

# Обнаружение и предотвращение атак при помощи ViPNet EndPoint Protection.

Разбор поведения  
злоумышленника по MITRE ATT&CK

Кадыков Иван  
Руководитель продуктового направления



техно infotecs  
2023 Фест  
ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

О чём пойдёт речь?

# «Болезни» последних шести лет





# Kill Chain

Атаку можно  
структурировать

MITRE | ATT&CK™

Adversary  
Tactics  
Techniques  
&  
Common  
Knowledge

Методология  
для специалистов ИБ

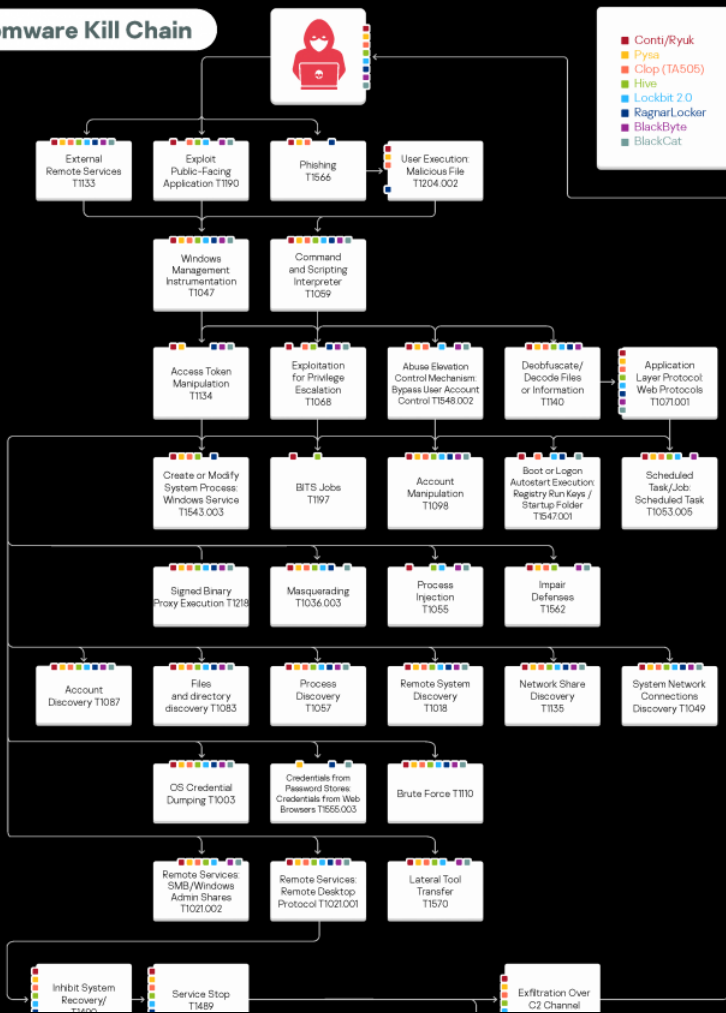
# Техники — Тактики — Процедуры

## 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 (8)	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 (8)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	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 (8)	External Remote Services	Container Command	Boot or Logon Autostart Execution (14)	Access Token Manipulation (3)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (8)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Data Manipulation (3)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forceful Authentication	Cloud Service Dashboard	Remote Services (8)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Container and Resource Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Domain Trust Discovery	Software Deployment Tools	Encrypted Channel (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Valid Accounts (4)	Trusted Relationship	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Execution Guardrails (1)	Man-in-the-Middle (2)	File and Directory Discovery	Taint Shared Content	Failback Channels	Ingress Tool Transfer	Firmware Corruption	Inhibit System Recovery
Search Open Websites/Domains (2)	Windows Management Instrumentation	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	Network Service Scanning	Use Alternate Authentication Material (4)	Multi-Stage Channels	Non-Application Layer Protocol	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Search Victim-Owned Websites			Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	Network Share Discovery		Scheduled Transfer	Non-Standard Port	Resource Hijacking	System Shutdown/Reboot
			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Hide Artifacts (7)	OS Credential Dumping (8)	Network Sniffing			Protocol Tunneling	Service Stop	
			User Execution (3)	Hijack Execution Flow (11)	Impair Defenses (7)	Hijack Execution Flow (11)	Steal Application Access Token	Peripheral Device Discovery			Proxy (4)		
			Windows Management Instrumentation	Implant Internal Image	Indicator Removal on Host (8)	Impair Defenses (7)	Steal Web Session Cookie	Password Policy Discovery			Remote Access Software		
				Modify Authentication Process (4)	Indirect Command Execution	Indirect Command Execution	Two-Factor Authentication Interception	Process Discovery			Traffic Signaling (1)		
				Office Application Startup (6)	Masquerading (8)	Masquerading (8)	Unsecured Credentials (7)	Query Registry			Web Service (3)		
				Pre-OS Boot (3)	Modify Authentication Process (4)	Modify Authentication Process (4)		Remote System Discovery					
				Scheduled Task/Job (7)	Modify Cloud Compute Infrastructure (6)	Modify Cloud Compute Infrastructure (6)		Software Discovery (1)					
				Server Software Component (3)	Modify Registry	Modify Registry		System Information Discovery					
				Traffic Signaling (1)	Modify System Image (2)	Modify System Image (2)		System Location Discovery					
					Network's Boundaries	Network's Boundaries		System Network Configuration					

