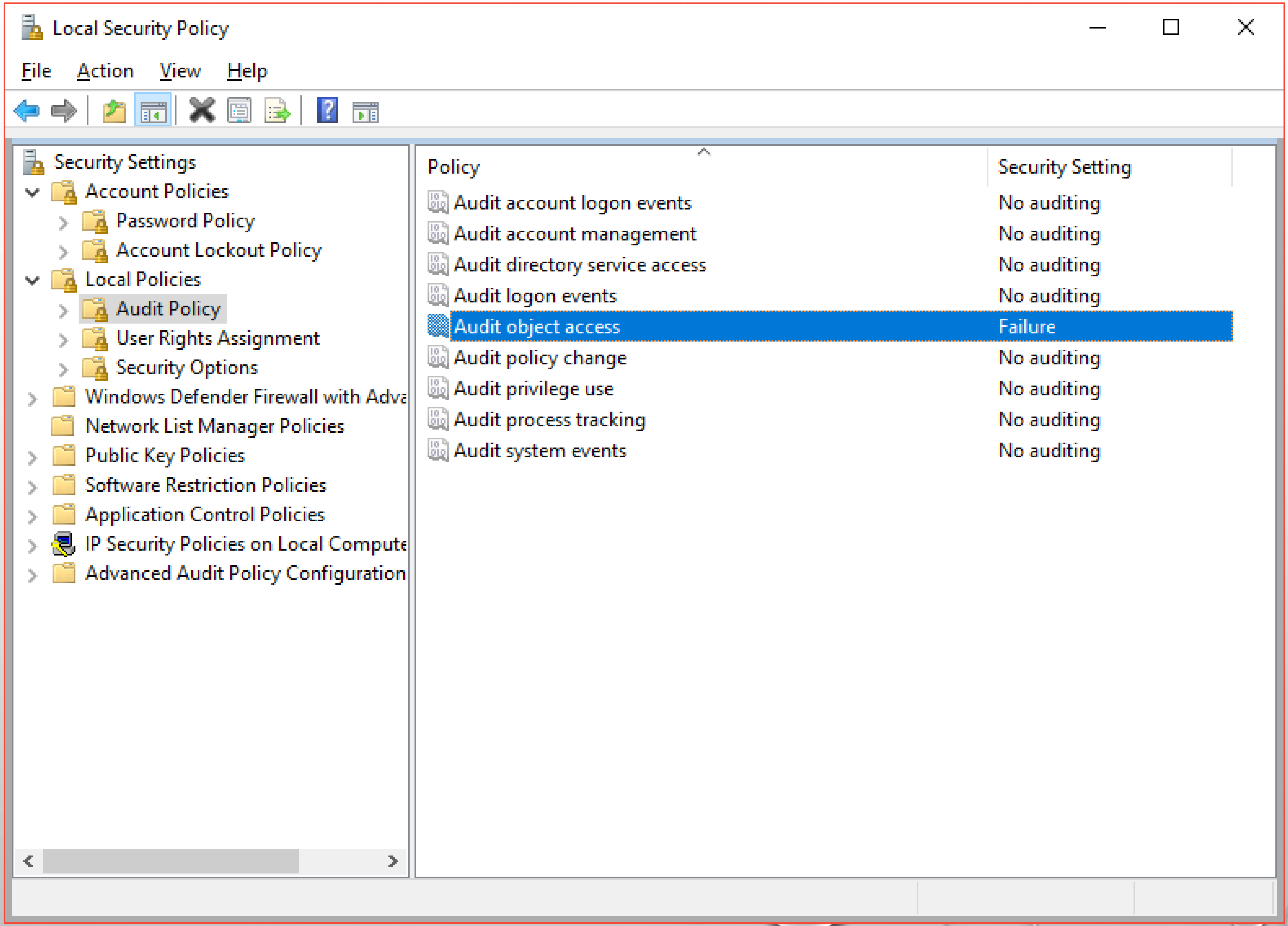
Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Account lockout duration
Account lockout threshold
Reset account lockout count
Account lockout threshold Properties
Local Security Setting
Explain
Account lockout threshold
OK
Cancel
Apply

Suggested Value Changes

Because the value of Account lockout threshold is now 5 invalid logon attempts, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Applicable	30 minutes
Reset account lockout counter after	Not Applicable	30 minutes

