ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
імені ГЕРОЇВ КРУТ

viti.edu.ua

Тема 1: Теоретичні основи побудови систем виявлення та реагування на кіберінциденти

Заняття 4: Порядок дій зловмисника при підготовці та реалізації кібератаки

Викладач кафедри № 33
старший лейтенант Цьопко Інна Едуардівна

КИЇВ-2021

1. Етапи реалізації кібератаки згідно Lockheed Martin Kill Chain.

2. Структура MITRE ATT&CK Matrix for Enterprise.

1. Етапи реалізації кібератаки згідно Lockheed Martin Kill Chain.

Сучасні спрямовані атаки - це цілий комплекс заходів, в результаті чого злом і зараження мережі не відбуваються «раптом з нічого». Цьому передує цілий набір дій.

Модель Cyber-Kill Chain і її розширена версія якраз і **описують всі етапи атаки**.

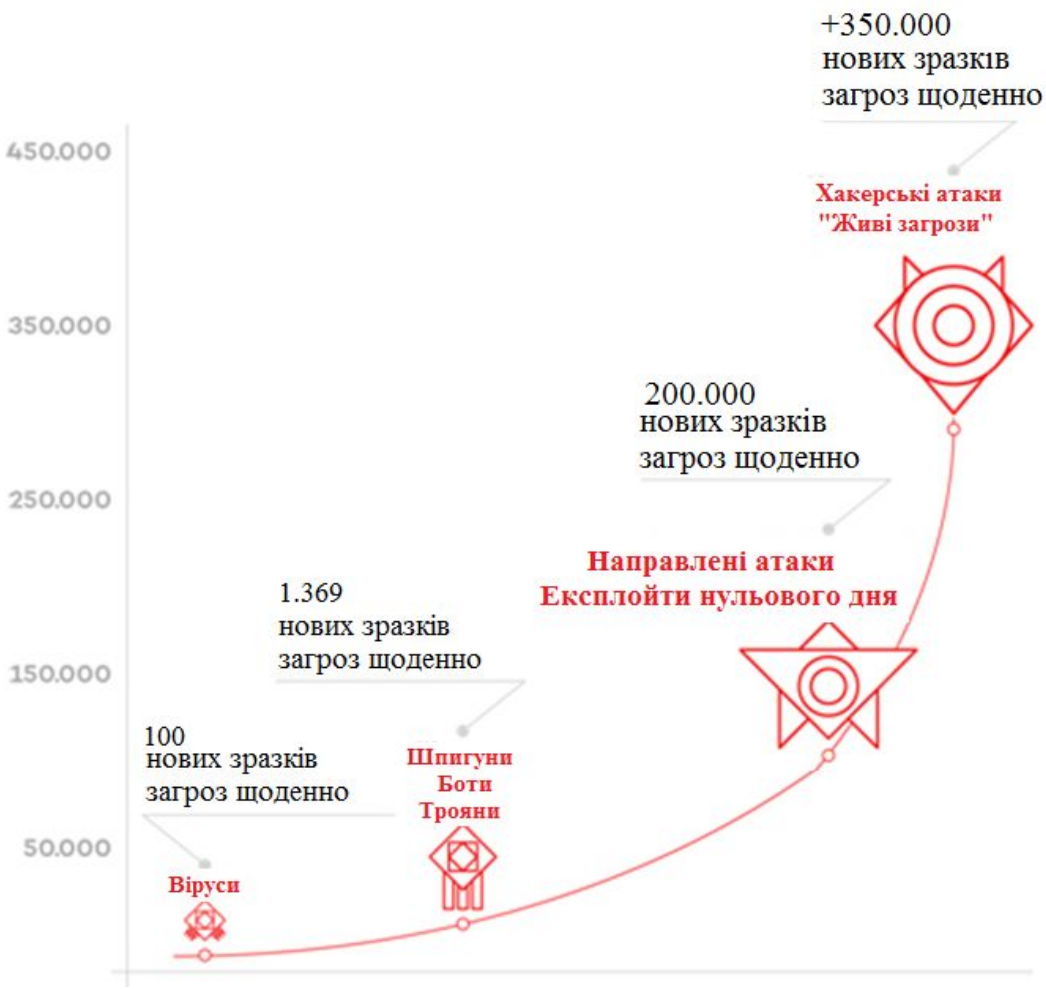
Мінливий ландшафт загроз, їх частота появи, складність і цільовий характер атак вимагає еволюції діючих правил безпеки з переходом до поєднання технологій запобігання, виявлення і реагування на кібератаки.

Найскладніше - це зупинити невідомі атаки , які спеціально створені з метою обходу наявної захисту за рахунок зміни сигнатур і шаблонів поведінки.

Існує 3 основні чинники успіху зловмисників.

Фактор 1. Еволюція атак

Шкідливе ПО стає все більш і більш витонченим. Також розвиваються і самі техніки виконання атак: тепер все частіше мета вибирається не випадково. Атаки стали спрямованими, скоординованими і з використанням різних векторів. Крім того, фінансова мотивація відіграє істотну роль.



Існує 3 основні чинники успіху зловмисників.

Фактор 2. Нове цифрове життя

Наша сучасна цифрова поведінка відбувається в умовах складного, взаємопов'язаного і гіпердинамічного оточення.

Зараз периметр знаходиться там, де користувач.

Складність IT-систем підвищує вразливість перед лицем кіберзагроз

Існує 3 основні чинники успіху зловмисників.