## Ransomware Kill Chain



# Тактики, техники и процедуры Ransomware группировок

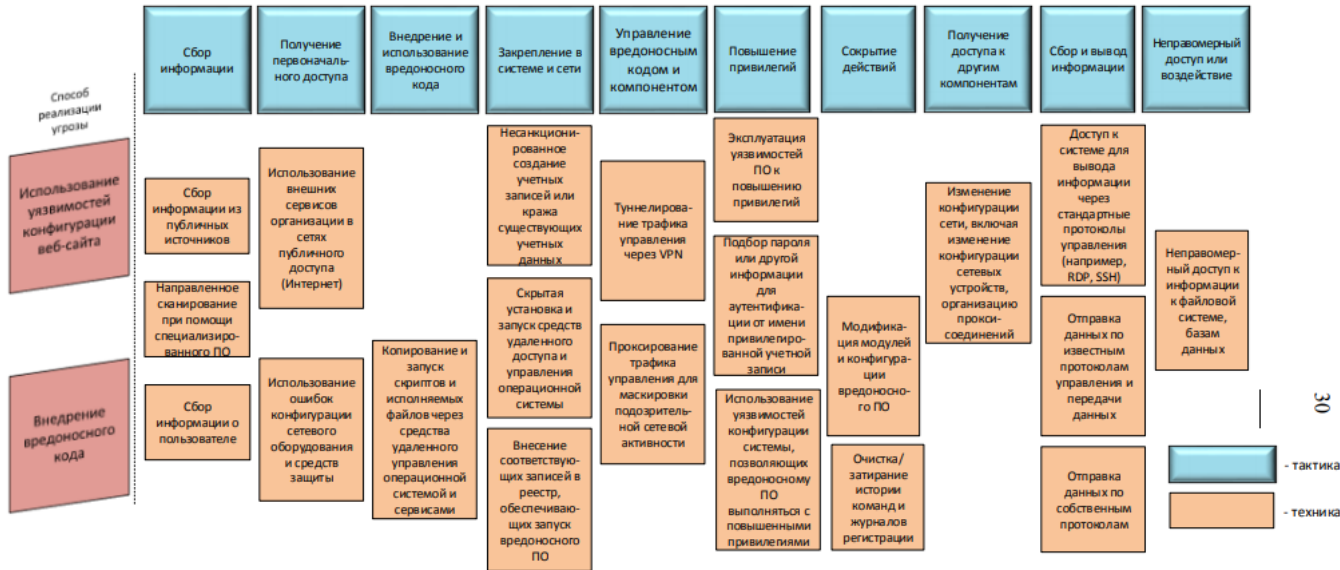
Исследования АО «Лаборатория  
Касперского»

Изображение взято с <https://securelist.ru/modern-ransomware-groups-ttps/105553/> По ссылке можно получить полный отчёт.

