

# Обнаружение и предотвращение атак при помощи ViPNet EndPoint Protection.

Разбор поведения злоумышленника по MITRE ATT&CK

Кадыков Иван  
Руководитель направления

техно infotecs  
2022 ФЕСТ

ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

О чём пойдёт речь?

# «Болезни» последних шести лет





# Kill Chain

Атаку можно структурировать

MITRE

ATT&CK™

Методология  
для специалистов ИБ

Adversary  
Tactics  
Techniques  
&  
Common  
Knowledge

# Техники — Тактики — Процедуры

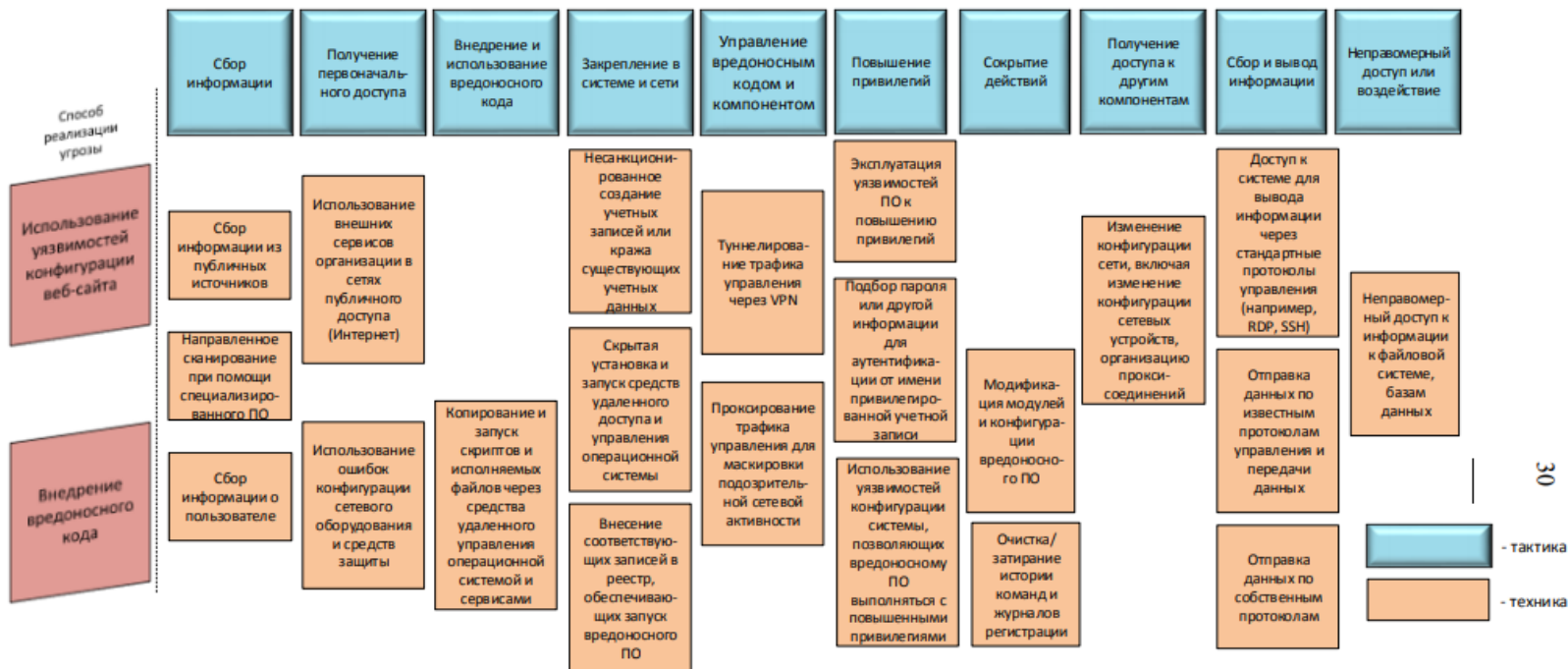
## ATT&CK Matrix for Enterprise

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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	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)	BITS Jobs	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 Autostart Execution (14)	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	Boot or Logon Initialization Scripts (5)	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	Create or Modify System Process (4)	Direct Volume Access	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)	Domain Policy Modification (2)	Domain Policy Modification (2)	Execution Guardrails (1)	Man-in-the-Middle (2)	Container and Resource Discovery	Data from Information Repositories (2)	Data from Local System	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)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Data from Network Shared Drive	Software Deployment Tools	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)	User Execution (3)	Windows Management Instrumentation	System Services (2)	External Remote Services	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Data from Network Shared Drive	Taint Shared Content	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Victim-Owned Websites			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	Hide Artifacts (7)	OS Credential Dumping (8)	File and Directory Permissions Modification (2)	Data from Removable Media	Use Alternate Authentication Material (4)	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (2)