Фактор 3. Традиційний підхід до захисту

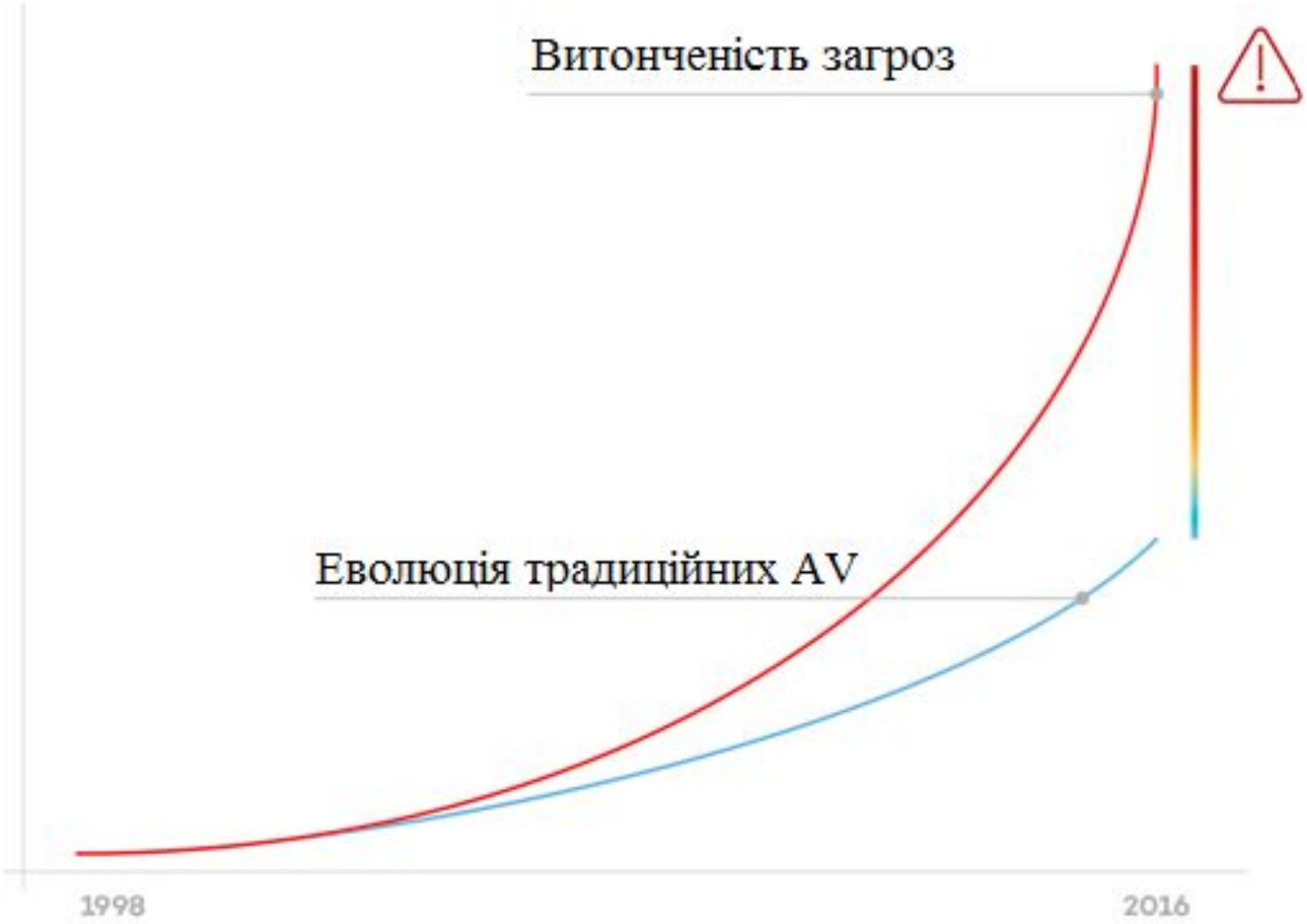
Не випадково ми все частіше чуємо про рішення захисту «наступного покоління». Дійсно, в переважній більшості випадків захист відбувається на основі традиційних рішень:

• на основі сигнатурних файлів. Їх розмір стає величезним, тому що зростає кількість шкідливих програм.

• виявляють переважно відомі загрози. Оскільки загрози стали більш витонченими, то компаніям необхідно виділяти все більше часу і ресурсів на дослідження нових атак.

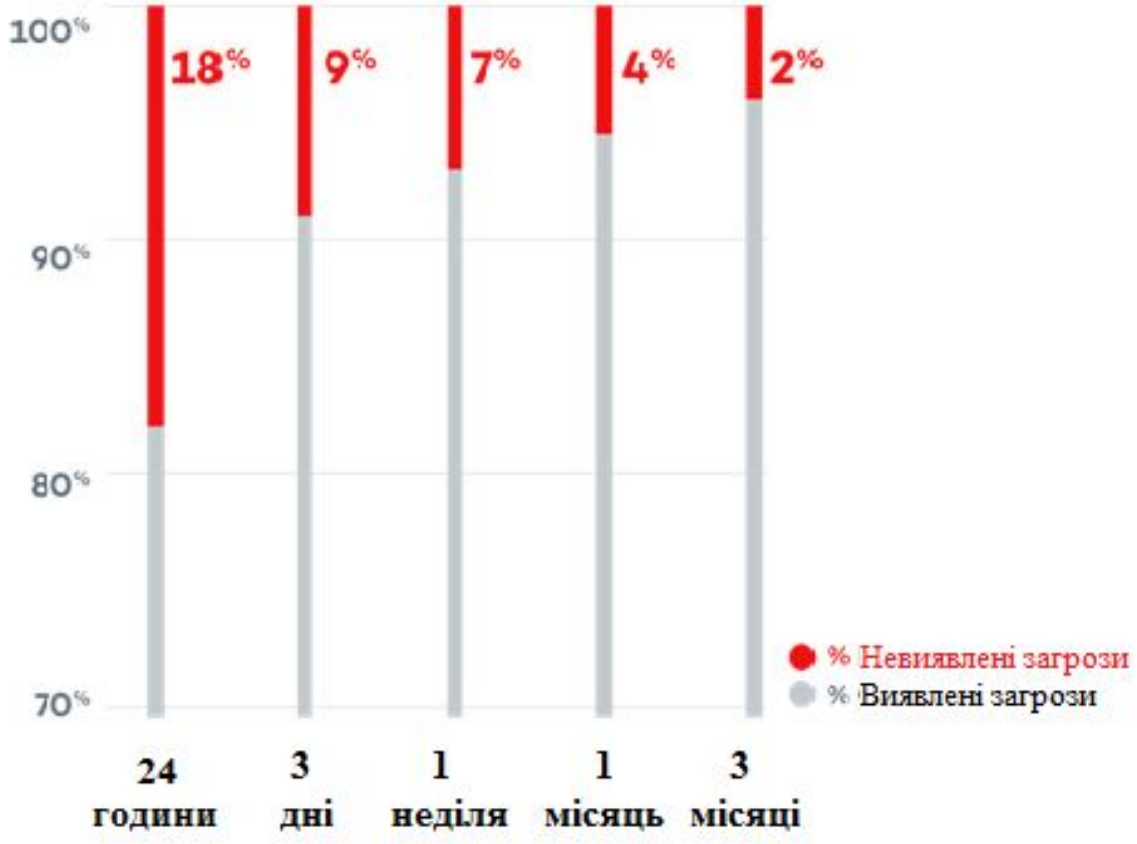
• засновані, як правило, на поведінці старих загроз. Ці системи виявлення застаріли, вони спрацьовують, як правило, тільки при спробі проникнення на комп'ютері відомої загрози або, в кращому випадку, підозрілої поведінки з точки зору традиційних технологій об'єкта. Вони не здійснюють глибокий моніторинг активності з аналізом причинно-наслідкового зв'язку.