# «Методика оценки угроз безопасности информации».

## ФСТЭК России

Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию

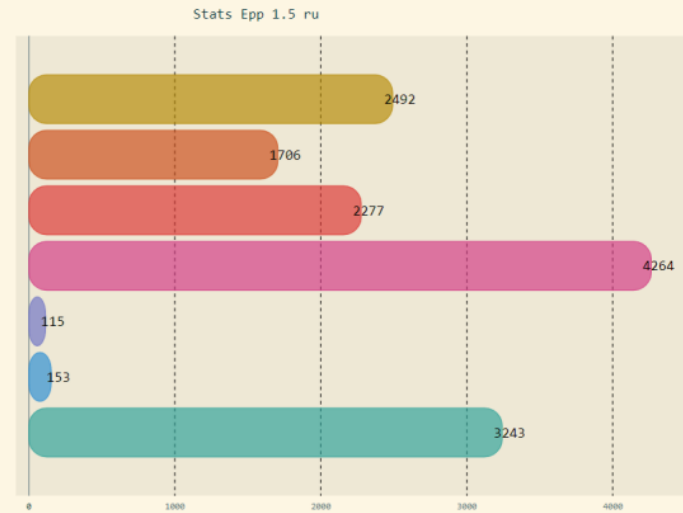




# VIPNet EndPoint Protection

## Контроль приложений

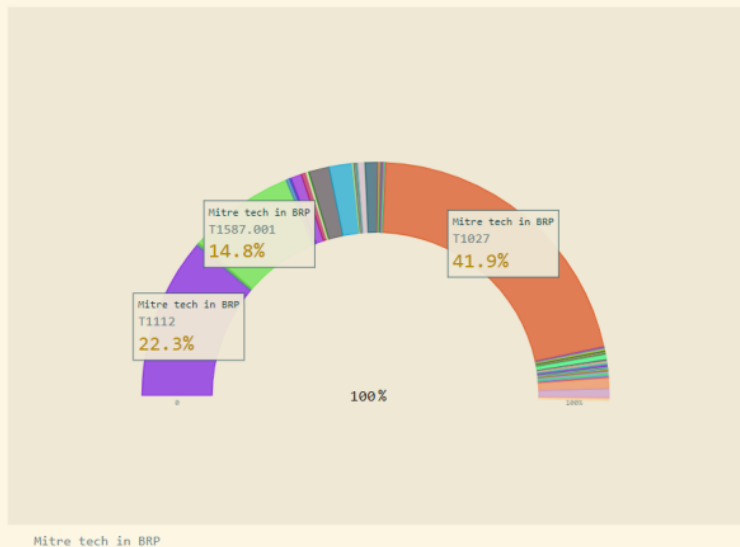




## Небольшая статистика

### БРП:

- Регулярно обновляем
- Актуализируем правила
- Обновляем информацию по уязвимостям





# Давайте попрактикуемся

**Продукт:**

ViPNet EndPoint Protection

**Знания:**

MITRE ATT&CK

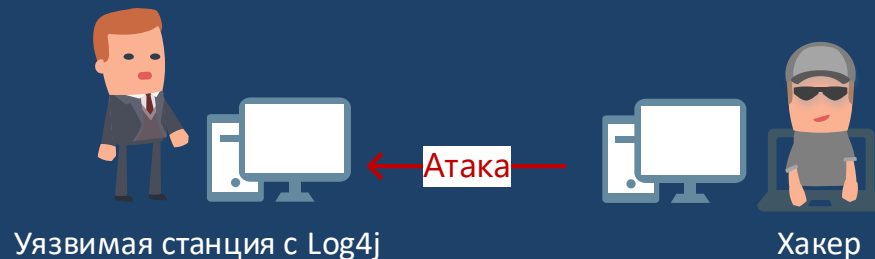
# ВАЖНО!

