



Техно infotecs  
2021 Фест

ТЕХНИЧЕСКИЙ  
ФЕСТИВАЛЬ

# Обнаружение и предотвращение атак при помощи ViPNet EndPoint Protection. Разбор поведения злоумышленника по MITRE ATT&CK

Иван Кадыков

О чём пойдёт речь?

# «Болезни» последних 5-ти лет





# Kill Chain

Атаку можно структурировать

MITRE

ATT&CK™

Методология  
для специалистов ИБ

Adversary  
Tactics  
Techniques  
&  
Common  
Knowledge

# Техники — Тактики — Процедуры

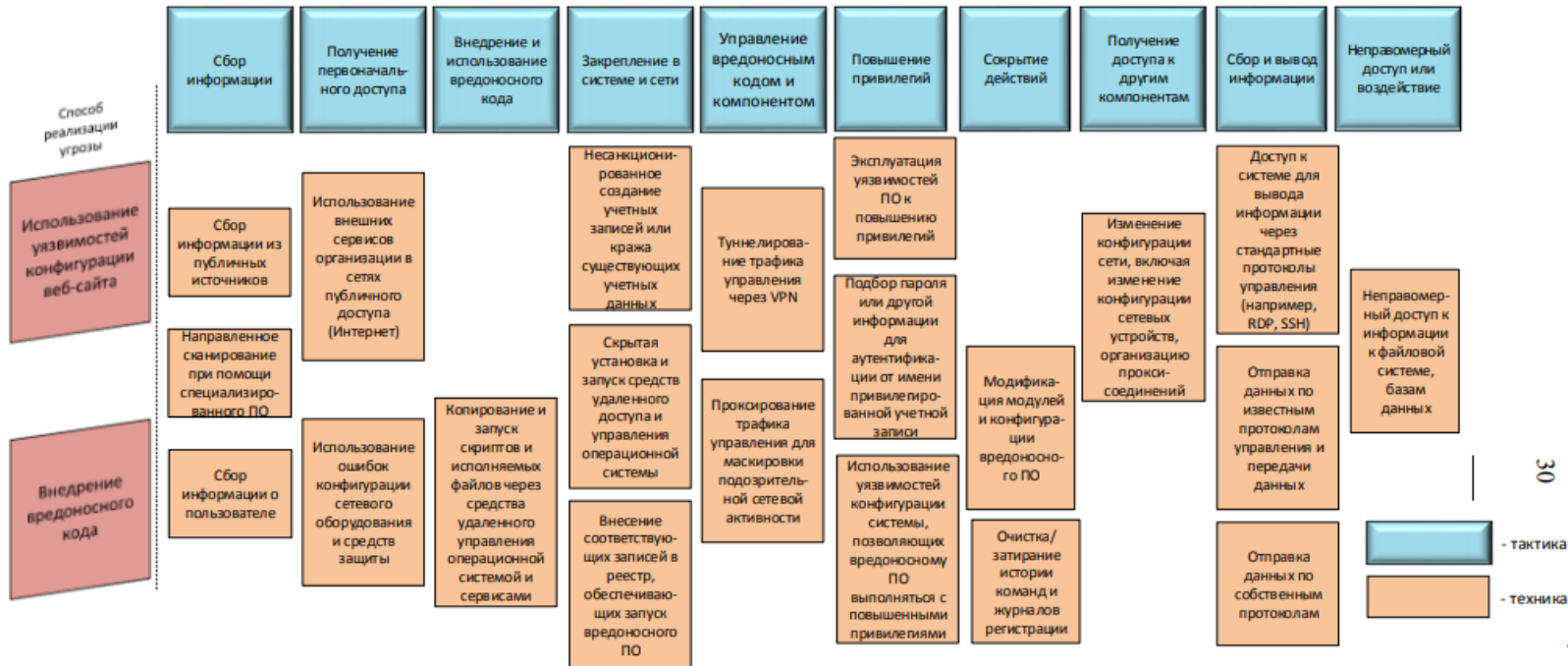
## ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Data from Information Repositories (2)	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Escape to Host	Execution Guardrails (1)	Modify Authentication Process (4)	Domain Trust Discovery	Data from Local System	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)	Valid Accounts (4)	Software Deployment Tools	System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	File and Directory Permissions Modification (2)	Data from Network Shared Drive	Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Victim-Owned Websites	Windows Management Instrumentation	System Services (2)	User Execution (3)	External Remote Services	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Permissions Modification (2)	Data from Network Shared Drive	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (2)
					Hijack Execution Flow (11)	Hide Artifacts (7)	Password Policy Discovery	Hide Artifacts (7)	Data from Removable Media	Data from Removable Media	Non-Standard Port		Resource Hijacking
					Process Injection (11)	Hijack Execution Flow (11)	Peripheral Device Discovery	Steal Application Access Token	Data Staged (2)	Data Staged (2)	Protocol Tunneling		System Shutdown/Reboot
					Indicator Removal on Host (6)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Steal Web Session Cookie	Email Collection (3)	Email Collection (3)	Proxy (4)		
					Scheduled Task/Job (7)	Indirect Command Execution	Permission Groups Discovery (3)	Process Discovery	Input Capture (4)	Input Capture (4)	Remote Access Software		
					Valid Accounts (4)	Masquerading (6)	Query Registry	Query Registry	Man in the Browser	Man in the Browser	Traffic Signaling (1)		
					Modify Authentication Process (4)	Modify Authentication Process (4)	Remote System Discovery	Remote System Discovery	Man-in-the-Middle (2)	Man-in-the-Middle (2)	Web Service (3)		
					Scheduled Task/Job (7)	Modify Cloud Compute Infrastructure (4)	Software Discovery (1)	System Information Discovery	Screen Capture	Screen Capture			
					Server Software Component (3)	Modify Registry	System Location Discovery	System Location Discovery	Video Capture	Video Capture			
					Traffic Signaling (1)	Modify System Image (2)	System Network Configuration	System Network Configuration					
						Network Boundary							