Відношення зростання кіберінцидентів та еволюції засобів захисту

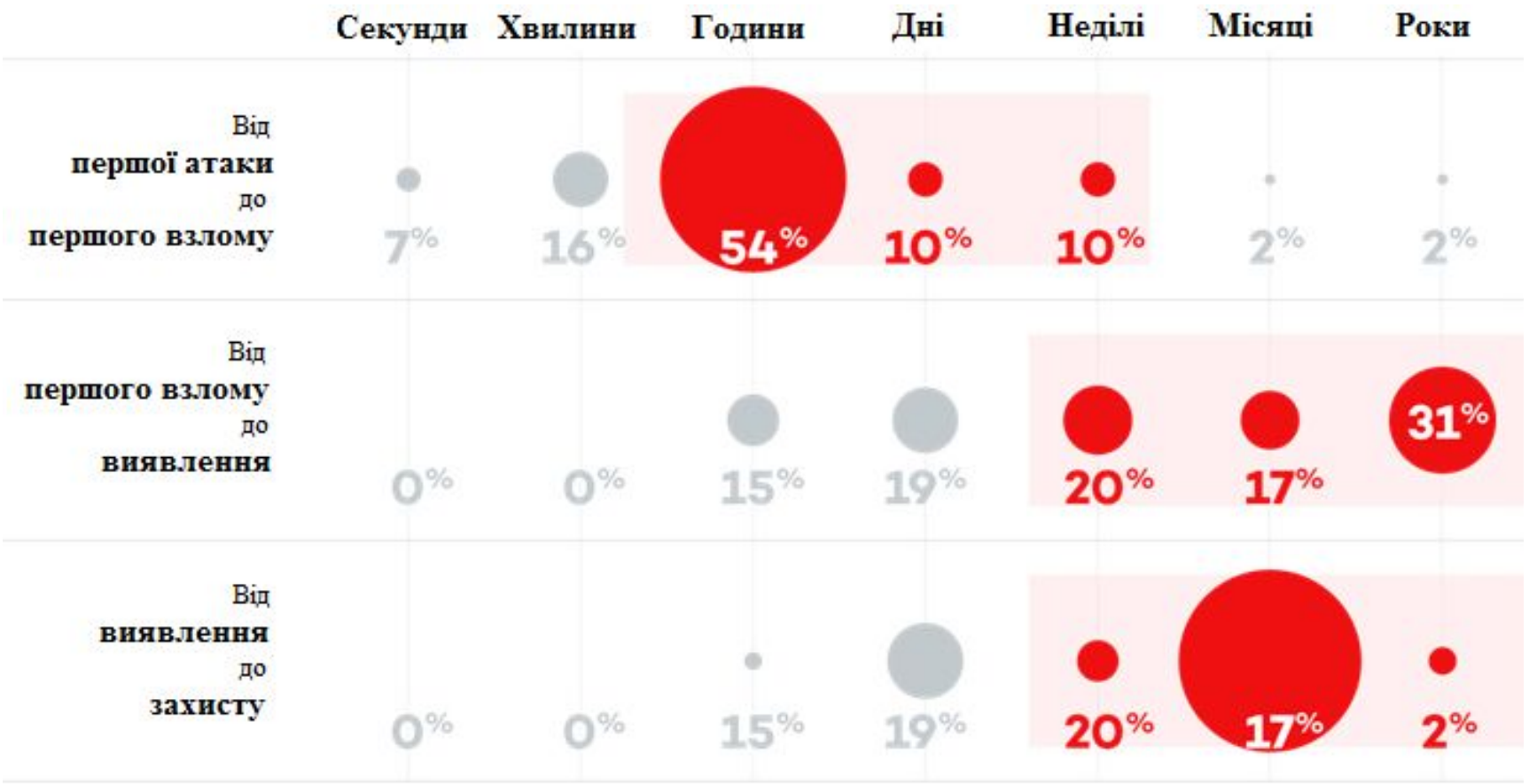


Невідомі загрози - це вікно можливостей.

За даними IDG Research, DARK Reading, **18% нових шкідливих програм залишаються непоміченими протягом перших 24 годин**, а 2% загроз можуть залишатися непоміченими навіть протягом 3 місяців після зараження.



Загроза може скомпрометувати систему за хвилини або години, в той час як **реакція організацій на ці загрози зазвичай займає тижні, місяці або навіть роки** .



Що таке **модель Cyber Kill Chain** і чому її треба враховувати в стратегії захисту.

Сучасні спрямовані атаки - це цілий комплекс заходів, в результаті чого злом і зараження мережі не відбуваються «раптом з нічого». Цьому передує цілий набір дій. Модель Cyber Kill Chain якраз і описує всі етапи атаки.

Cyber Kill Chain (CKC) - це класична модель кібербезпеки, розроблена командою реагування на інциденти, що порушують комп'ютерну безпеку (CSIRT - computer security incident response team) в компанії Lockheed Martin.

Мета моделі полягає в тому, щоб краще зрозуміти етапи, через які повинна пройти атака для її проведення, і допомогти командам безпеки зупинити атаку на кожному етапі.

Модель **Cyber Kill Chain** має **7 етапів (кроків)**, які проходить зловмисник для успішної реалізації своєї атаки:

1. Розвідка (**Reconnaissance**)
2. Озброєння (**Weaponization**)
3. Доставка (**Delivery**)
4. Експлуатація (зараження) (**Exploitation**)
5. Встановлення (**Installation**)
6. Управління та контроль (**Command and Control**)
7. Виконання дій (**Actions on Objective**)

1 Етап. Розвідка (**Reconnaissance**)

Дослідження, ідентифікація і вибір жертви, часто використовуючи публічні джерела даних - соцмережі, сайти конференцій, списки розсилки і т.п.

Цей етап може бути визначений як фаза вибору мети, виявлення особливостей організації, специфічних вимог в даній галузі, вибір технологій, вивчення активності компанії в соцмережах або через розсилки.

По суті, зловмисник намагається знайти точки входу в систему організації, отримати відповіді на запитання:

Які методи атаки будуть працювати?

Де, що або хто є найслабшим елементом захисту?

Як вдасться діяти непомітно та результативно?.

2 Етап. Озброєння (**Weaponization**)

Підбір інструментарію, створення експлойтів, оснащення шкідливим вмістом файли (наприклад, PDF або MS Office), використання атак типу «watering hole» або іншого контенту, який повинен бути прочитаний/відкритий жертвою.