				Hijack Execution Flow (11)	Scheduled Task/Job (7)	Hijack Execution Flow (11)	Steal Application Access Token	Exploitation for Privilege Escalation	Data Staged (2)		Non-Standard Port		Resource Hijacking
				Implant Internal Image	Valid Accounts (4)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	File and Directory Permissions Modification (2)	Peripheral Device Discovery		Protocol Tunneling		System Shutdown/Reboot
				Modify Authentication Process (4)		Indicator Removal on Host (6)	Steal Web Session Cookie	Hide Artifacts (7)	Password Policy Discovery		Proxy (4)		
				Office Application Startup (6)		Scheduled Task/Job (7)	Process Discovery	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)		Remote Access Software		
				Pre-OS Boot (5)		Two-Factor Authentication Interception	Query Registry	Process Injection (11)	Permission Groups Discovery (3)		Traffic Signaling (1)		
				Scheduled Task/Job (7)		Masquerading (6)	Remote System Discovery	Indicator Removal on Host (6)	Process Discovery		Web Service (3)		
				Server Software Component (3)		Modify Authentication Process (4)	Software Discovery (1)	Indirect Command Execution	Remote System Discovery				
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)	System Information Discovery	Two-Factor Authentication Interception	System Location Discovery				
						Modify Registry	System Network Configuration	Unsecured Credentials (7)	System Location Discovery				
						Modify System Image (2)							
						Network Boundary							

# «Методика оценки угроз безопасности информации». ФСТЭК России

Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию



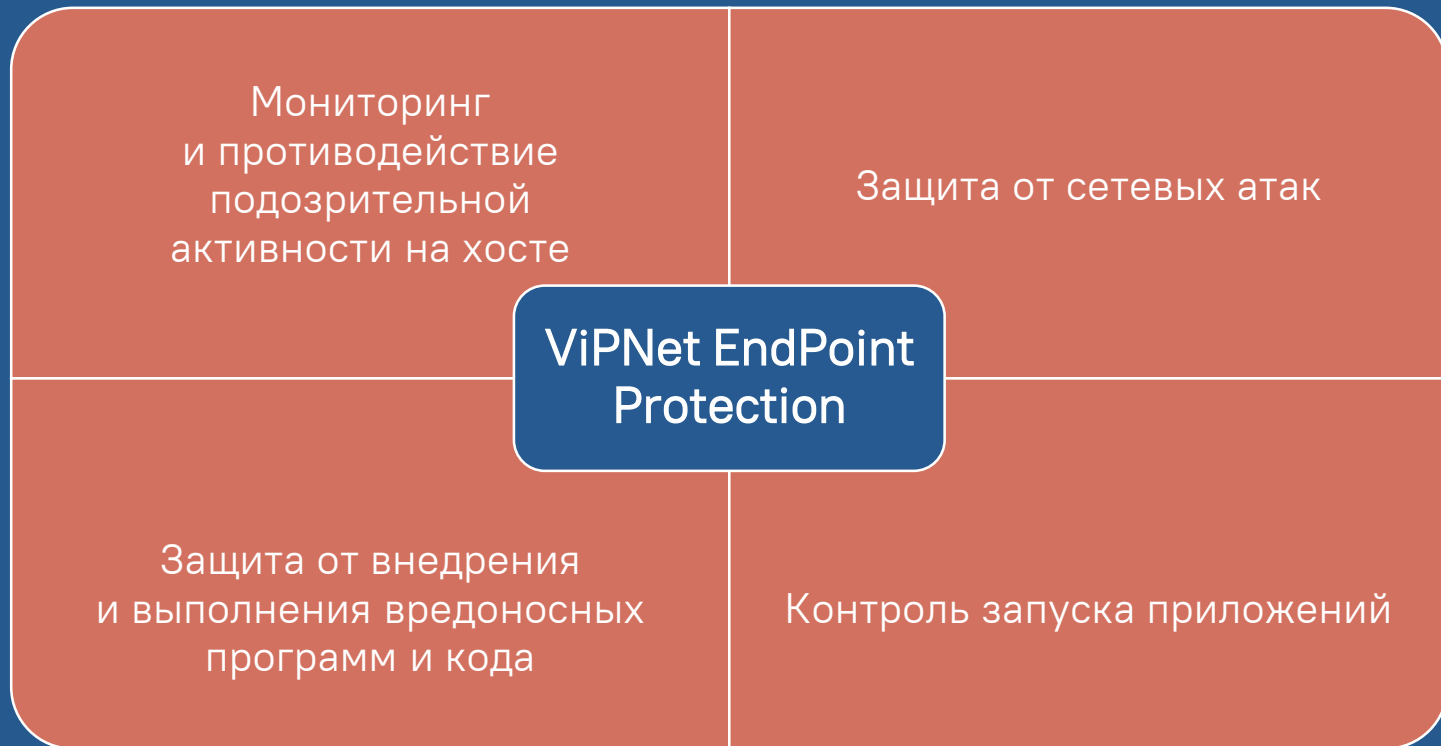
# VIPNet EndPoint Protection

Контроль приложений





# Решаемые задачи





## Давайте попрактикуемся

Продукт:

ViPNet EndPoint Protection

Знания:

MITRE ATT&CK

# ВАЖНО!

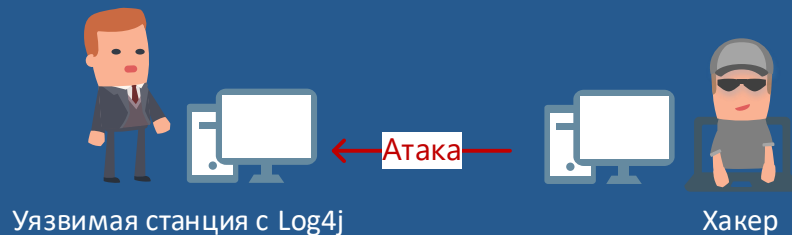
- Мы не учим атаковать, мы показываем атаку и учим, как от нее защищаться!
- Все материалы по атакам взяты из открытых источников.
- Не стоит повторять атаки дома или на работе 😊
- А вот средства защиты использовать надо! 😊 😊 😊



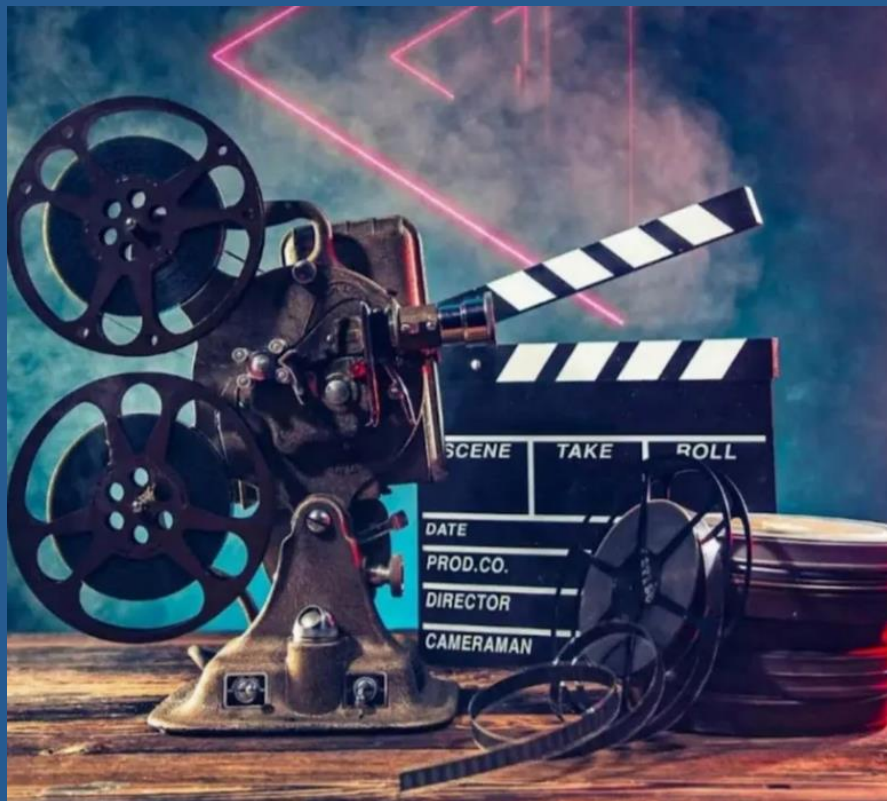
# Сценарий 1. Атака через уязвимость в Log4j. Запуск произвольного кода или приложения