# «Методика оценки угроз безопасности информации» — ФСТЭК России

Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию



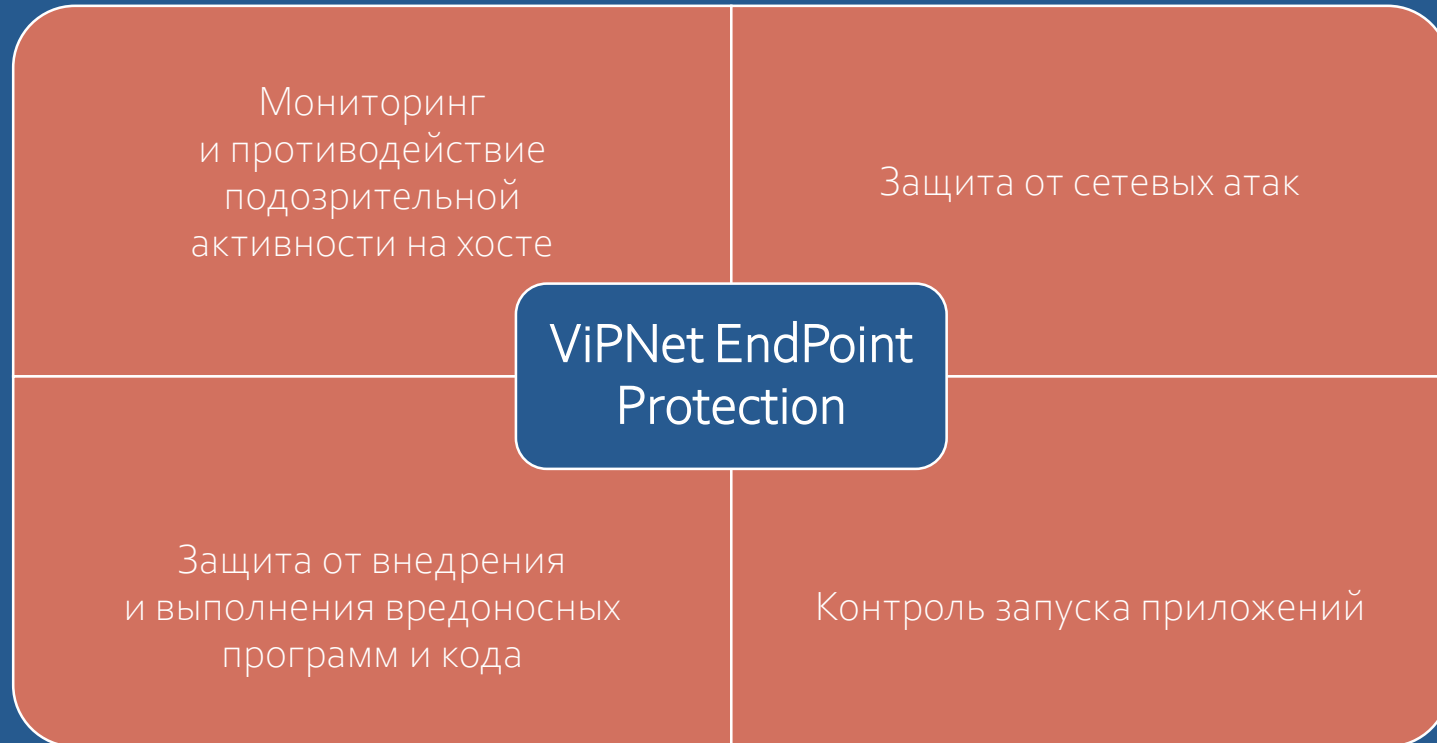
# VIPNet EndPoint Protection



Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.



