

# 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

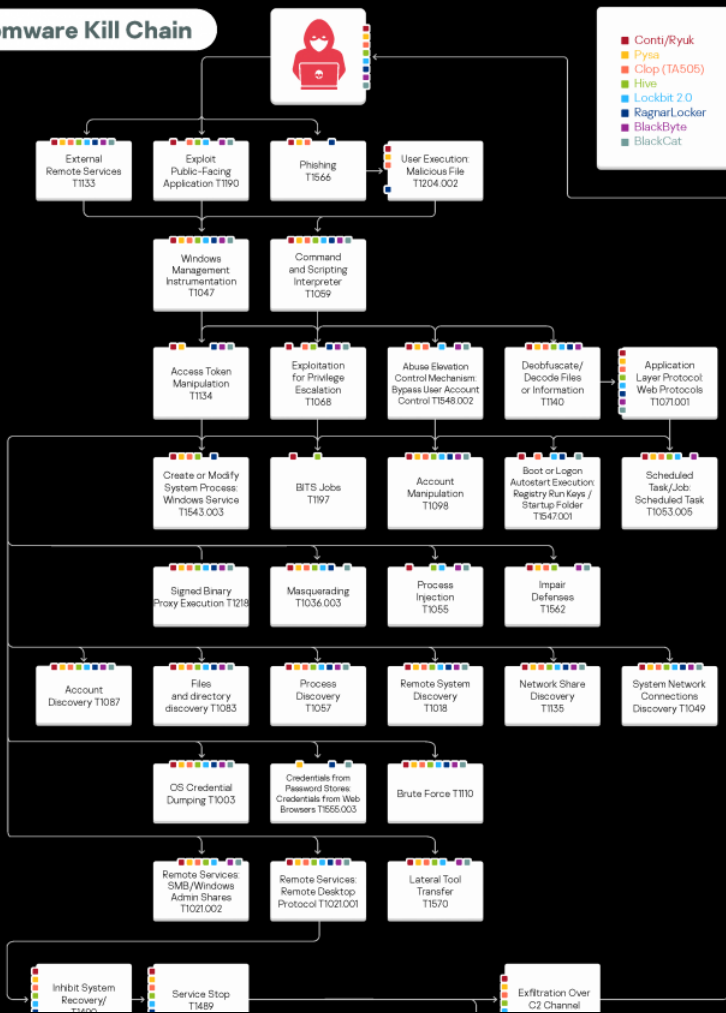
# Техники – Тактики – Процедуры

## 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)	Build Image on Host	Build Image on Host	Exploitation for Credential Access	Browser Bookmark Discovery	Remote Service Session Hijacking (2)	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 (3)	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Services (8)	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 (3)	Deploy Container	Deploy Container	Forceful Authentication	Cloud Service Dashboard	Forge Web Credentials (2)	Data from Configuration Repository (2)	Data from Other Network Medium (1)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Inter-Process Communication (2)	Create or Modify System Process (4)	Direct Volume Access	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Discovery	Input Capture (4)	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (3)	Native API	Domain Policy Modification (2)	Execution Guardrails (1)	Execution Guardrails (1)	Man-in-the-Middle (2)	Container and Resource Discovery	Man-in-the-Middle (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)	Disk Wipe (2)
Search Open Technical Databases (3)	Valid Accounts (4)	Trusted Relationship	Scheduled Task/Job (7)	Event Triggered Execution (15)	Escape to Host	Escape to Host	Modify Authentication Process (4)	Domain Trust Discovery	Modify Authentication Process (4)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption	Inhibit System Recovery
Search Open Websites/Domains (2)	Windows Management Instrumentation	Valid Accounts (4)	Shared Modules	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)	Resource Hijacking
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Non-Application Layer Protocol	Transfer Data to Cloud Account	Service Stop	System Shutdown/Reboot
			System Services (2)	Hijack Execution Flow (11)	Impair Defenses (7)	Impair Defenses (7)	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Non-Standard Port		Service Stop	System Shutdown/Reboot
			User Execution (3)	Implant Internal Image	Indicator Removal on Host (8)	Indicator Removal on Host (8)	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Protocol Tunneling		Service Stop	System Shutdown/Reboot
			Valid Accounts (4)	Modify Authentication Process (4)	Indirect Command Execution	Indirect Command Execution	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Proxy (4)		Service Stop	System Shutdown/Reboot
			Windows Management Instrumentation	Office Application Startup (6)	Masquerading (8)	Masquerading (8)	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Remote Access Software		Service Stop	System Shutdown/Reboot
				Pre-OS Boot (3)	Modify Authentication Process (4)	Modify Authentication Process (4)	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Traffic Signaling (1)		Service Stop	System Shutdown/Reboot
				Scheduled Task/Job (7)	Modify Cloud Compute Infrastructure (6)	Modify Cloud Compute Infrastructure (6)	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Web Service (3)		Service Stop	System Shutdown/Reboot
				Server Software Component (3)	Modify Registry	Modify Registry	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)			Service Stop	System Shutdown/Reboot
				Traffic Signaling (1)	Modify System Image (2)	Modify System Image (2)	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)			Service Stop	System Shutdown/Reboot
					Network Boundaries	Network Boundaries	Network Sniffing	File and Directory Permissions Modification (2)	OS Credential Dumping (8)			Service Stop	System Shutdown/Reboot