Створене зловмисником шкідливе програмне забезпечення може використовувати нові, раніше не виявлені вразливості (також відомі як **експлойти нульового дня**).

3 Етап. Доставка (**Delivery**)

Передача необхідного (шкідливого) контенту або за ініціативою жертви (наприклад, користувач заходить на шкідливий сайт, в результаті чого передається шкідлива програма, або він відкриває шкідливий PDF-файл), або з ініціативи хакера (SQL-ін'єкція або компрометація мережної служби), або передача шкідливого програмного забезпечення за допомогою вкладень електронної пошти та USB-накопичувачів.

4 Етап. Експлуатація (**Exploitation**)

Після доставки на ПЕОМ користувача, необхідний (шкідливий) контент **запускається зловмисний код.**

Як правило, це відбувається при використанні відомої вразливості, для якої раніше був доступний патч. У більшості випадків (в залежності від мети) зловмисникам не потрібно проводити додаткові витрати на пошук і експлуатацію невідомих вразливостей.

Також на етапі експлуатації зловмисники можуть шукати додаткові вразливі місця або слабкі місця, які вони можуть використати всередині системи.

Наприклад, ззовні зловмисник може не мати доступу до баз даних організації, але після вторгнення вони можуть бачити, що база даних використовує застарілу версію та піддається добре відомій вразливості.

5 Етап. Встановлення (**Installation**)

Встановлення віддаленого доступу для непомітного управління і поновлення шкідливого коду, додавання функціональних модулів, завантаження додаткового шкідливого програмного забезпечення з Інтернету, дозволяючи зловмиснику виконувати свої зловмисні дії в системі.

Паралельно з етапом експлуатації зловмисники зазвичай намагаються закріпитися в системі, встановивши постійний чорний хід (**back door**).

Суть полягає в тому, щоб гарантувати, що віддалений доступ до мережі організації збережеться після перезавантаження скомпрометованих пристроїв.

6 Етап. Управління та контроль (**Command and Control**)

Після того, як буде встановлений постійний чорний хід в мережі організації, зловмисна програма буде встановлювати віддалене з'єднання зі зловмисником, щоб отримувати виправлення, функціональні оновлення і інструкції про подальші дії.

На цьому етапі зловмисники починають контролювати мережу жертви за допомогою таких методів управління (як правило, віддалених), як DNS, Internet Control Message Protocol (ICMP), веб-сайти і соціальні мережі.

В результаті чого відбувається збір інформації зловмисником.

6 Етап. Управління та контроль (**Command and Control**)

Використовуються такі **методи збору даних** :

- знімки екрану;
- контроль натискання клавіш;
- злом паролів;
- моніторинг мережі на облікові дані;
- збір критичного контенту і документів.

Часто призначається проміжний хост, куди копіюються всі дані, а потім вони стискаються / шифруються для подальшої відправки зловмиснику.

7 Етап. Виконання дій (**Actions on Objective**)

Збір і крадіжка даних, шифрування файлів, перехоплення управління, підміна даних та інші завдання, які можуть стояти перед порушником.

На фінальному етапі зловмисник відправляє зібрані дані і / або виводить з ладу мережу. Потім проводяться заходи щодо виявлення інших цілей, розширення своєї присутності всередині організації і (що найважливіше) вилучення даних.

Потім ланцюжок повторюється. Взагалі, особливістю Cyber-Kill Chain є те, що вона кругова, а не лінійна. Як тільки зловмисник проник в мережу, він знову починає цей ланцюжок всередині мережі, здійснюючи додаткову розвідку і виконуючи горизонтальне просування всередині мережі організації.