# Решаемые задачи





## Давайте попрактикуемся

Продукт:

ViPNet EndPoint Protection

Знания:

MITRE ATT&CK

# ВАЖНО!

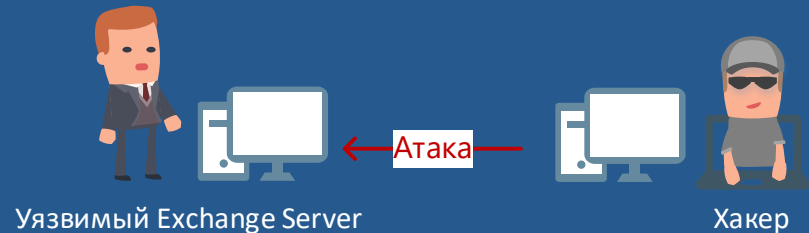
- Мы не учим атаковать, мы показываем атаку и учим, как от нее защищаться!
- Все материалы по атакам взяты из открытых источников
- Не стоит повторять атаки дома или на работе 😊
- А вот средства защиты использовать надо! 😊 😊 😊



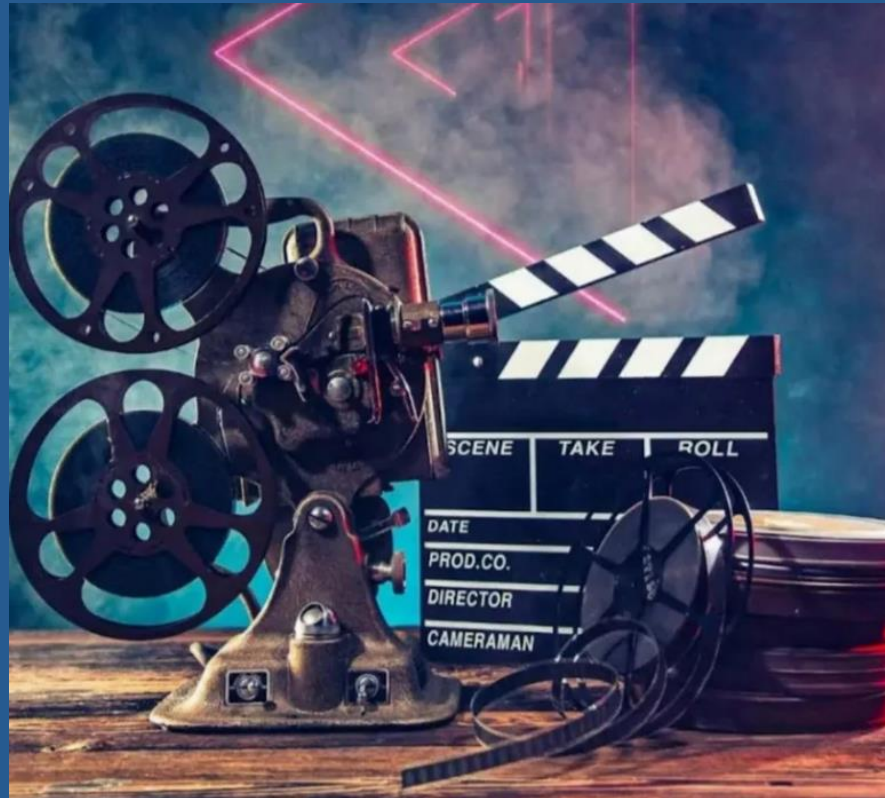
# Сценарий 1. Атака уязвимого Exchange- сервера. Получение хэша пароля администратора