- 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! 😊 😊 😊

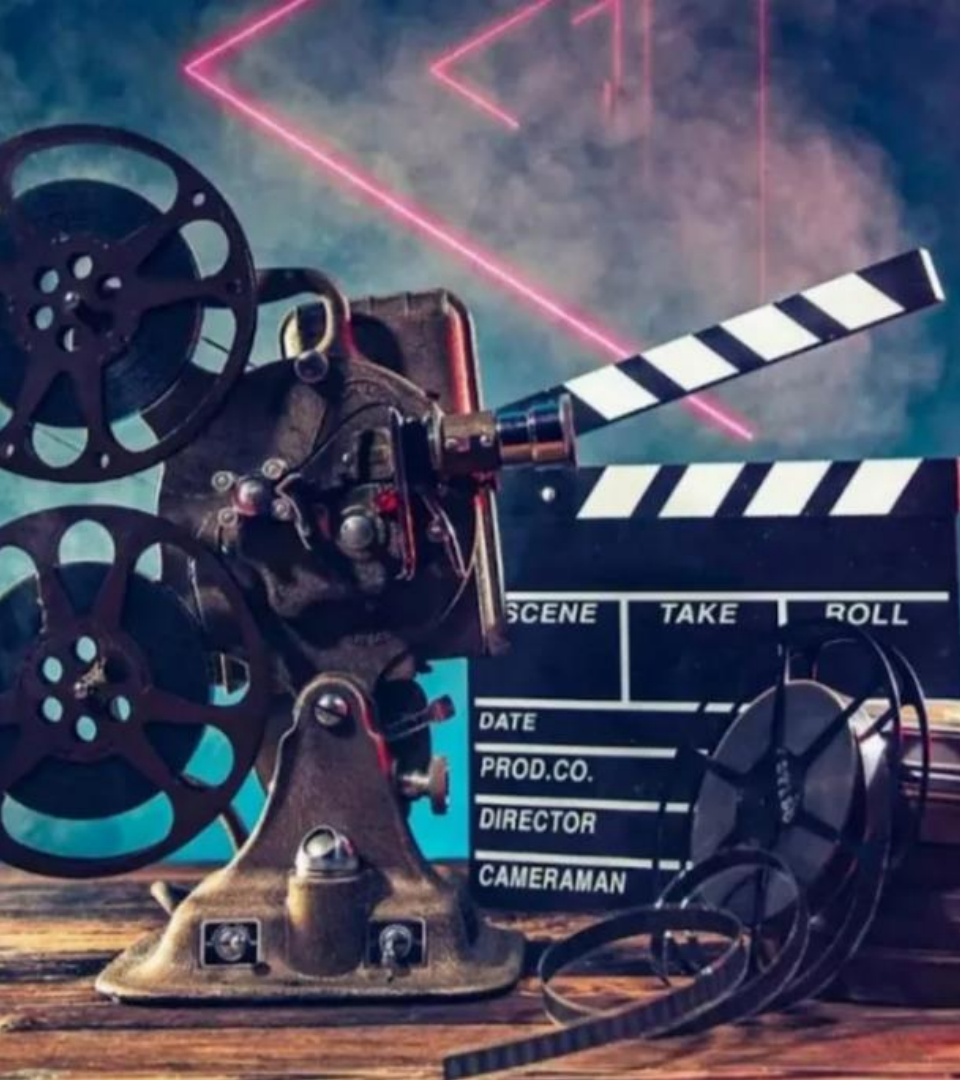


# Сценарий 1. Атака через уязвимость в Log4j. Запуск произвольного кода или приложения

# Что за атака?

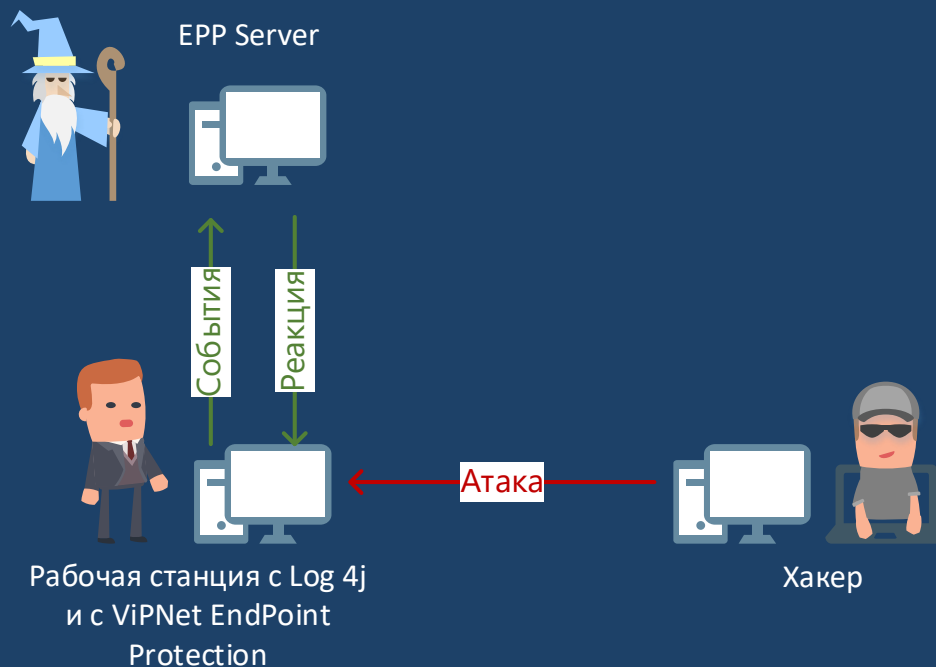


- Злоумышленник будет использовать известную уязвимость в Log4j, точнее CVE-2021-44228
- Суть атаки – работающий Log4j позволяет запустить любую программу или команду на сервере, при помощи Java Naming and Directory Interface (JNDI)
- Запустим калькулятор через cmd



Демонстрируем атаку!