# Что за атака?

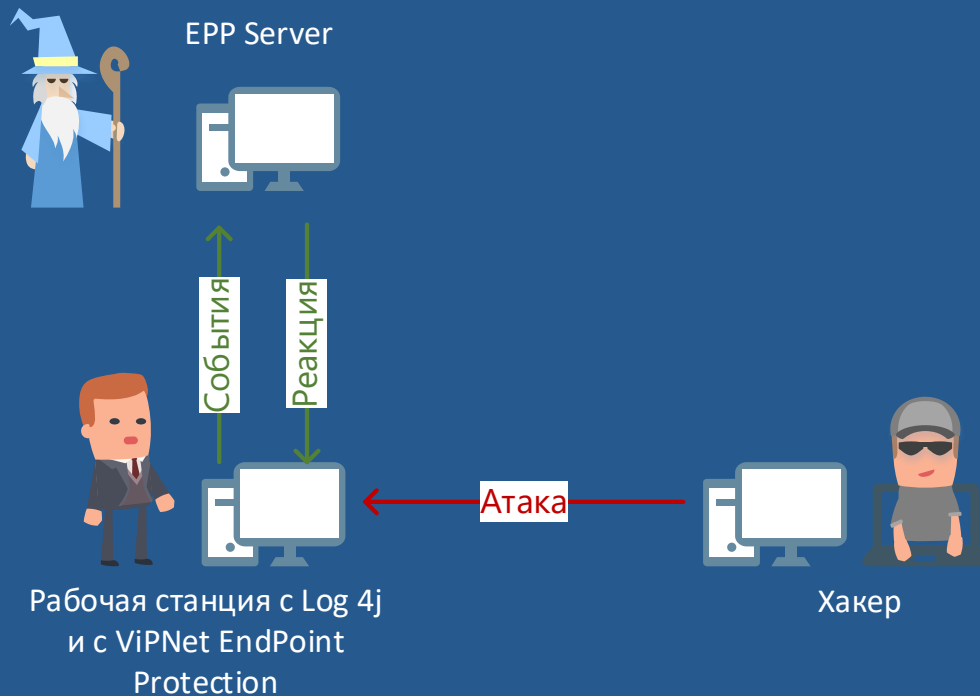
- Злоумышленник будет использовать известную уязвимость в Log4j, точнее CVE-2021-44228.
- Суть атаки – работающий Log4j позволяет запустить любую программу или команду на сервере, при помощи Java Naming and Directory Interface (JNDI).
- Запустим калькулятор через cmd.



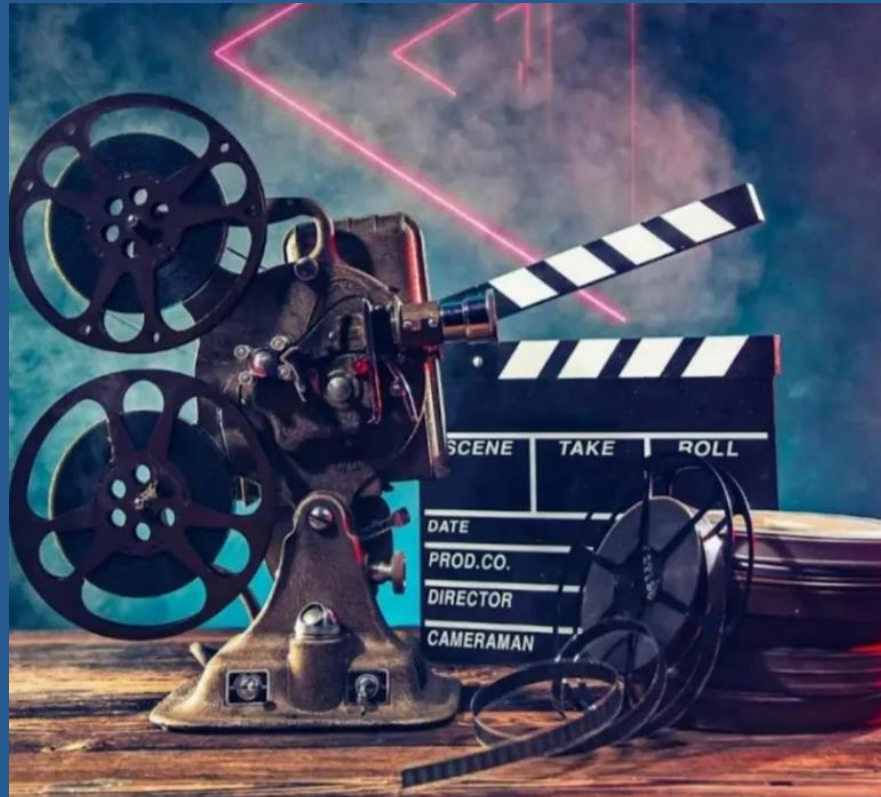
# Демонстрируем атаку!