# Что за атака?

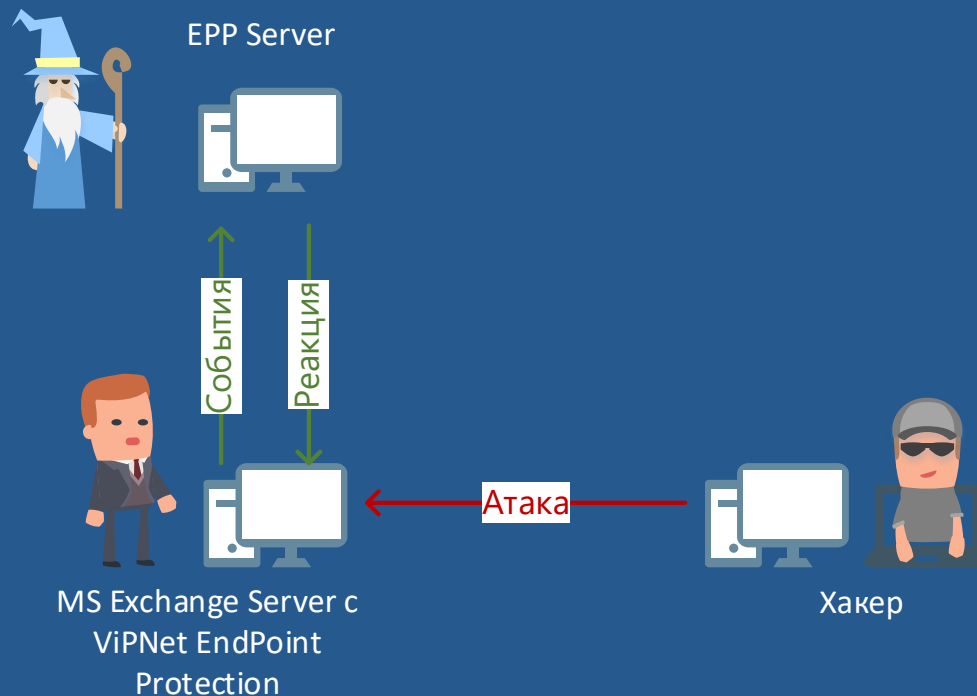
- Злоумышленник будет использовать известную уязвимость ProxyLogon, точнее CVE-2021-26857 (2 марта 2021 года Microsoft выпустила обновления безопасности, чтобы закрыть эти уязвимости).
- Суть атаки – отправка HTTP-запроса для обхода механизма аутентификации, с дальнейшим проникновением в систему и закрепление.



# Демонстрируем атаку!



# В инфраструктуре появился ViPNet EndPoint Protection



# Что же должно быть включено в EPP?

## Персональный межсетевой экран



### Полная блокировка трафика

Блокируется любой входящий и исходящий трафик.



### Публичная сеть

Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.



### Частная сеть

Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры.



### Защищенная сеть

Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.



### Отключен

Personal Firewall полностью отключен и не влияет на сетевой трафик.

## Контроль приложений



### Блокировать

Запуск неизвестных приложений блокируется. Активность остальных приложений определяется правилами Контроля приложений.



### Разрешать

Запуск неизвестных приложений разрешен. Активность остальных приложений определяется правилами Контроля приложений.



### Отключен

Контроль приложений отключен и не влияет на активность приложений.

## Обнаружение и предотвращение вторжений

Модуль обнаружения вторжений активен



### Усиленный

Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.



### Базовый

Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.



### Минимальный

Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.