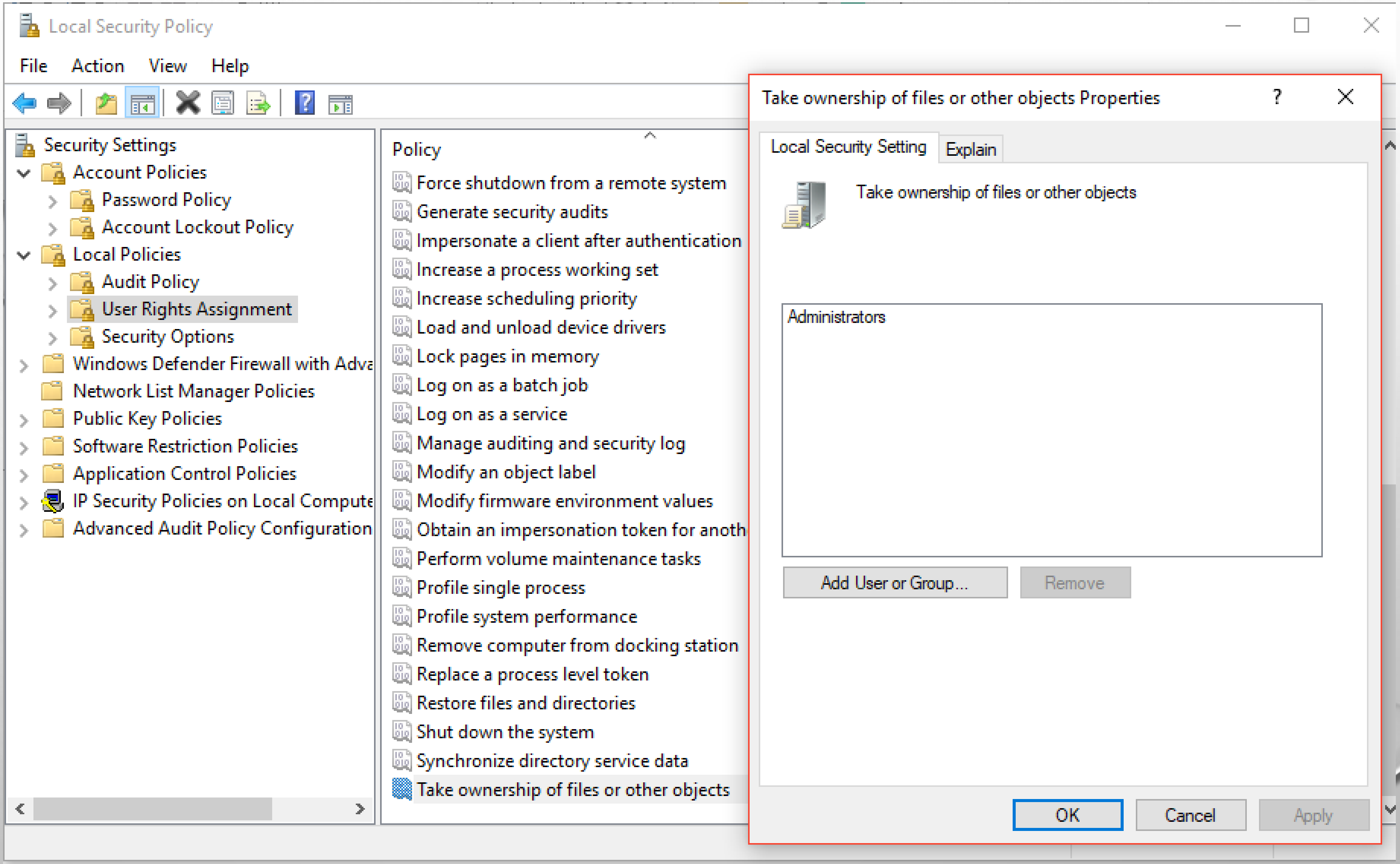
LOCAL POLICIES \ AUDIT POLICY



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	Failure
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