RECONNAISSANCE

INFORMATION GATHERING ABOUT THE TARGET

PASSIVE

- WHOIS
- ARIN
- GOOGLE
- SHODAN
- JOB LISTINGS
- COMPANY WEBSITE

ACTIVE

- NMAP
- PORT SCANNING
- BANNER GRABBING
- VULNERABILITY SCANNERS

PROTECT

- LIMIT PUBLIC INFORMATION (JOB POSTINGS, LINKEDIN, ECT..)
- SOCIAL MEDIA ACCEPTABLE USE
- MODIFY SERVER ERROR MESSAGES

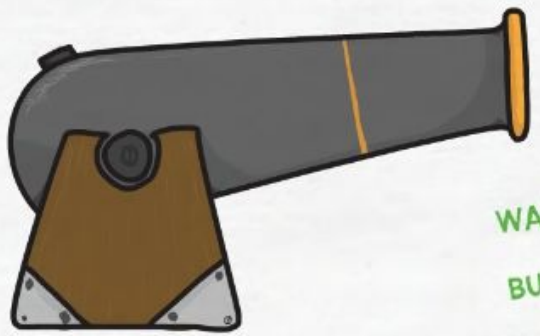
PROTECT

- DISABLE UNUSED PORTS/SERVICES
- HONEYPOTS
- FIREWALL
- IPS
- TOR & 3RD PARTY VPN INBOUND BLOCKING

WEAPONIZATION

FIND OR CREATE THE ATTACK TO EXPLOIT THE WEAKNESS

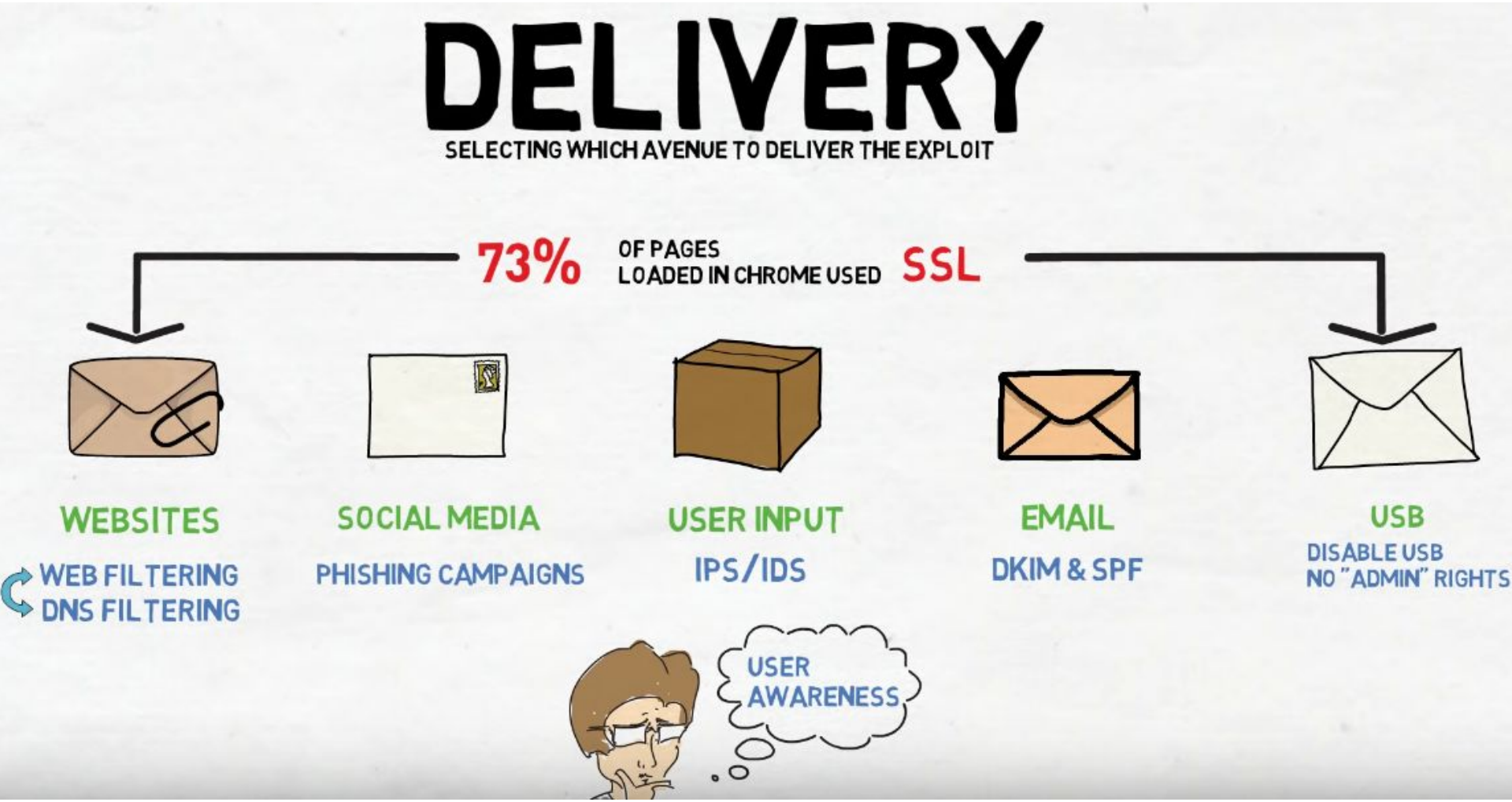
CAIN AND ABEL
SQLMAP
AIRCRACK
MALTEGOWEB APP
METASPLOIT
EXPLOIT-DB
VEIL FRAMEWORK
SOCIAL ENGINEERING TOOLKIT
WAPITI
BURPSUIT
FRATRAT

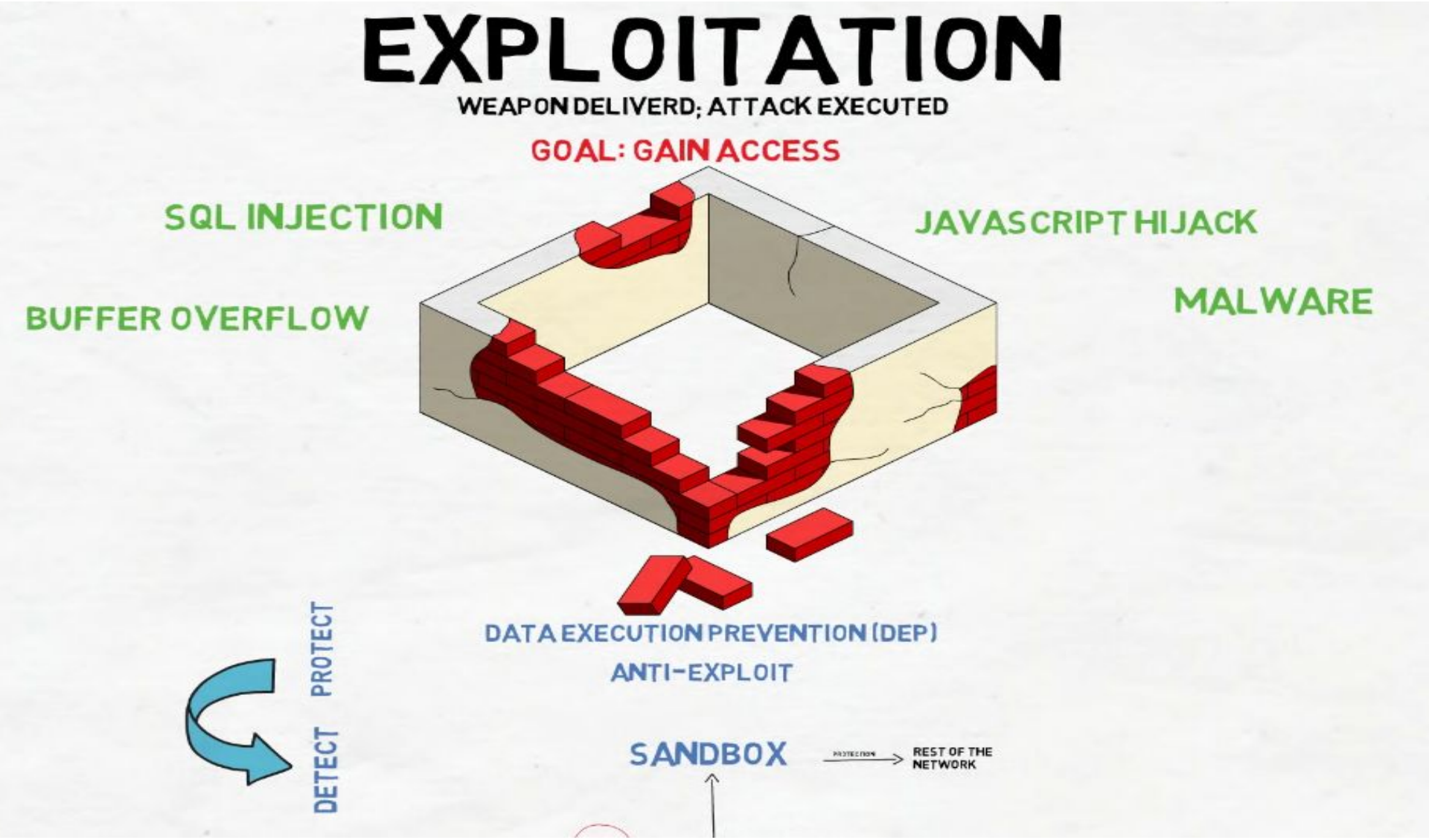


DEFENSIVE:

ADMINISTRATIVE CONTROLS:
- PATCH MANAGEMENT
- DISABLE: OFFICE MACROS, JAVASCRIPT AND BROWSER PLUGINS

TECHNICAL CONTROLS:
SECURITY BASICS
- AV
- IPS
- EMAIL SECURITY
- MFA
- AUDIT LOGGING
- ECT..