## Ransomware Kill Chain



# Тактики, техники и процедуры Ransomware группировок

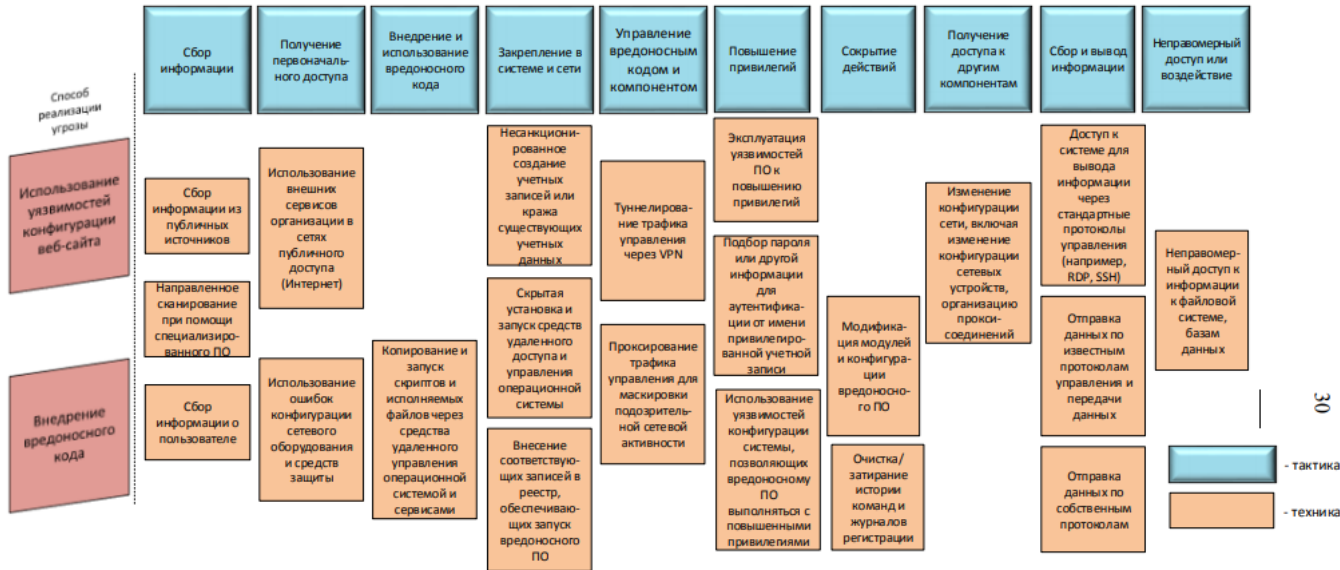
Исследования АО «Лаборатория  
Касперского»