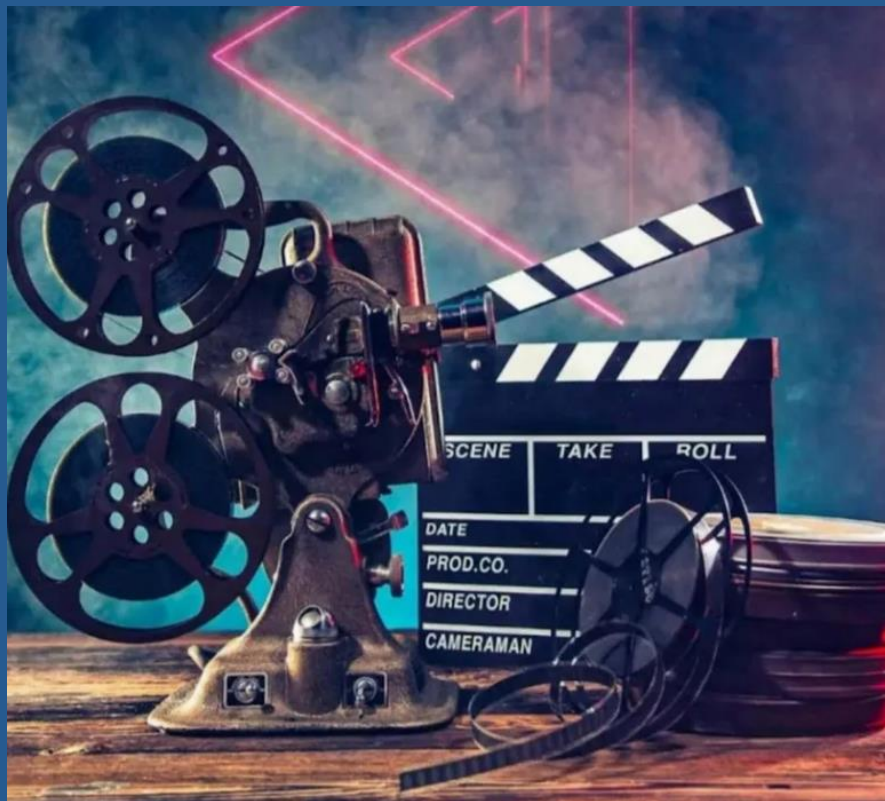


### Отключен

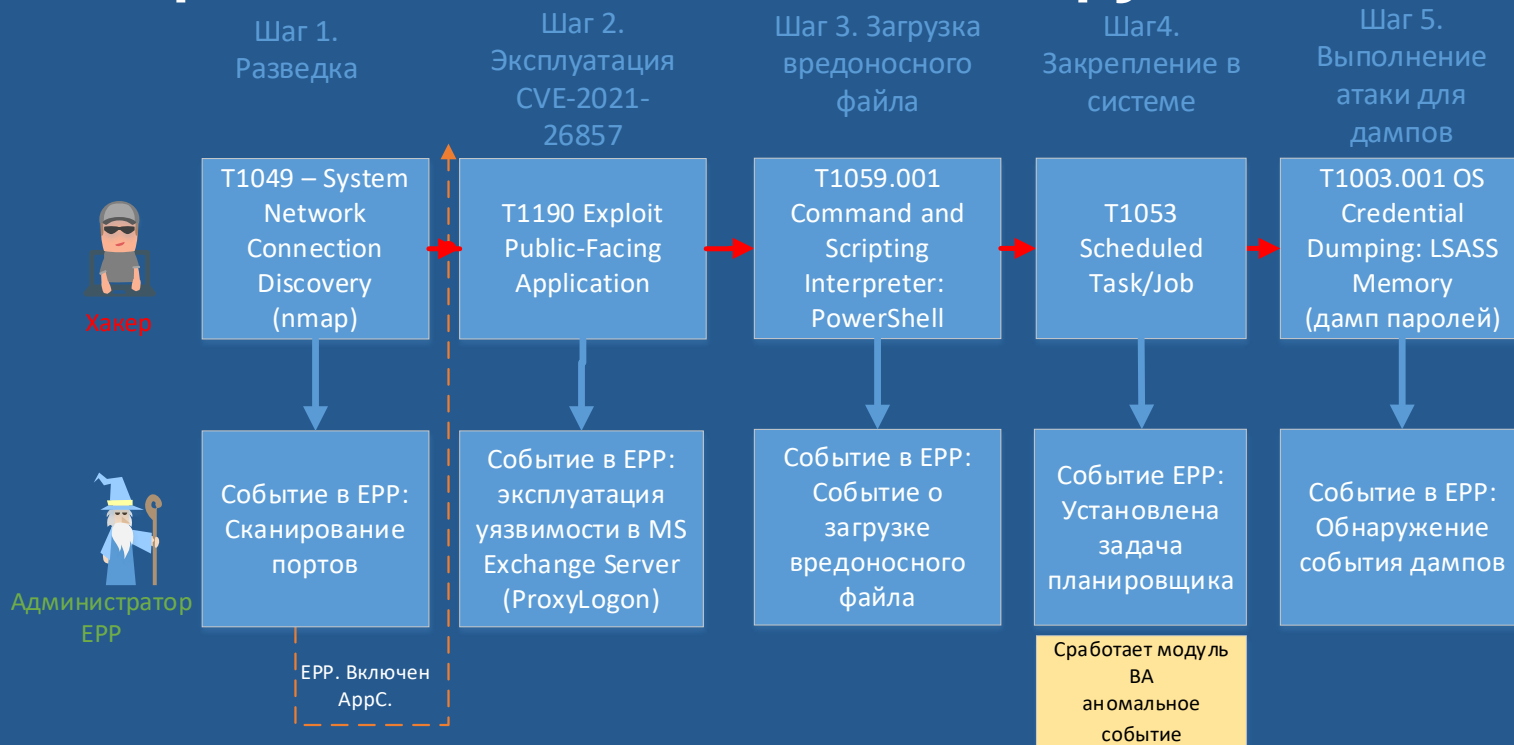
Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.