LOCAL POLICIES \ USER RIGHTS ASSIGNMENT



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy

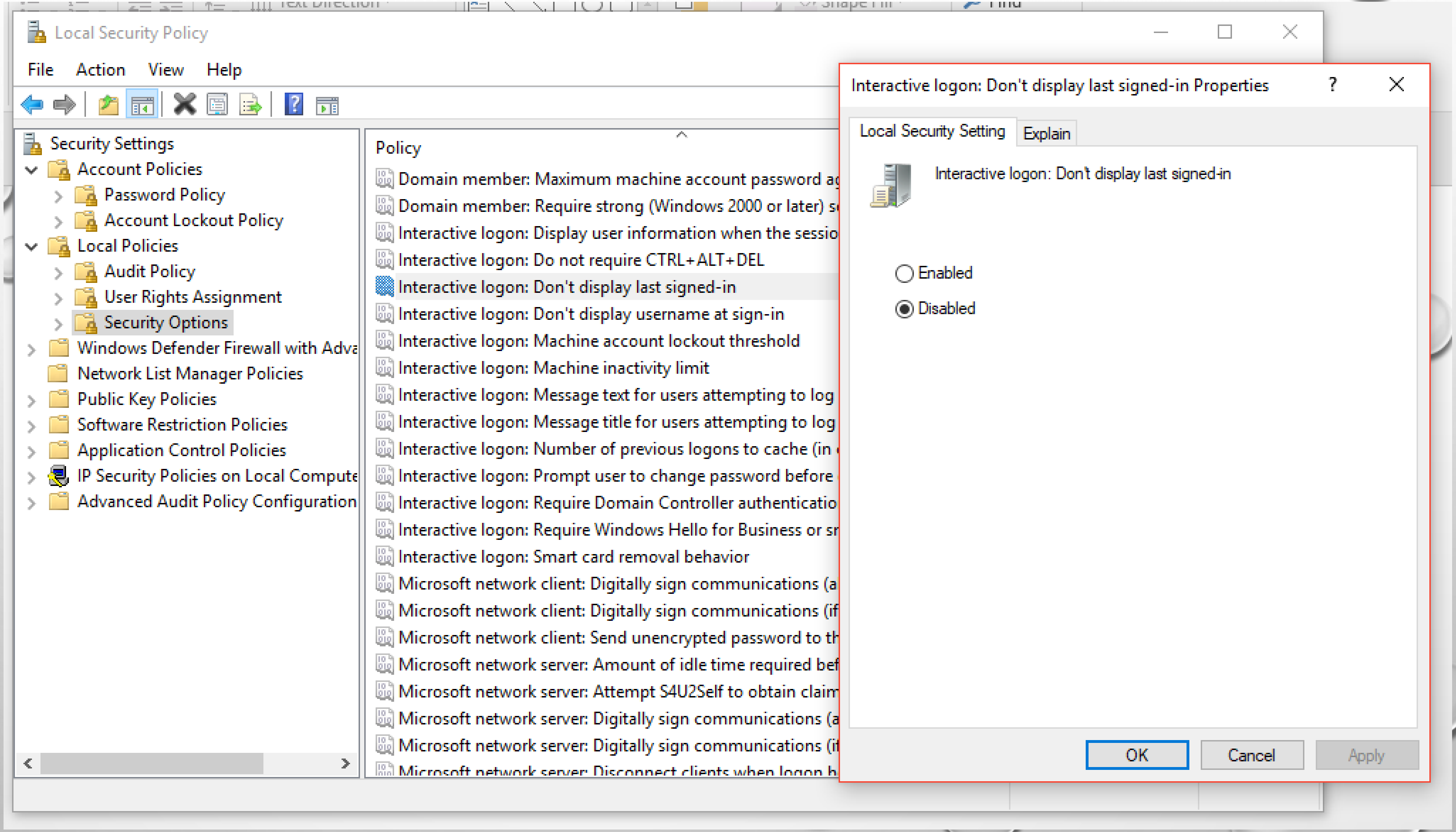
- Force shutdown from a remote system
- Generate security audits
- Impersonate a client after authentication
- Increase a process working set
- Increase scheduling priority
- Load and unload device drivers
- Lock pages in memory
- Log on as a batch job
- Log on as a service
- Manage auditing and security log
- Modify an object label
- Modify firmware environment values
- Obtain an impersonation token for anoth
- Perform volume maintenance tasks
- Profile single process
- Profile system performance
- Remove computer from docking station
- Replace a process level token
- Restore files and directories
- Shut down the system
- Synchronize directory service data
- Take ownership of files or other objects

Take ownership of files or other objects Properties

Take ownership of files or other objects

Administrators

LOCAL POLICIES \ SECURITY OPTIONS



Local Security Policy

File Action View Help

- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy

Domain member: Maximum machine account password ag
Domain member: Require strong (Windows 2000 or later) s
Interactive logon: Display user information when the sessio
Interactive logon: Do not require CTRL+ALT+DEL
Interactive logon: Don't display last signed-in
Interactive logon: Don't display username at sign-in
Interactive logon: Machine account lockout threshold
Interactive logon: Machine inactivity limit
Interactive logon: Message text for users attempting to log
Interactive logon: Message title for users attempting to log
Interactive logon: Number of previous logons to cache (in
Interactive logon: Prompt user to change password before
Interactive logon: Require Domain Controller authenticatio
Interactive logon: Require Windows Hello for Business or sr
Interactive logon: Smart card removal behavior
Microsoft network client: Digitally sign communications (a
Microsoft network client: Digitally sign communications (if
Microsoft network client: Send unencrypted password to th
Microsoft network server: Amount of idle time required bef
Microsoft network server: Attempt S4U2Self to obtain claim
Microsoft network server: Digitally sign communications (a
Microsoft network server: Digitally sign communications (if
Microsoft network server: Disconnect clients when logon h