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

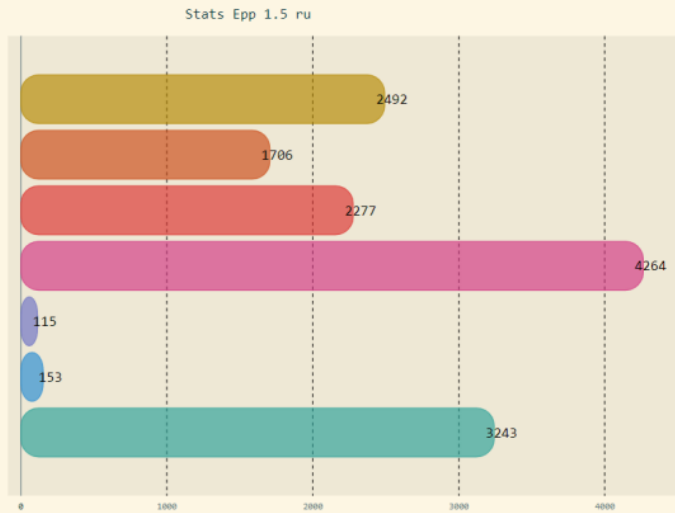




# VIPNet EndPoint Protection

## Контроль приложений

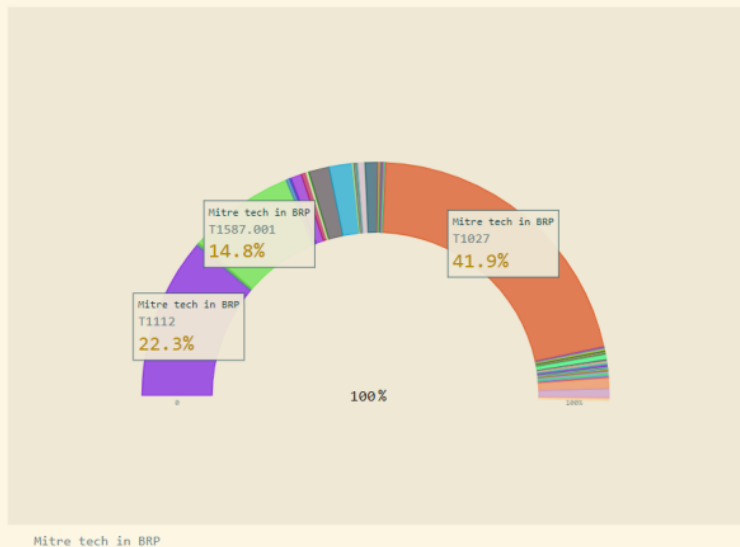




## Небольшая статистика

### БРП:

- Регулярно обновляем
- Актуализируем правила
- Обновляем информацию по уязвимостям





# Давайте попрактикуемся

**Продукт:**

ViPNet EndPoint Protection

**Знания:**

MITRE ATT&CK

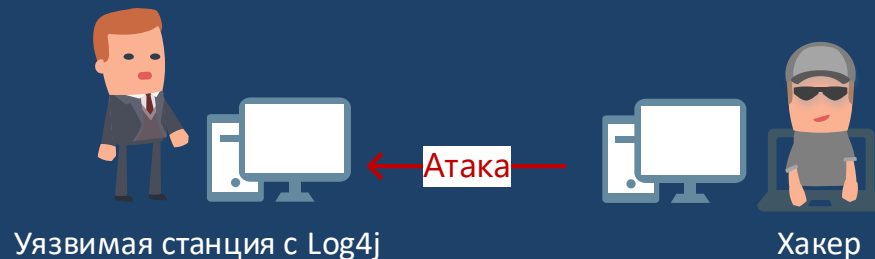
# ВАЖНО!