# В инфраструктуре появился ViPNet EndPoint Protection

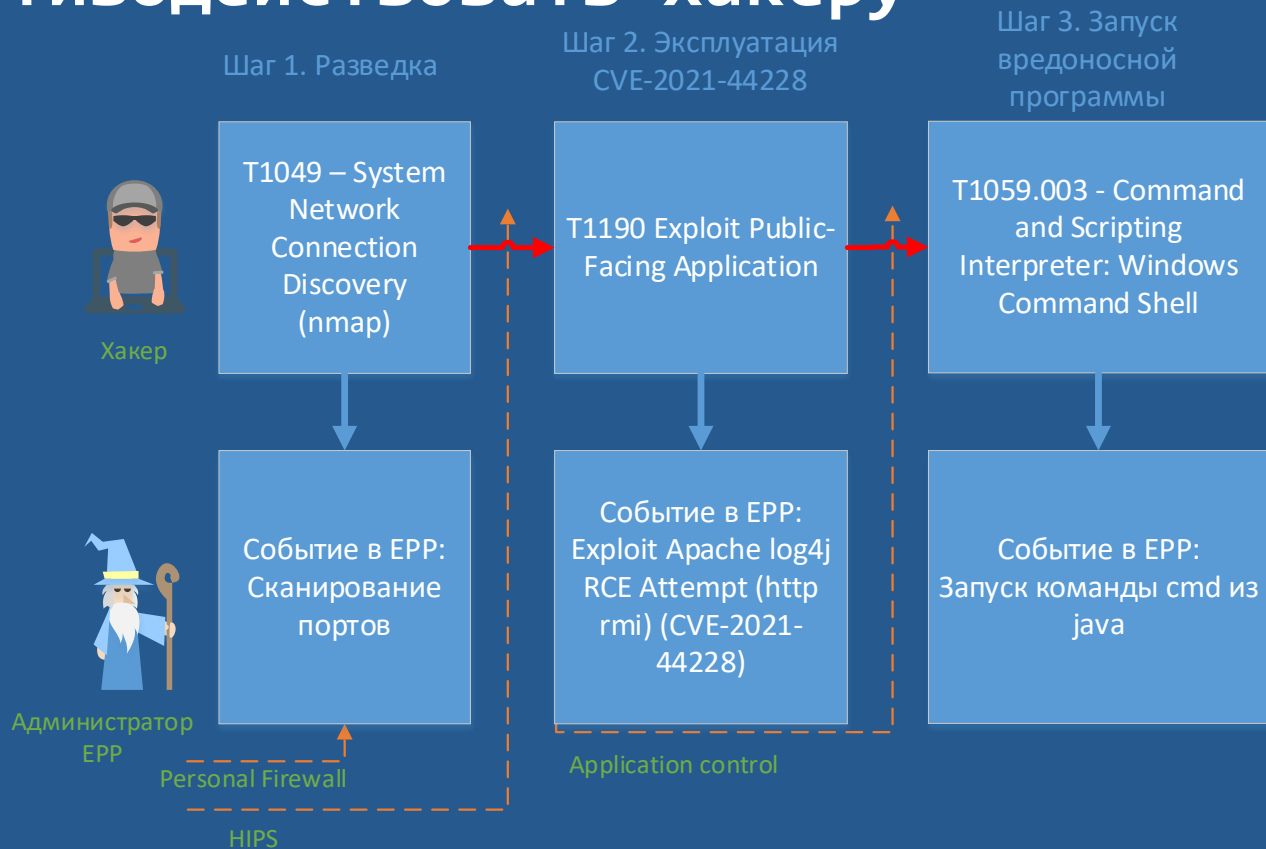


# Повторно атакуем, с включенным ViPNet EndPoint Protection





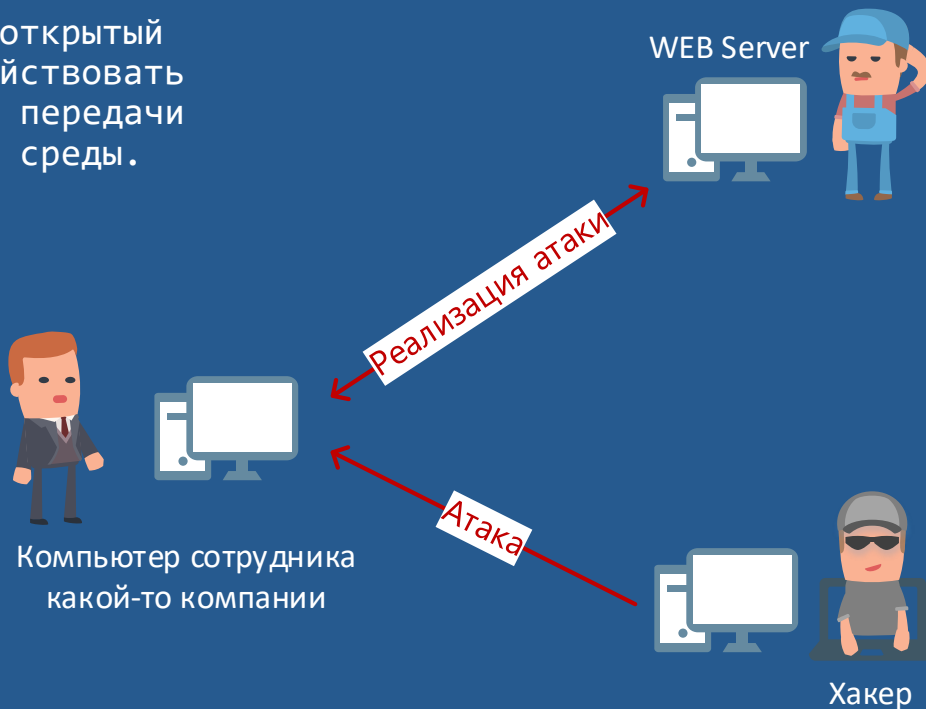
# Пошаговый разбор. Как противодействовать хакеру