DELIVERY
SELECTING WHICH AVENUE TO DELIVER THE EXPLOIT
73%
OF PAGES LOADED IN CHROME USED
SSL
WEBSITES
WEB FILTERING
DNS FILTERING
SOCIAL MEDIA
PHISHING CAMPAIGNS
USER INPUT
IPS/IDS
EMAIL
DKIM & SPF
USB
DISABLE USB
NO "ADMIN" RIGHTS
USER AWARENESS


EXPLOITATION
WEAPON DELIVERD; ATTACK EXECUTED
GOAL: GAIN ACCESS
SQL INJECTION
JAVASCRIPT HIJACK
BUFFER OVERFLOW
MALWARE
DATA EXECUTION PREVENTION (DEP)
ANTI-EXPLOIT
PROTECT
DETECT
SANDBOX
REST OF THE NETWORK

INSTALLATION

PAYLOAD INJECTED AFTER THE EXPLOIT TO GAIN BETTER ACCESS

OFFENSIVE TOOLS:

- -DLL HIJACKING
- -METERPRETER
- -REMOTE ACCESS TOOLS (RAT)
- -REGISTRY CHANGES
- -POWERSHELL COMMANDS

PROTECT

- -LINUX: CHROOT
- WINDOWS: DISABLE POWERSHELL

DETECT

- -UBA/EDR

RESPOND

- -FOLLOW INCIDENT RESPONSE SOPS
  (I.D. DEVICE -> ISOLATE -> WIPE)

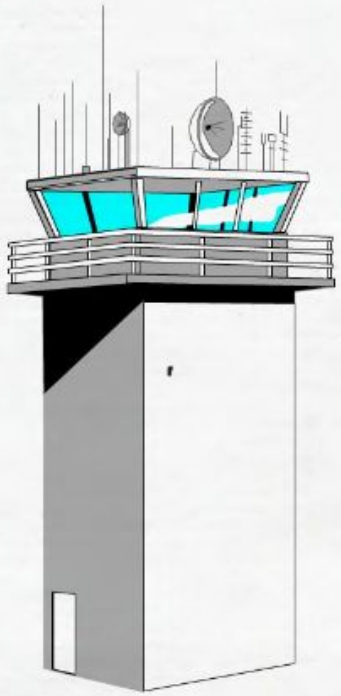
RECOVER

- -RESTORE OR REIMAGE

GOAL: GAIN PERSISTANT ACCESS

COMMAND AND CONTROL

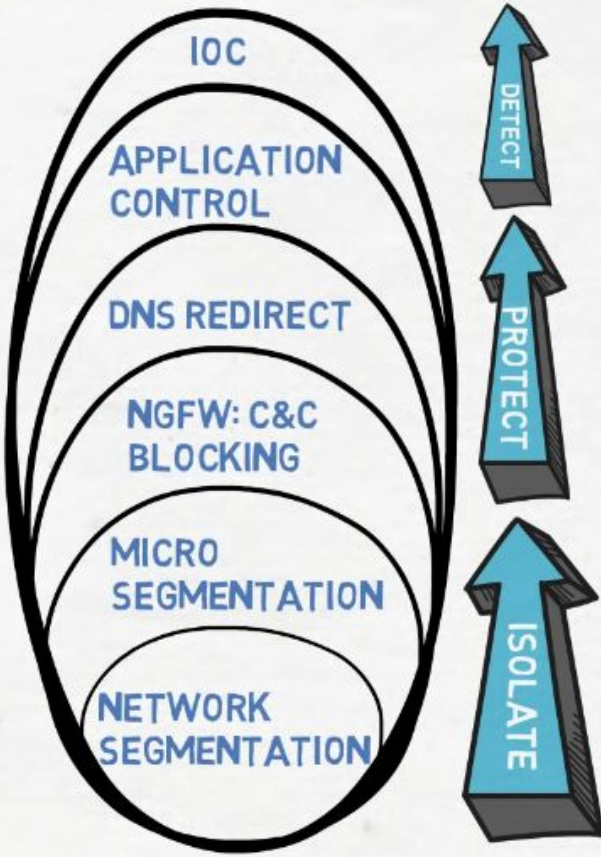
REMOTE CONTROL OF THE SYSTEM BY THE ATTACKER



```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
[*] msv credentials
===================

AuthID     Package    Domain           User             Password
------     -------    ------           ----             --------
0;1035282  NTLM       WIN-LOANLOTDQLU  Ralf             lm{ 00000000000000000000
0000000000000 }, ntlm{ 2e520e18228ad8ea4060017234af43b2 }
0;1035232  NTLM       WIN-LOANLOTDQLU  Ralf             lm{ 00000000000000000000
0000000000000 }, ntlm{ 2e520e18228ad8ea4060017234af43b2 }
0;669397   NTLM       WIN-LOANLOTDQLU  Fred             lm{ aad3b435b51404eeaad
3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;669366   NTLM       WIN-LOANLOTDQLU  Fred             lm{ aad3b435b51404eeaad
3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;997      Negotiate  NT AUTHORITY     LOCAL SERVICE    n.s. (Credentials KO)
0;996      Negotiate  WORKGROUP        WIN-LOANLOTDQLU$ n.s. (Credentials KO)
0;42061    NTLM                                         n.s. (Credentials KO)
0;999      NTLM       WORKGROUP        WIN-LOANLOTDQLU$ n.s. (Credentials KO)

meterpreter >
```



☑ SSL DEEP PACKET INSPECTION

ACTIONS ON OBJECTIVE

ATTACKER EXECUTES DESIRED ACTION

FINANCIAL

POLITICAL

ESPIONAGE

MALICIOUS INSIDER

LATERAL MOVEMENT

EXFILTRATE DATA

- DATA LEAKAGE PREVENTION (DLP)
- USER BEHAVIOUR ANALYSIS (UBA)