# Повторно атакуем, с включенным ViPNet EndPoint Protection



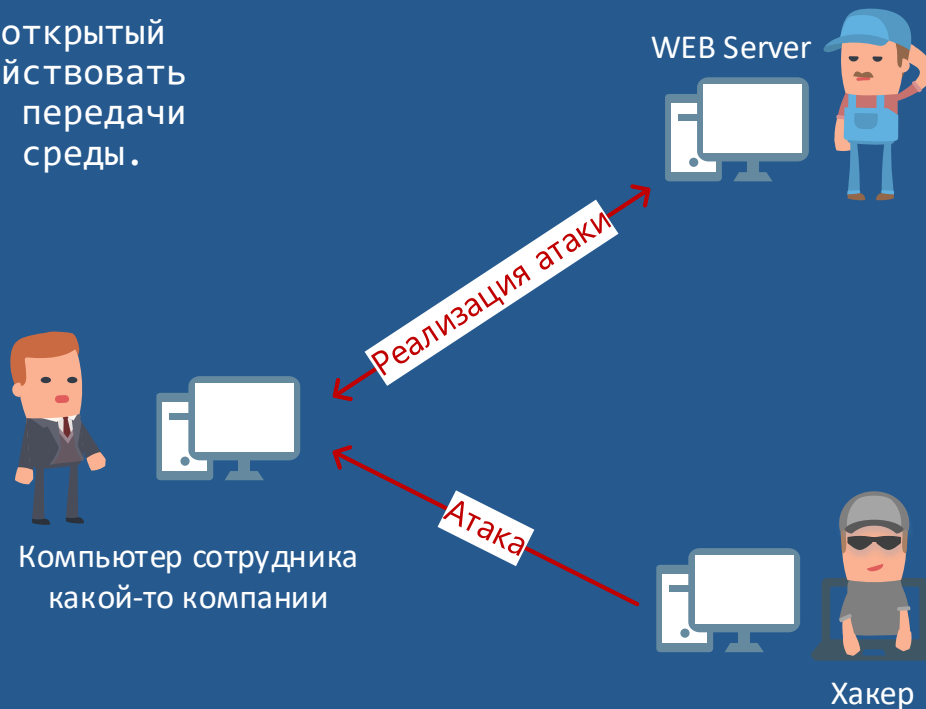
# Пошаговый разбор. Как противодействовать хакеру



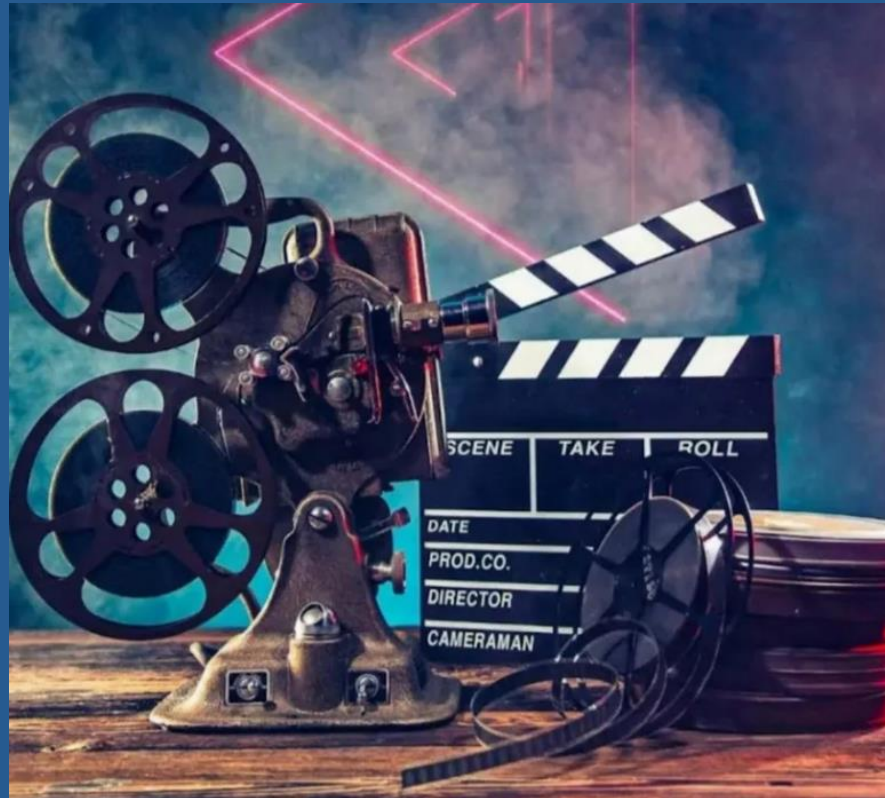
**Сценарий 2.  
Загрузка вредоносной  
программы через открытый  
порт 22 (ssh), используя  
Resolve DNS.**