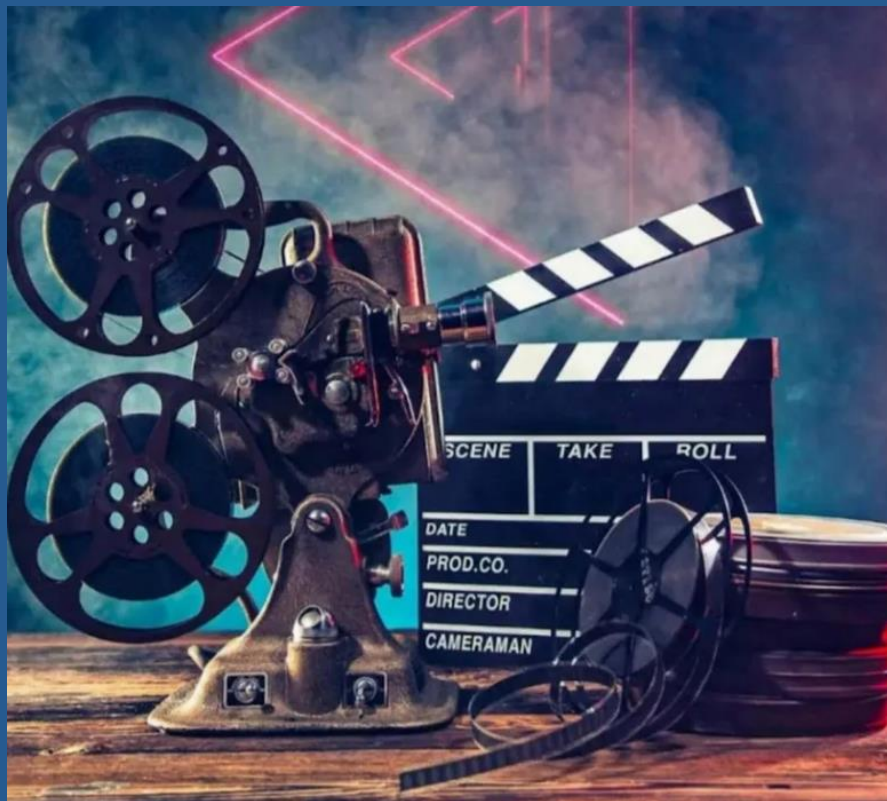
Сценарий 2.  
Загрузка вредоносной  
программы через открытый  
порт 22 (ssh)  
с использованием Resolve  
DNS.

# Что за атака?

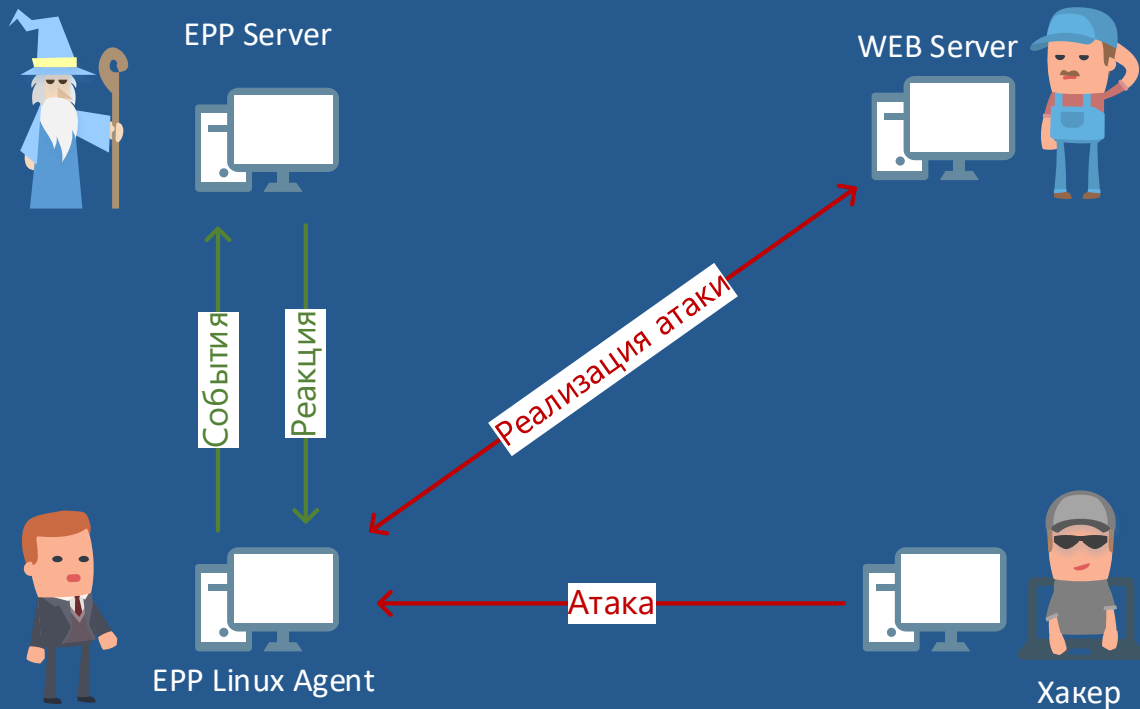
- Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб-службу для передачи данных в/из корпоративной среды.