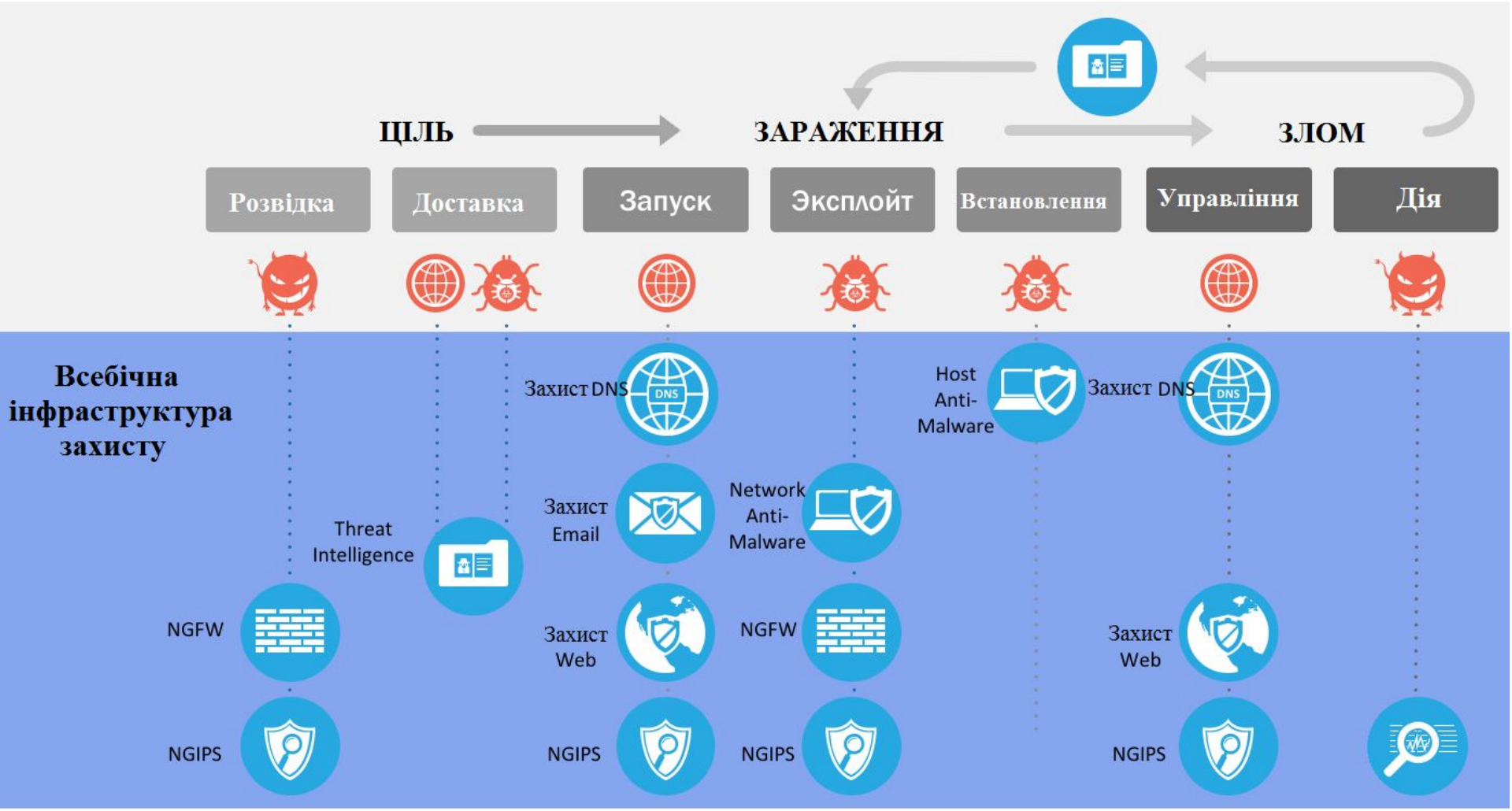
LATERAL MOVEMENT

- NETWORK SEGMENTATION

Етапи реалізації кібератаки згідно Lockheed Martin Kill Chain.

Розвідка	Збір електронної пошти	Соціальні мережі	Пасивний пошук	Визначення IP	Сканування портів
Озброєння	Створення зловмисного коду	Система доставки	Приманка		
Доставка	Фішинг	Зараження сайту	Оператори зв'язку		
Проникнен	Активація	Виконання коду	Визначення плацдарму	Проникнення на інші ресурси	
Інсталяція	Троян або бекдор	Підвищення привілеїв	Руткіт	Забезпечення непомітності	
Управлінн	Канал управління	Розширення плацдарму	Внутрішнє сканування	Підтримання непомітності	
Реалізація	Розширення зараження	Витік даних	Перехоплення управління	Виведення з ладу	
Знищення слідів	Підтримка непомітності	Зачищання лог-файлів			

Етапи реалізації кібератаки згідно Lockheed Martin Kill Chain.



Cyber Kill Chain це систематичний процес досягнення порушником мети для отримання бажаного ефекту. Тому це поняття варто включити в арсенал служб інформаційної безпеки.

Використовувати це поняття можна при моделюванні загроз, а з практичної точки зору Cyber Kill Chain використовується при оцінці ефективності побудованої Security інфраструктури.

2. Структура MITRE ATT&CK Matrix for Enterprise.

Ланцюг Cyber Kill Chain добре підходить для моделювання загроз.

Тобто мова йде про систематизацію наявної інформації про всі методи атак, які використовуються зловмисниками. І в цьому допомагає матриця

ATT&CK (Adversarial Tactics, Techniques & Common Knowledge - Тактики, техніки і загальновідомі знання про зловмисників),

яка розроблена американською корпорацією MITRE

MITRE ATT & CK - це структурований список відомих поведінок зловмисників, розділений на тактики і методи, і виражений у вигляді таблиць (матриць).

Матриці для різних ситуацій і типів зловмисників публікуються на сайті MITRE.

Оскільки цей список дає комплексне уявлення про поведінку зловмисників при зломі мереж, він вкрай корисний для різних захисних заходів, моніторингу, навчання і інших застосувань.

Зокрема, матриця ATT & CK може бути корисна в кіберрозвідці, оскільки вона дозволяє стандартизовано описувати поведінку зловмисників.

Зловмисники можуть відслідковуватися за допомогою ведення спостереження за подіями в мережі використовуючи методи і тактики в ATT & CK, які використовують ті чи інші угруповання.

Фахівцям з ІБ це дозволяє оцінювати свій рівень захищеності, аналізуючи здатності наявних засобів захисту виявляти або блокувати ті чи інші методи та тактики, що дає уявлення про сильні та слабкі сторони проти певних зловмисників.

Проводиться візуалізація сильних та слабких сторін засобів захисту.

MITRE розбила ATT & CK на декілька різних матриць:

- Enterprise
- Mobile
- PRE-ATT & CK .