# Что за атака?

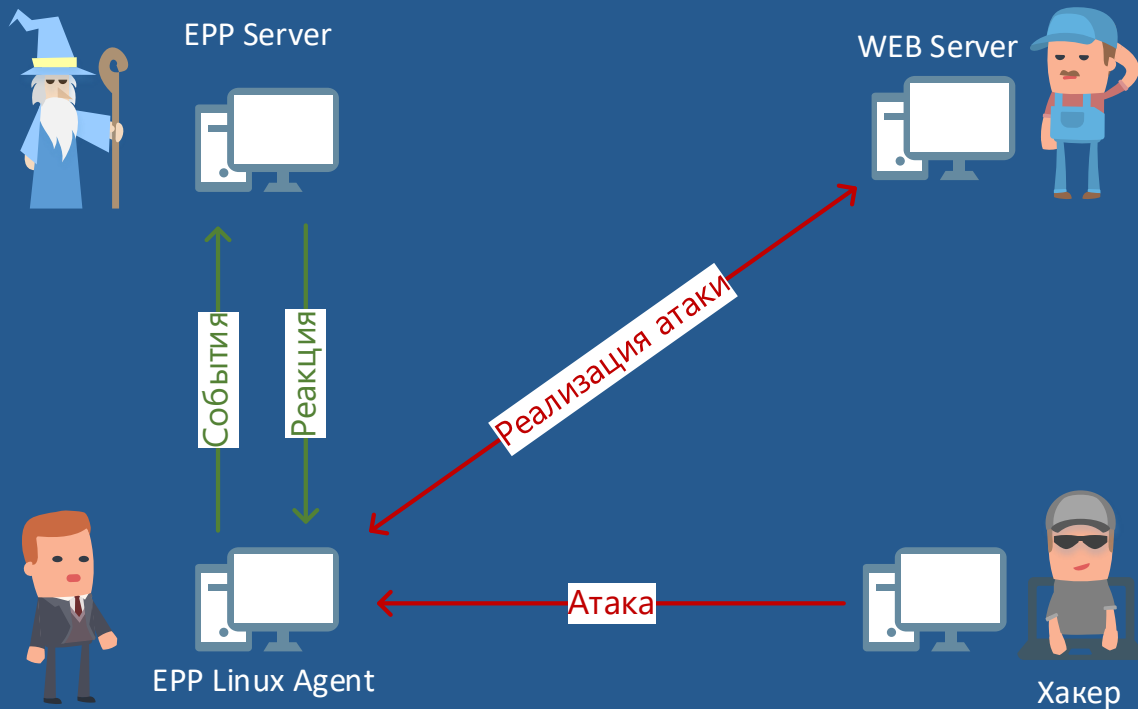
- Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб службу для передачи данных в/из корпоративной среды.



# Демонстрируем атаку!



# В инфраструктуре появился ViPNet EndPoint Protection



# Что же должно быть включено в EPP?

## Персональный межсетевой экран



### Полная блокировка трафика

Блокируется любой входящий и исходящий трафик.



### Публичная сеть

Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.



### Частная сеть

Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры.



### Защищенная сеть

Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.



### Отключен

Personal Firewall полностью отключен и не влияет на сетевой трафик.

## Контроль приложений



### Блокировать

Запуск неизвестных приложений блокируется. Активность остальных приложений определяется правилами Контроля приложений.



### Разрешать

Запуск неизвестных приложений разрешен. Активность остальных приложений определяется правилами Контроля приложений.



### Отключен

Контроль приложений отключен и не влияет на активность приложений.

## Обнаружение и предотвращение вторжений



Модуль обнаружения вторжений активен



### Усиленный

Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.



### Базовый

Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.



### Минимальный

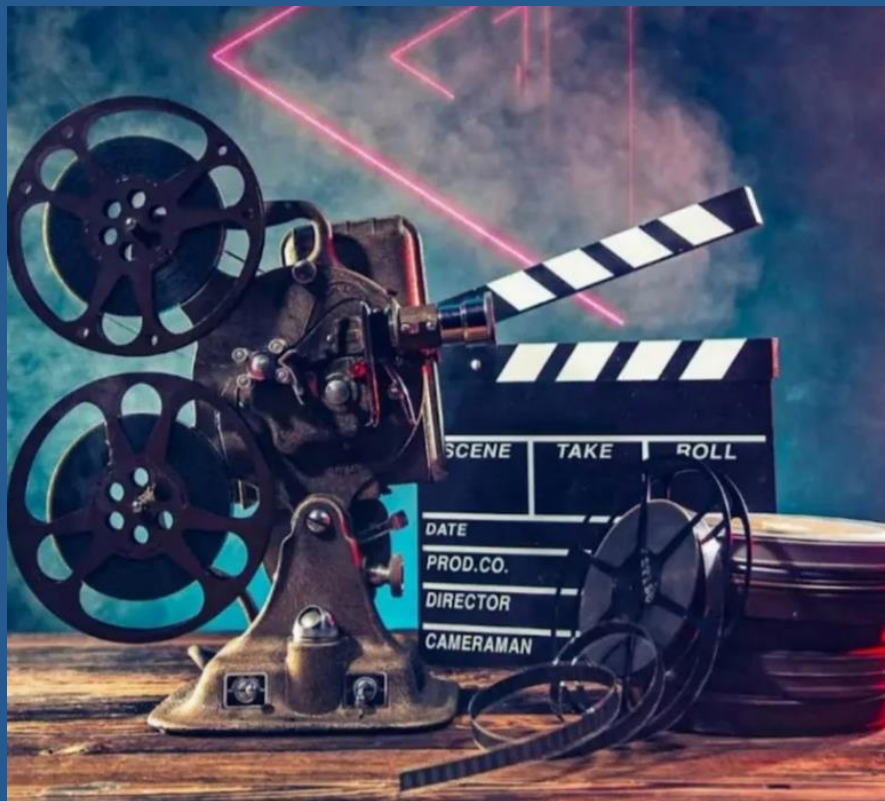
Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.