# В инфраструктуре появился ViPNet EndPoint Protection

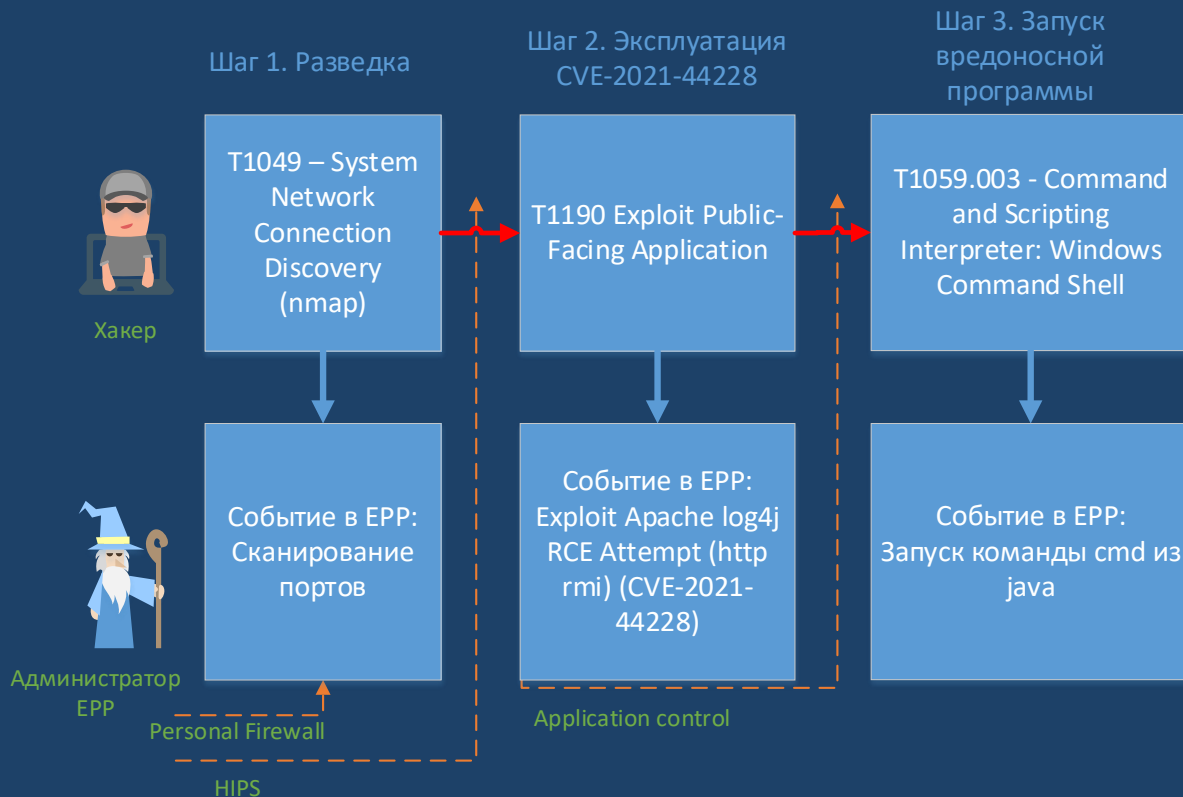






Повторно атакуем,  
с включенным  
ViPNet EndPoint  
Protection

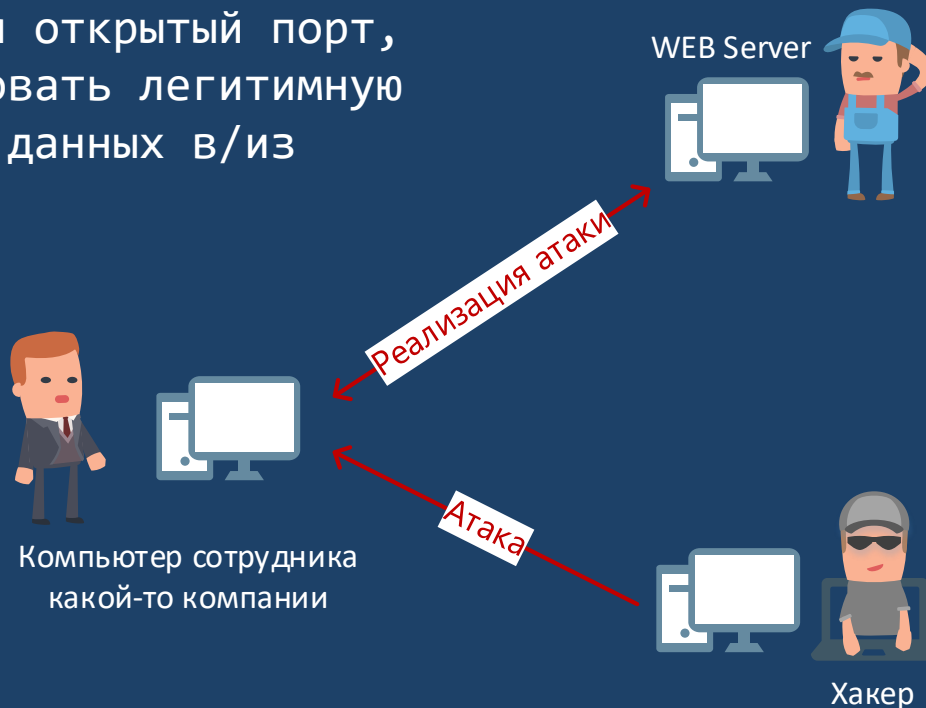
# Пошаговый разбор. Как противодействовать хакеру