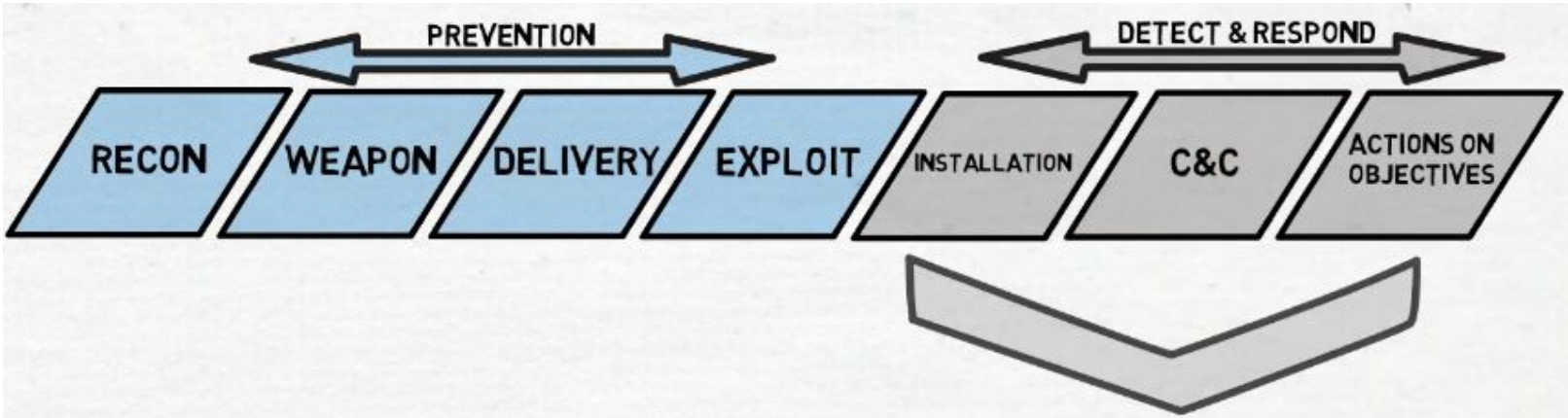
Кожна з цих матриць містить різні тактики та техніки, пов'язані з предметом цієї матриці.

Матриця Enterprise складається з методів і тактик, що застосовуються до систем Windows, Linux та / або MacOS. Mobile містить тактику та техніку, що стосуються мобільних пристроїв. PRE-ATT & CK містить тактику та техніку, пов’ язану з тим, що роблять зловмисники до того, як вони намагаються використати певну цільову мережу або систему.

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares

Структура MITRE ATT&CK Matrix for Enterprise.

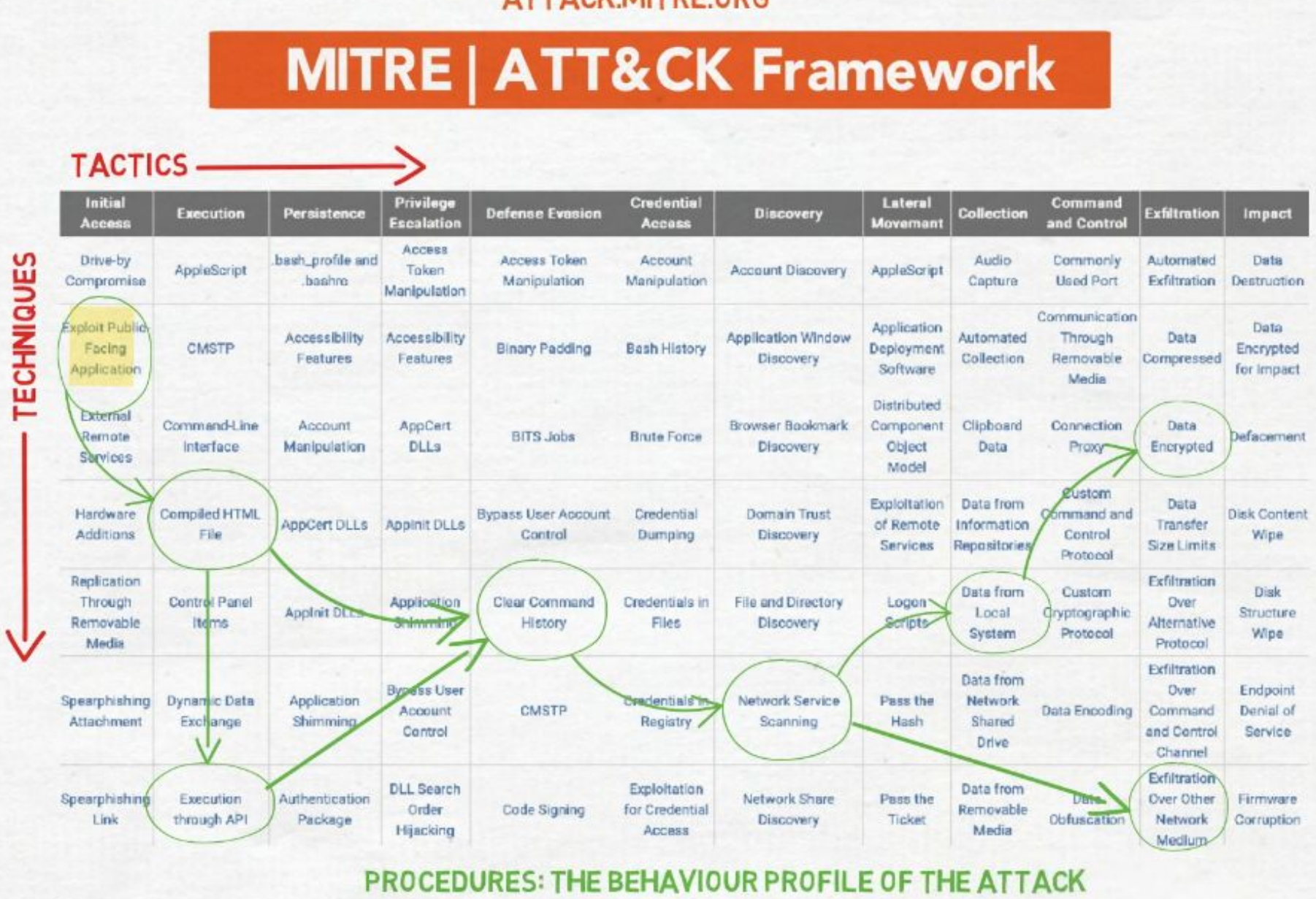


BASED ON REAL WORLD ATTACKS

OVER 290 TECHNIQUES

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking

Структура MITRE ATT&CK Matrix for Enterprise.



ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
імені ГЕРОЇВ КРУТ

viti.edu.ua

ДЯКУЮ ЗА УВАГУ!

ПИТАННЯ???

КИЇВ-2019