# Демонстрируем атаку!



# В инфраструктуре появился ViPNet EndPoint Protection



# Что же должно быть включено в ЕРР?

## 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

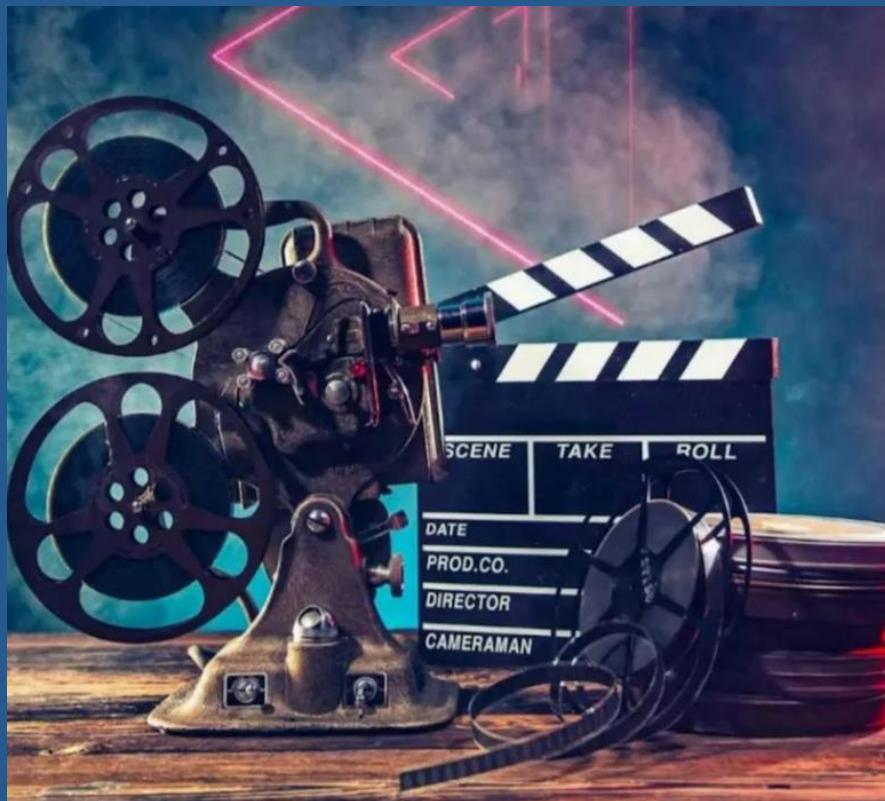
Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.