### Отключен

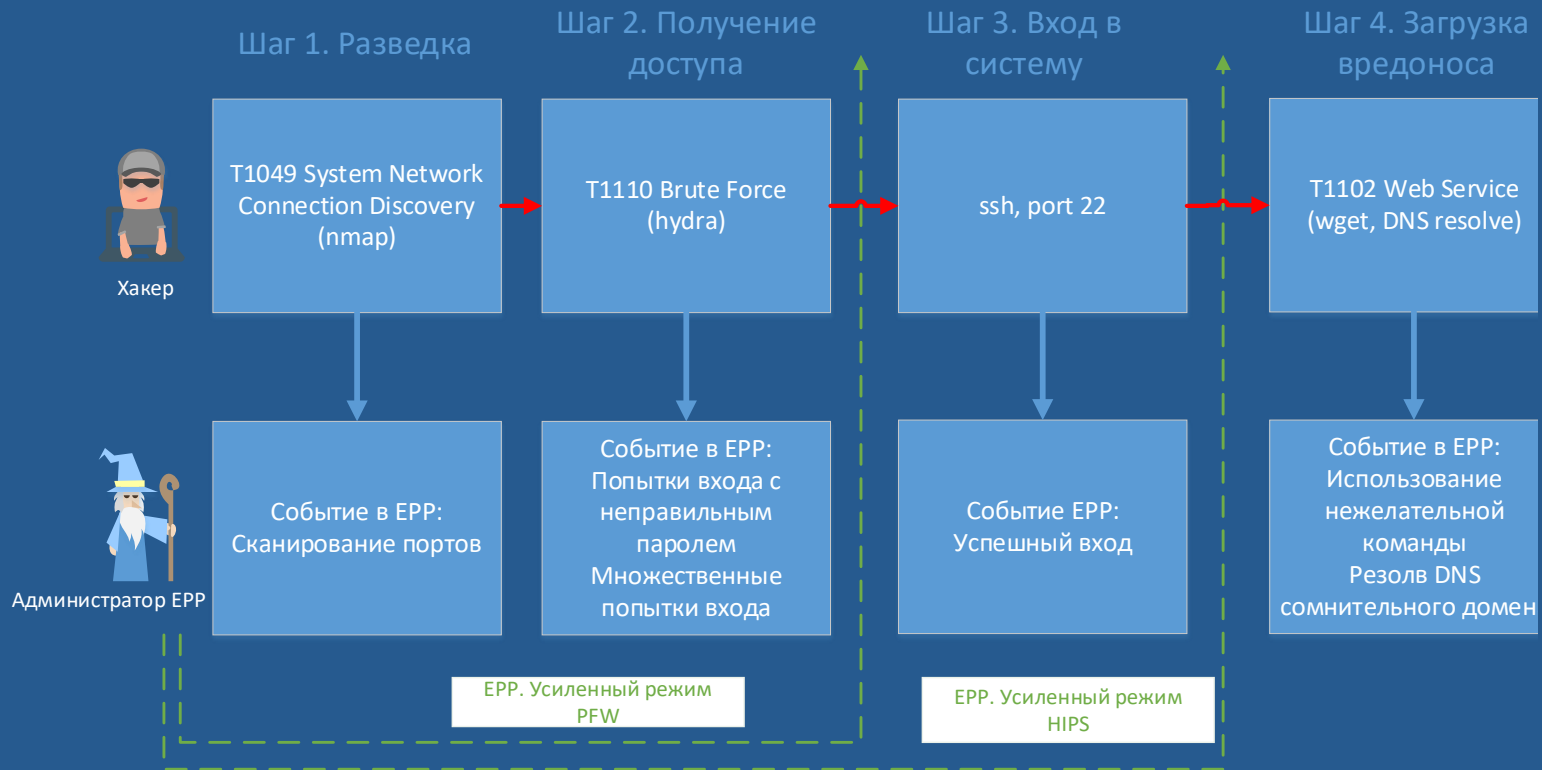
Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.

# Повторно атакуем, с включенным ViPNet EndPoint Protection





# Пошаговый разбор. Как противодействовать хакеру



ТЕХНО infotecs  
2021 Фест

Спасибо  
за внимание!

Подписывайтесь на наши соцсети



@infotecs.ru



@vpninfotecs



@InfoTeCS\_Moscow