Interactive logon: Don't display last signed-in Properties

Local Security Setting | Explain

Interactive logon: Don't display last signed-in

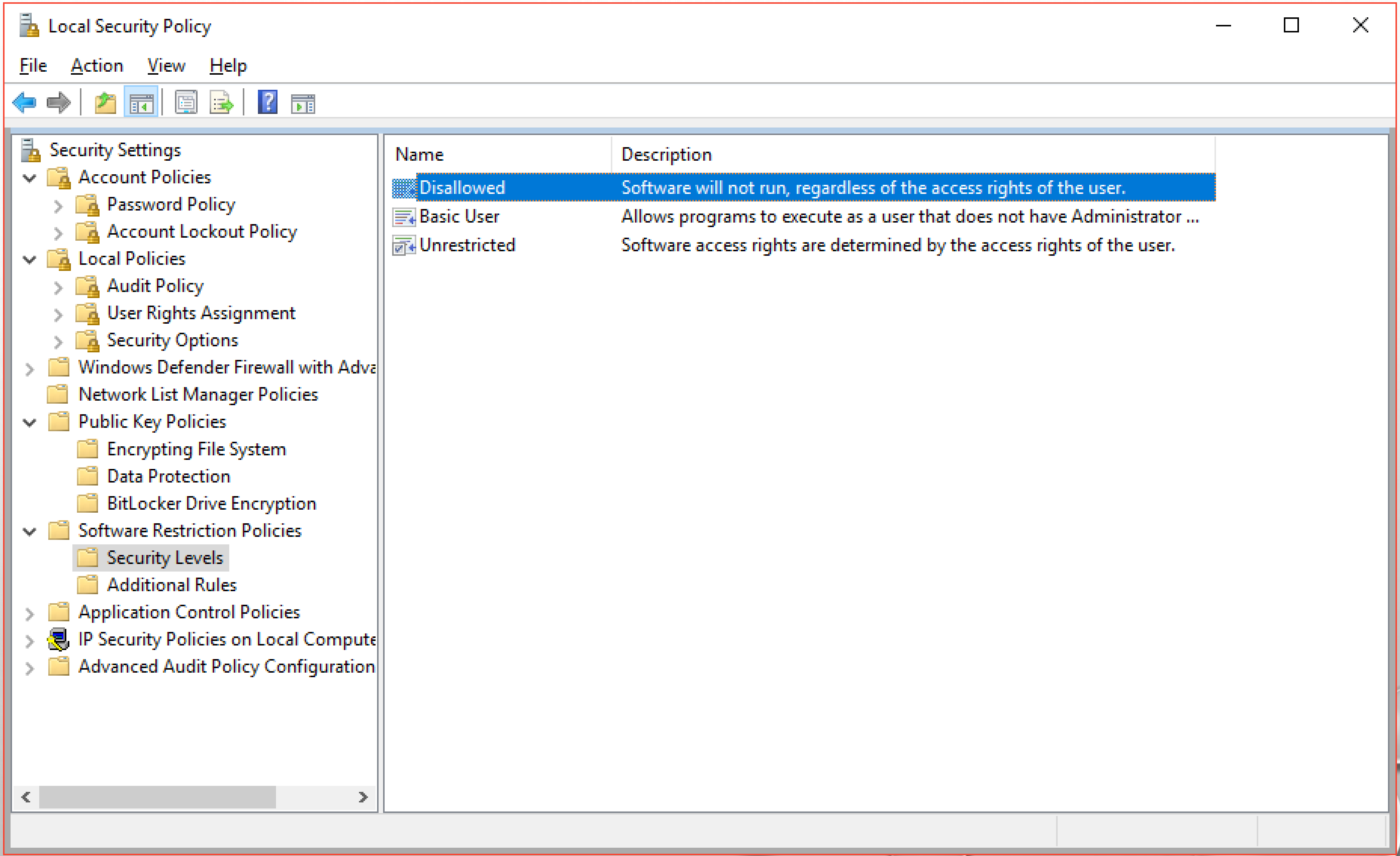
○ Enabled
● Disabled

OK Cancel Apply

Zvereva O. (OS - Lecture 9)