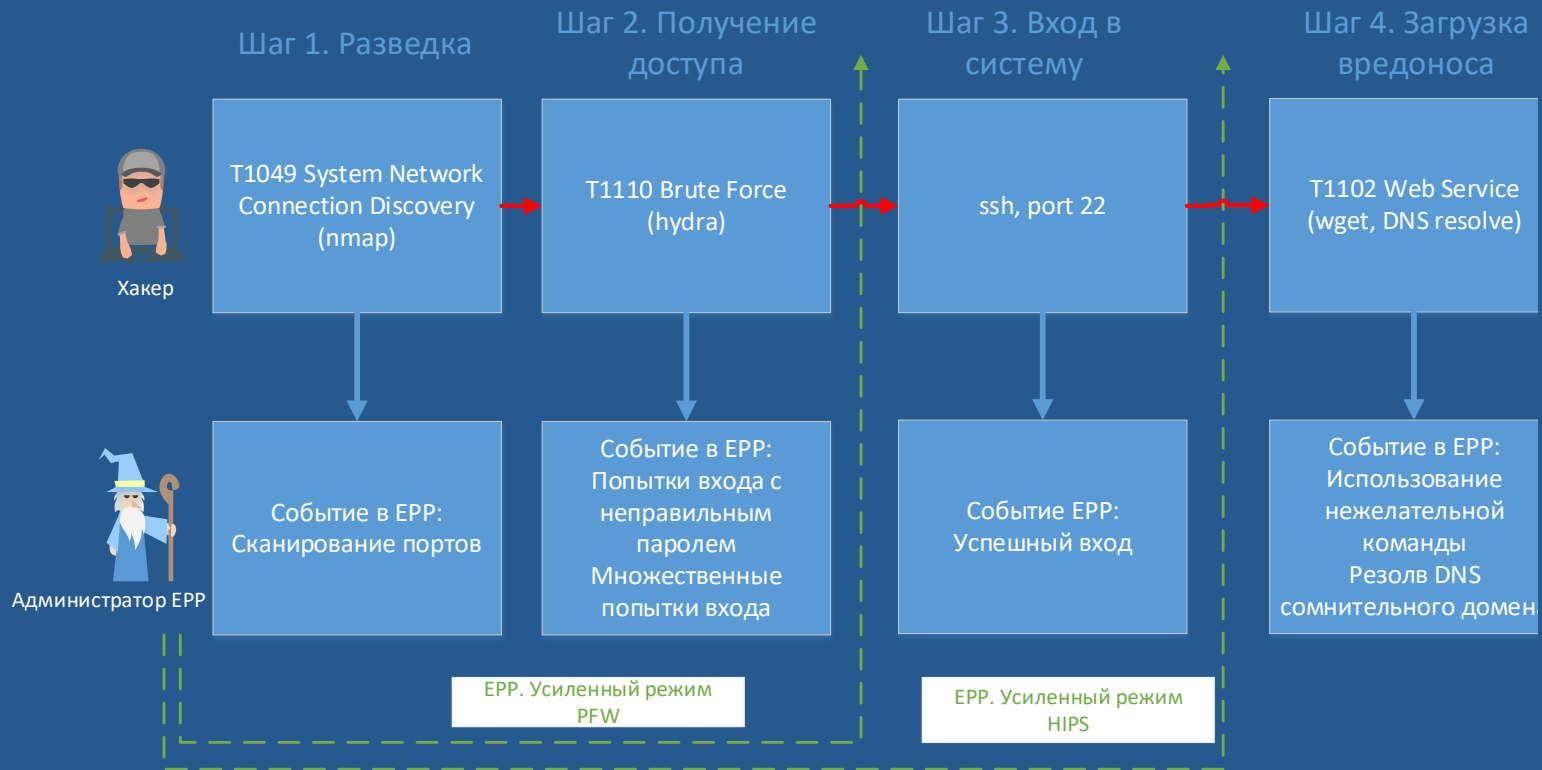
### Отключен

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

# Повторно атакуем, с включенным ViPNet EndPoint Protection



# Пошаговый разбор. Как противодействовать хакеру





# Акция «За безопасность!»

Лицензии на перечисленные продукты предоставляются на безвозмездной основе на 6 месяцев!!!

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
<ul style="list-style-type: none"><li>• ViPNet Coordinator VA</li><li>• ViPNet xFirewall VA</li><li>• ViPNet TLS Gateway VA</li><li>• ViPNet PKI Client</li><li>• ViPNet Client</li></ul>	<ul style="list-style-type: none"><li>• ViPNet Administrator</li><li>• ViPNet Policy Manager</li></ul>	<ul style="list-style-type: none"><li>• ViPNet SafeBoot</li><li>• ViPNet SafePoint</li><li>• ViPNet IDS HS*</li></ul>	<ul style="list-style-type: none"><li>• ViPNet TIAS VA</li><li>• ViPNet IDS MC VA</li><li>• ViPNet IDS NS VA</li><li>• ViPNet IDS HS*</li></ul>

*Перевод отдела технической поддержки на усиленный режим работы и предоставление консультаций по подбору оптимальных решений для обеспечения информационной безопасности в рамках импортозамещения. Для получения консультации вы можете отправить электронное письмо с вопросами и контактными данными на адрес [sos@infotecs.ru](mailto:sos@infotecs.ru).*



ТЕХНО infotecs  
2022 ФЕСТ

Спасибо  
за внимание!

---

Подписывайтесь на наши соцсети



[https://vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_news](https://t.me/infotecs_news)