- 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! 😊 😊 😊

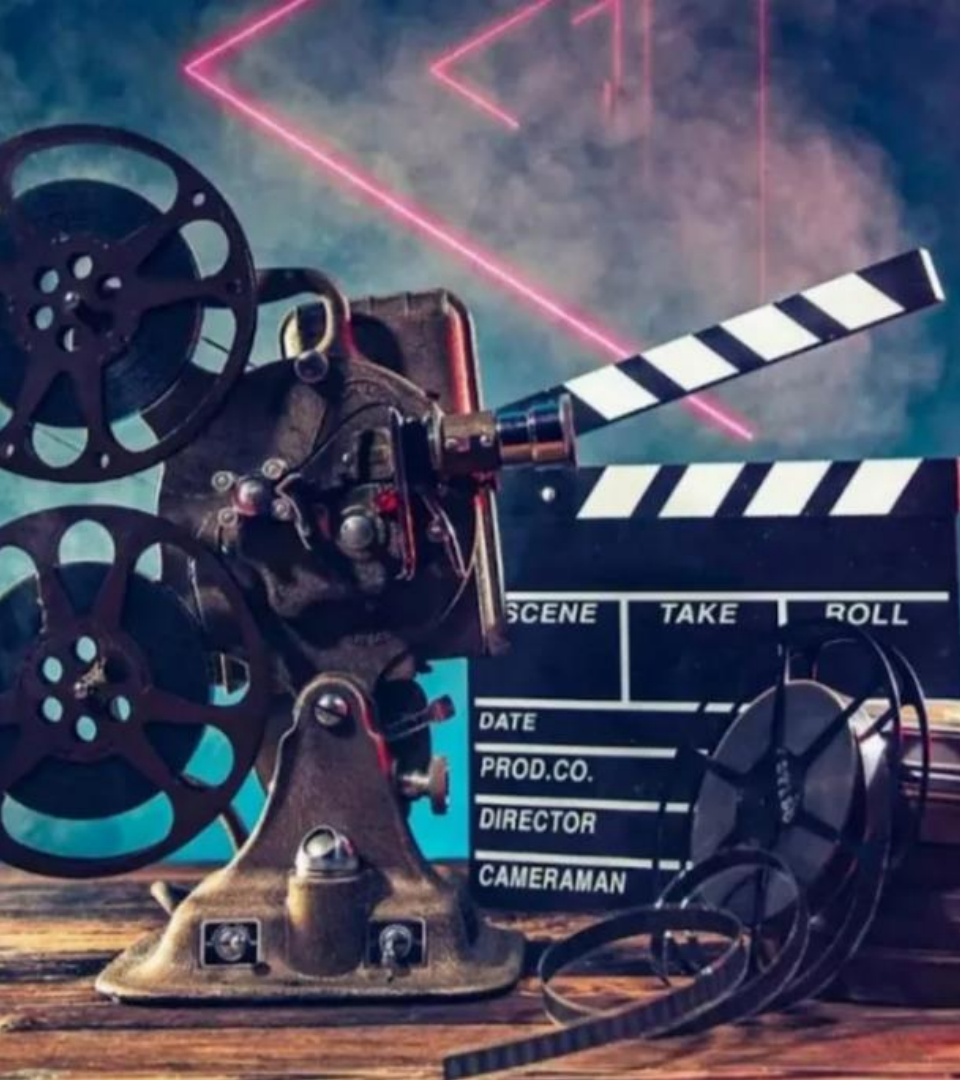


# Сценарий 1. Атака через уязвимость в Log4j. Запуск произвольного кода или приложения

# Что за атака?

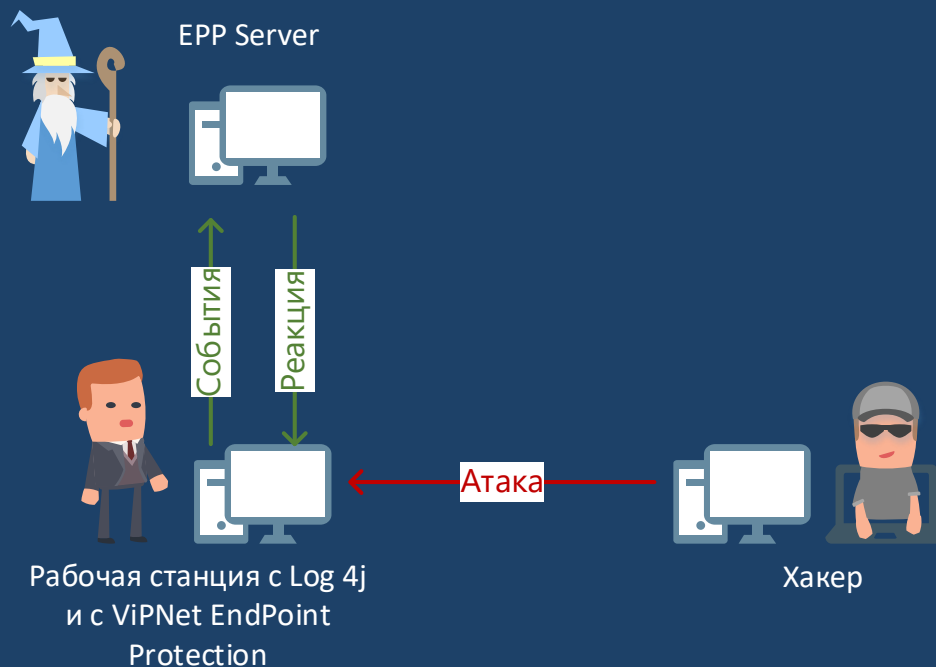


- Злоумышленник будет использовать известную уязвимость в Log4j, точнее CVE-2021-44228
- Суть атаки – работающий Log4j позволяет запустить любую программу или команду на сервере, при помощи Java Naming and Directory Interface (JNDI)
- Запустим калькулятор через cmd



Демонстрируем атаку!