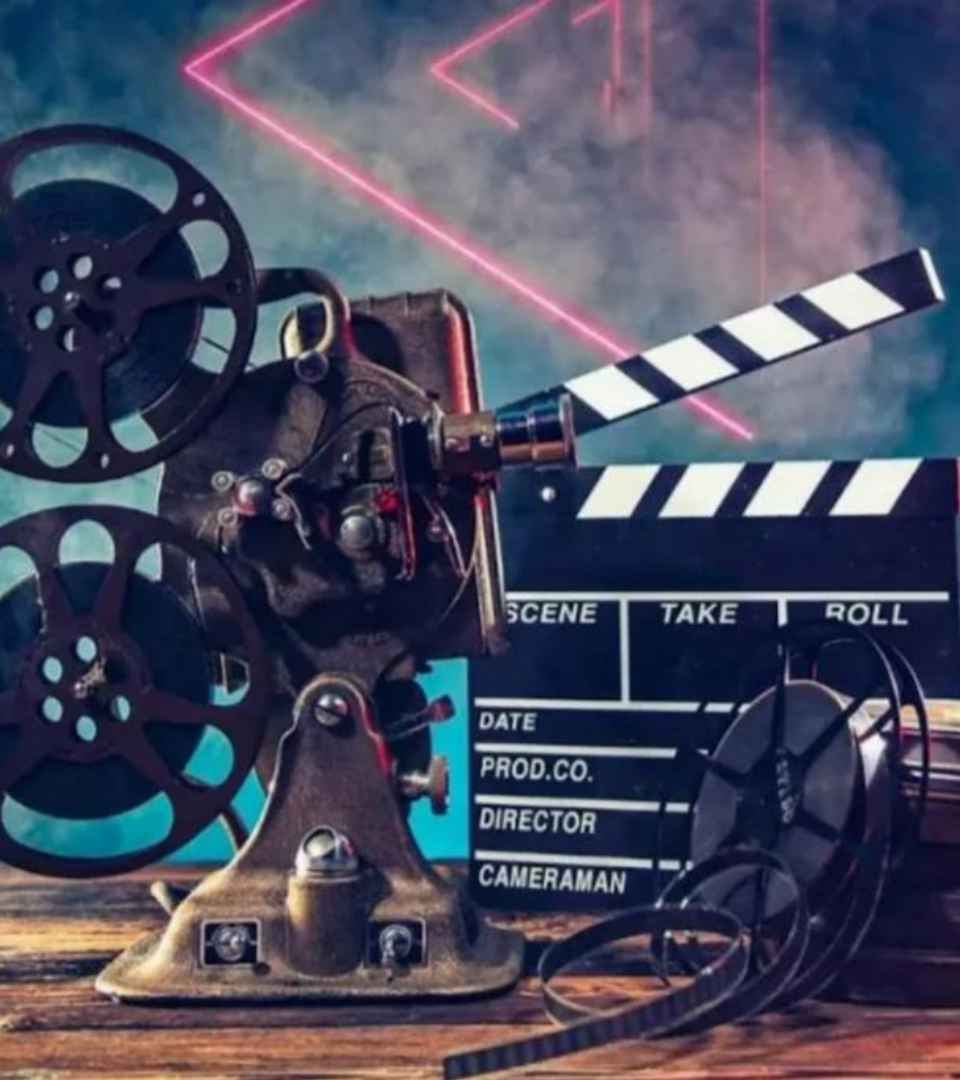


**Сценарий 2.  
Загрузка вредоносной  
программы через  
открытый порт 22 (ssh)  
с использованием  
Resolve DNS.**

# Что за атака?

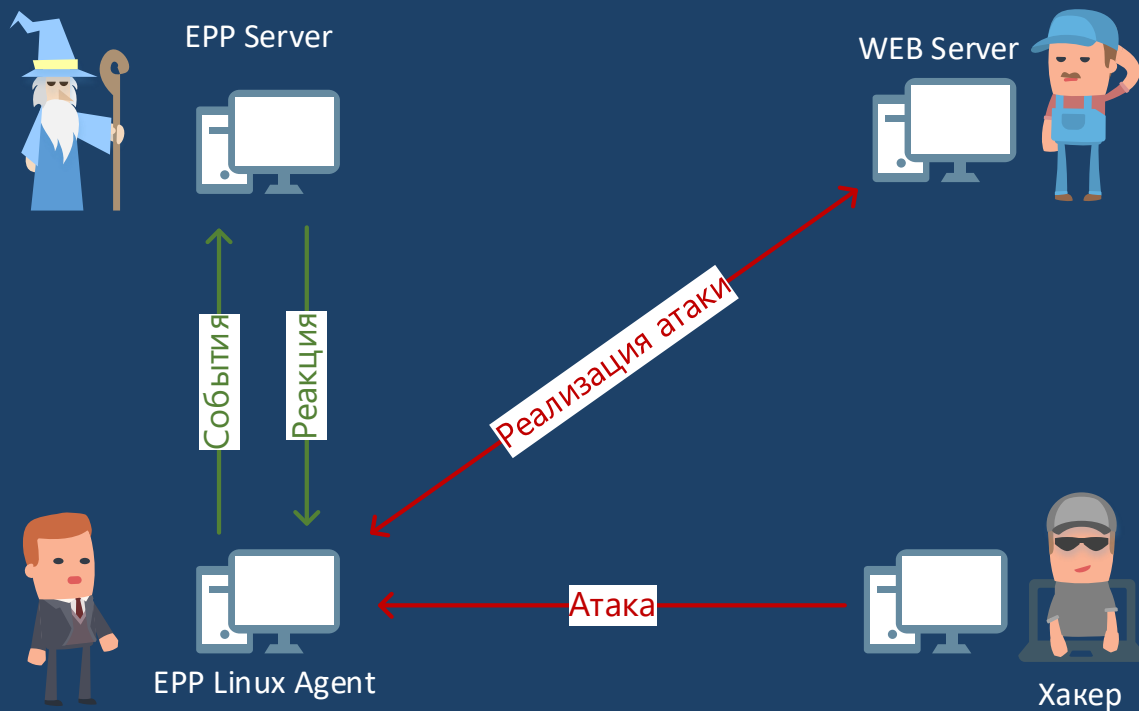
Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб-службу для передачи данных в/из корпоративной среды.





Демонстрируем атаку!