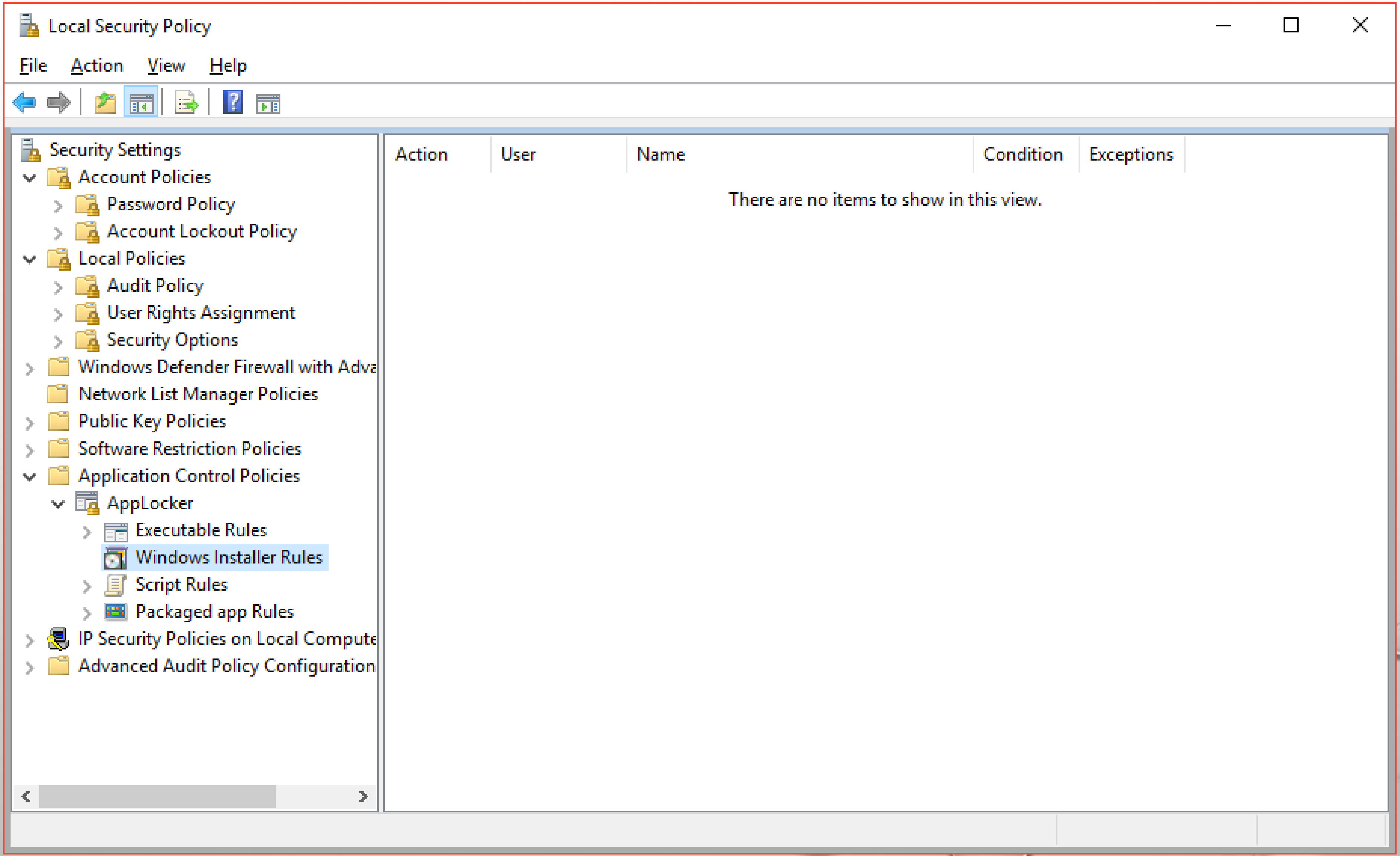
SOFTWARE RESTRICTION POLICIES

You can restrict running apps from the places other than specified here (protect from malware which can start from infected flash drive, for example).



Name	Description
Disallowed	Software will not run, regardless of the access rights of the user.
Basic User	Allows programs to execute as a user that does not have Administrator ...
Unrestricted	Software access rights are determined by the access rights of the user.

APPLICATION CONTROL POLICIES



Action	User	Name	Condition	Exceptions

There are no items to show in this view.