# В инфраструктуре появился ViPNet EndPoint Protection

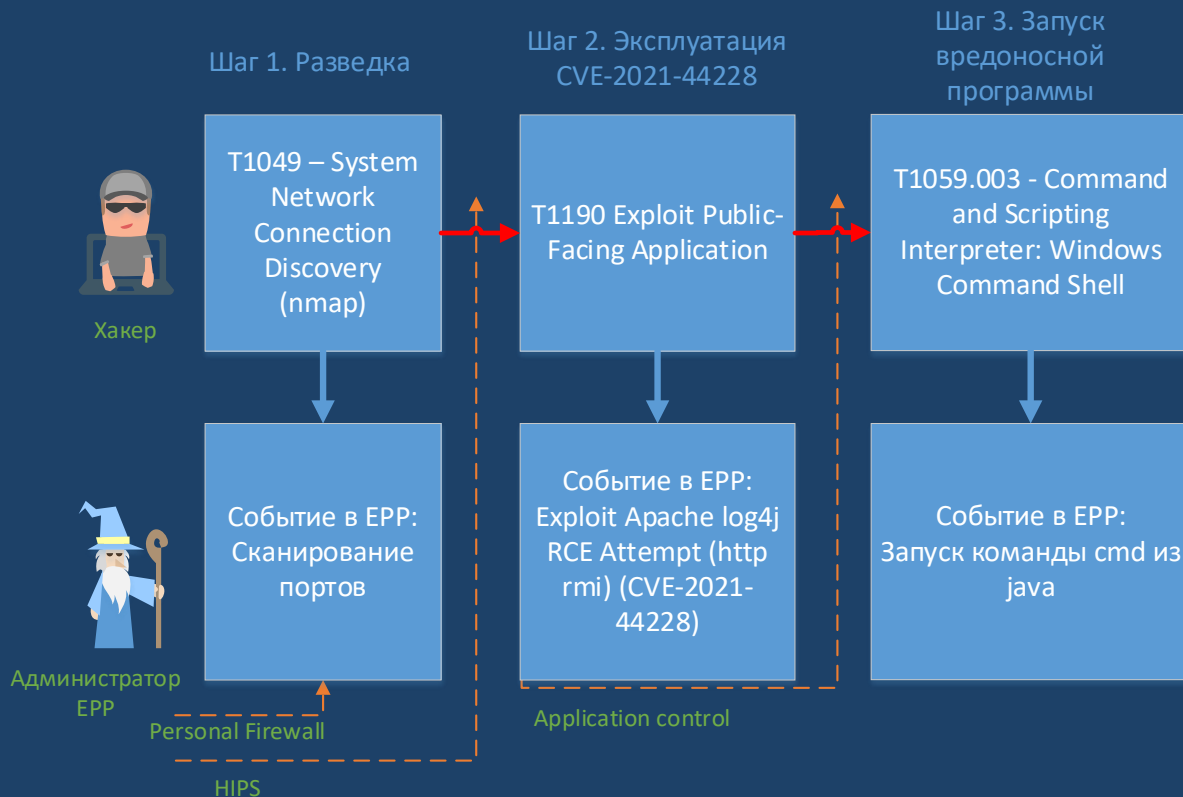






Повторно атакуем,  
с включенным  
ViPNet EndPoint  
Protection

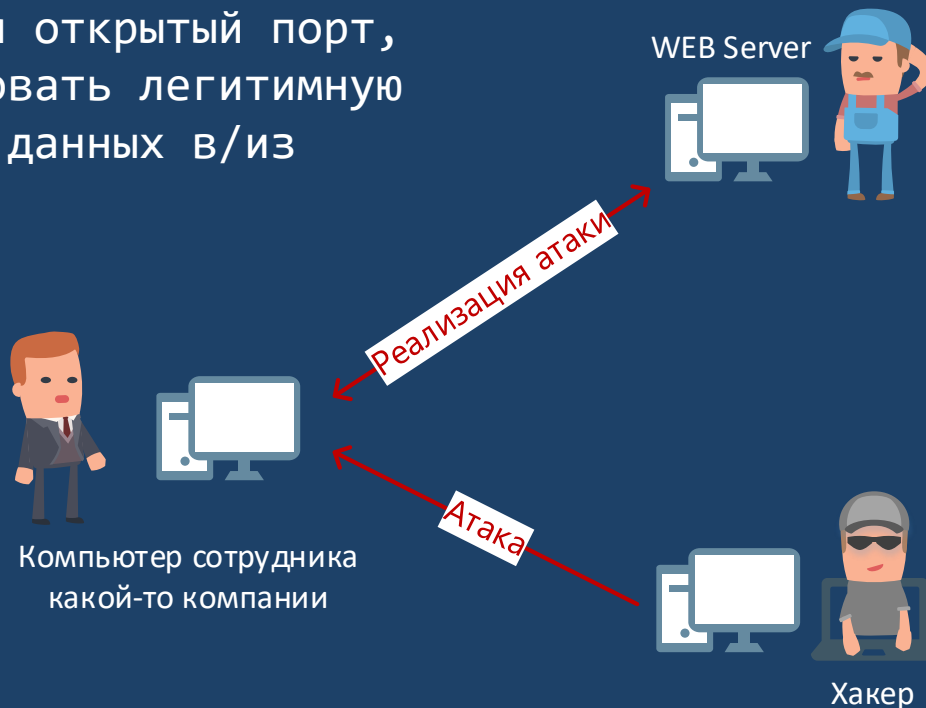
# Пошаговый разбор. Как противодействовать хакеру