# В инфраструктуре появился ViPNet EndPoint Protection



# Что же должно быть включено в 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.



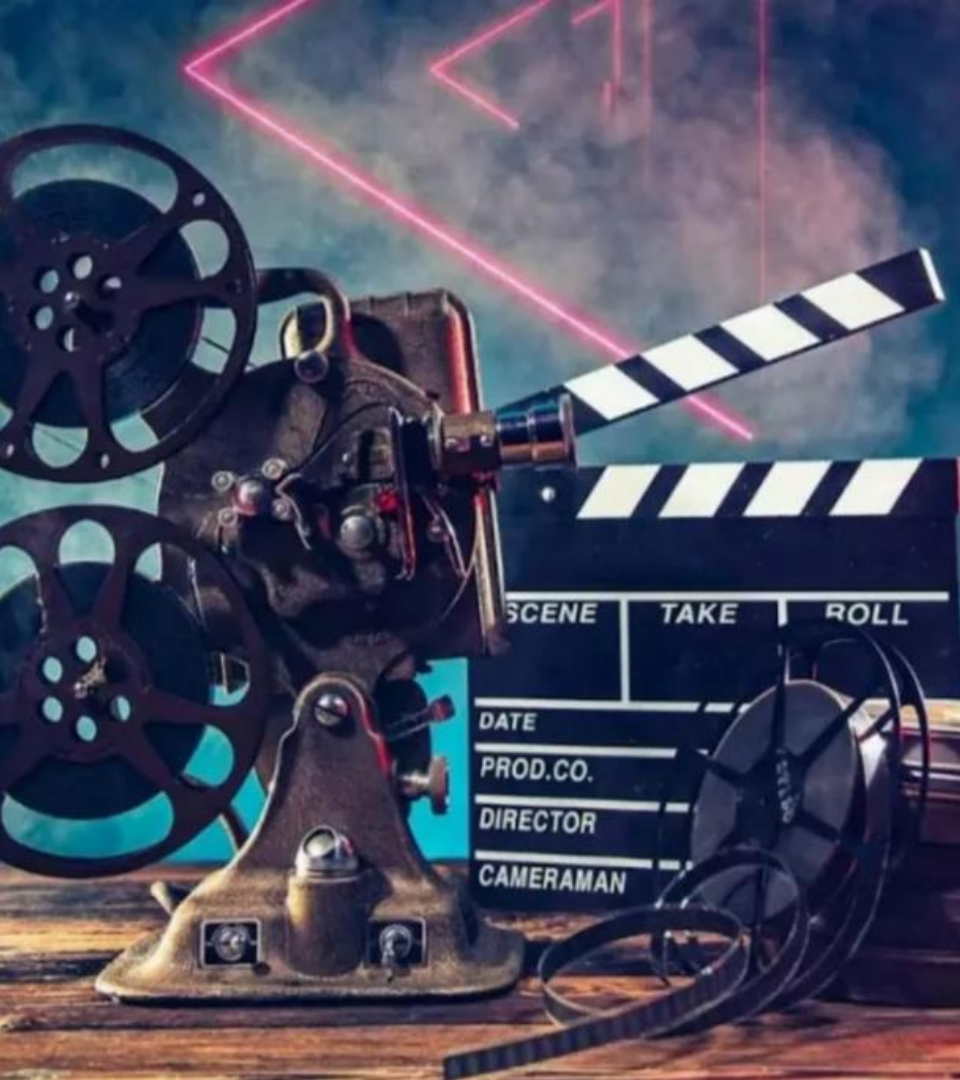
### Минимальный

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



### Отключен

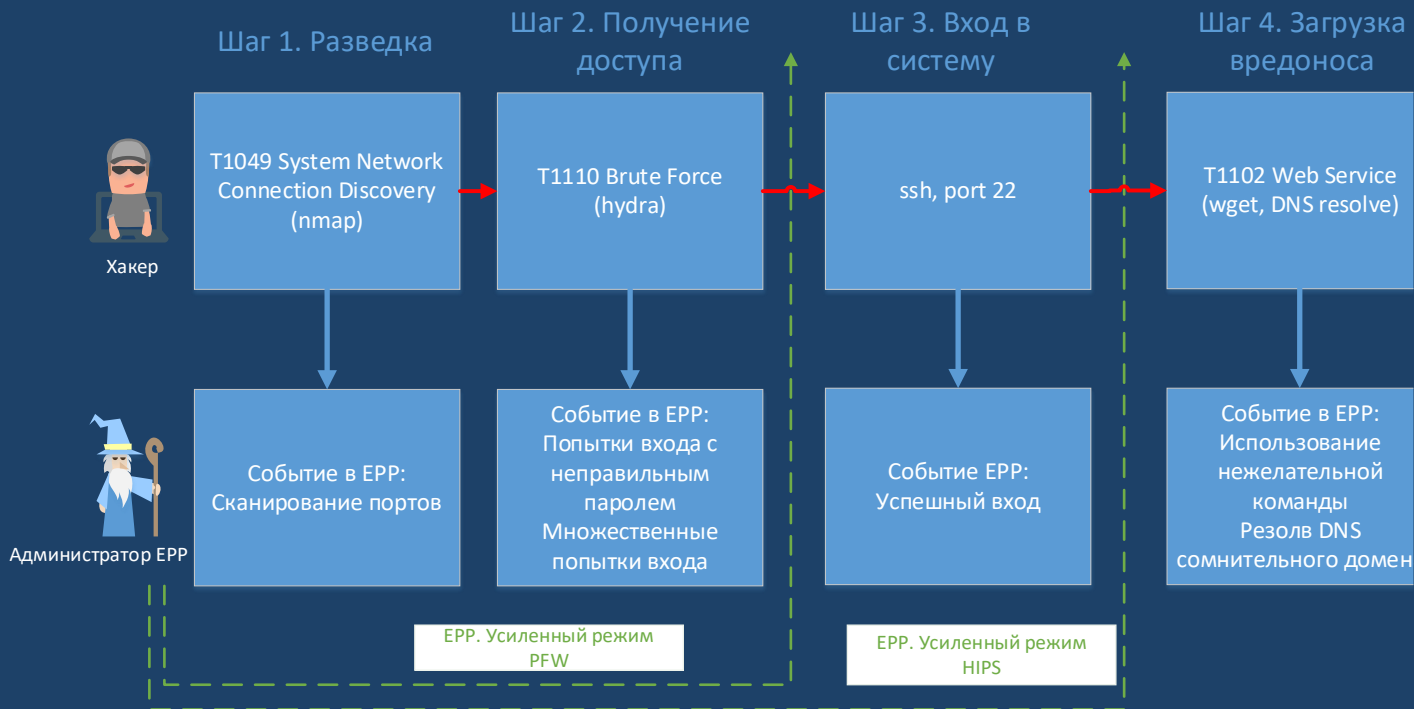
Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.



Повторно  
атакуем,  
с включенным  
ViPNet EndPoint  
Protection



# Пошаговый разбор. Как противодействовать хакеру





Спасибо  
за внимание!

---

Подписывайтесь на наши соцсети



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



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)