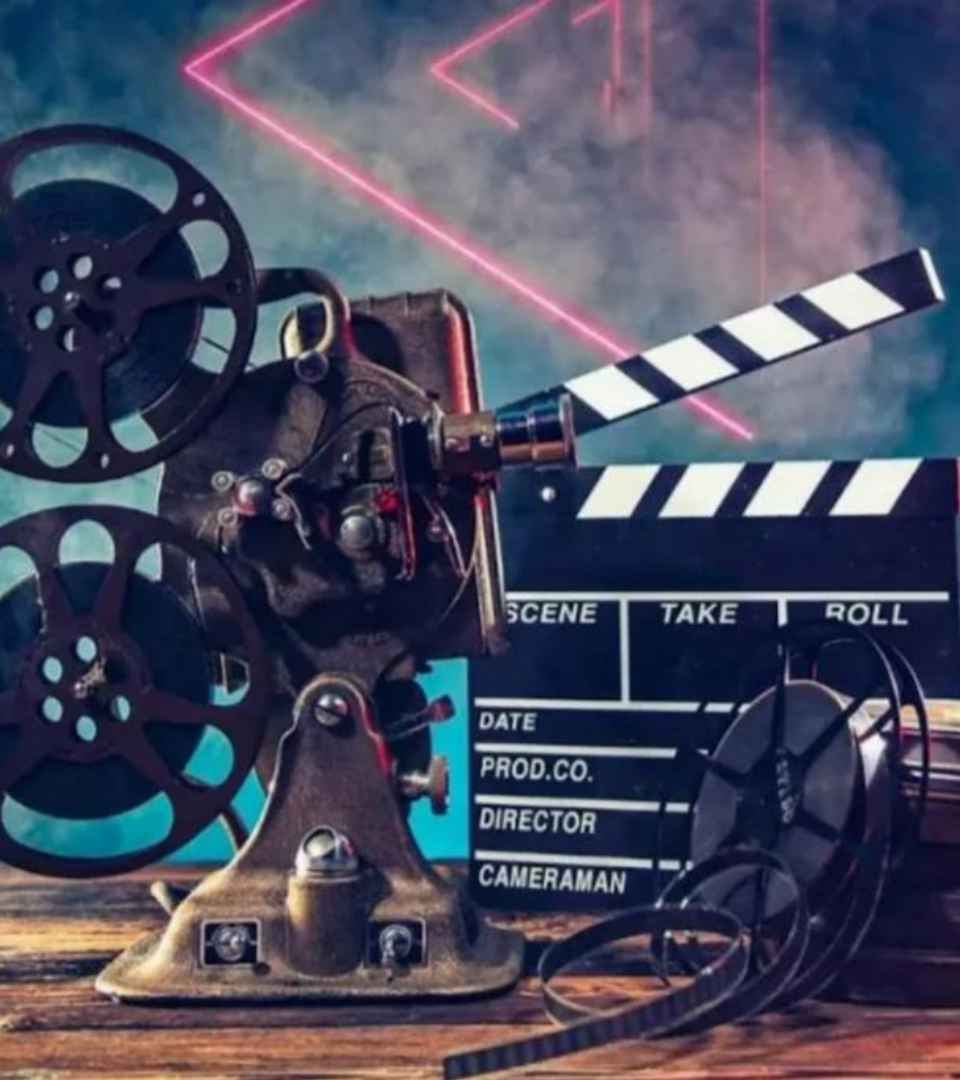


**Сценарий 2.  
Загрузка вредоносной  
программы через  
открытый порт 22 (ssh)  
с использованием  
Resolve DNS.**

# Что за атака?

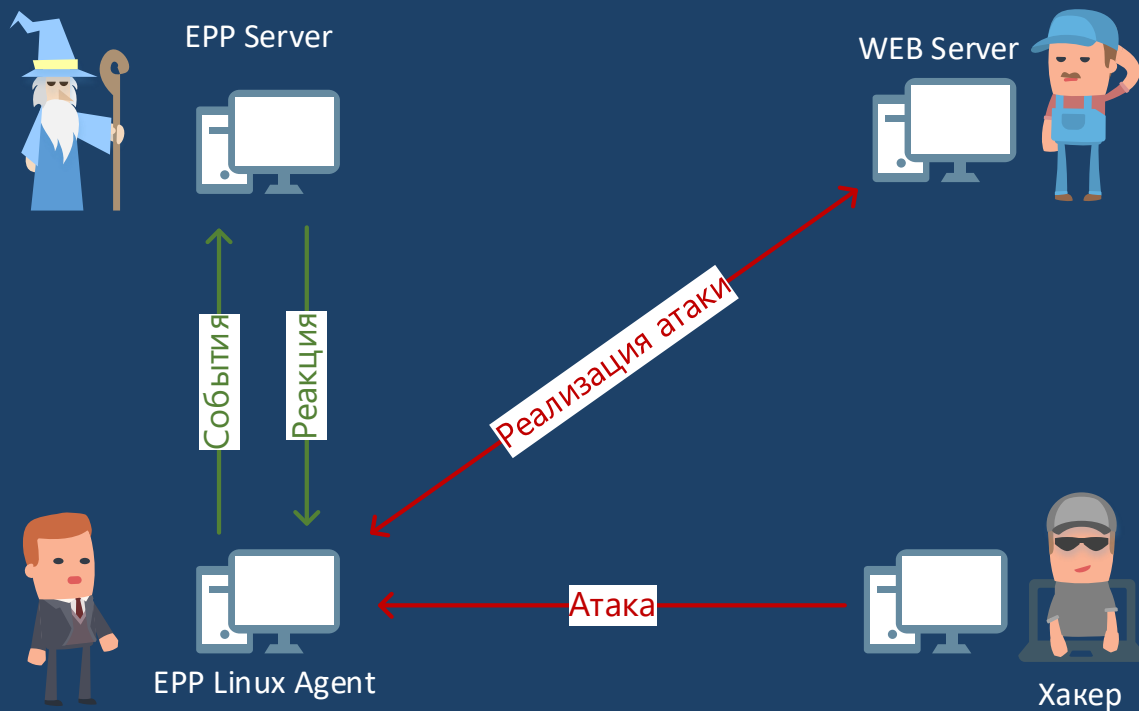
Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб-службу для передачи данных в/из корпоративной среды.





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.



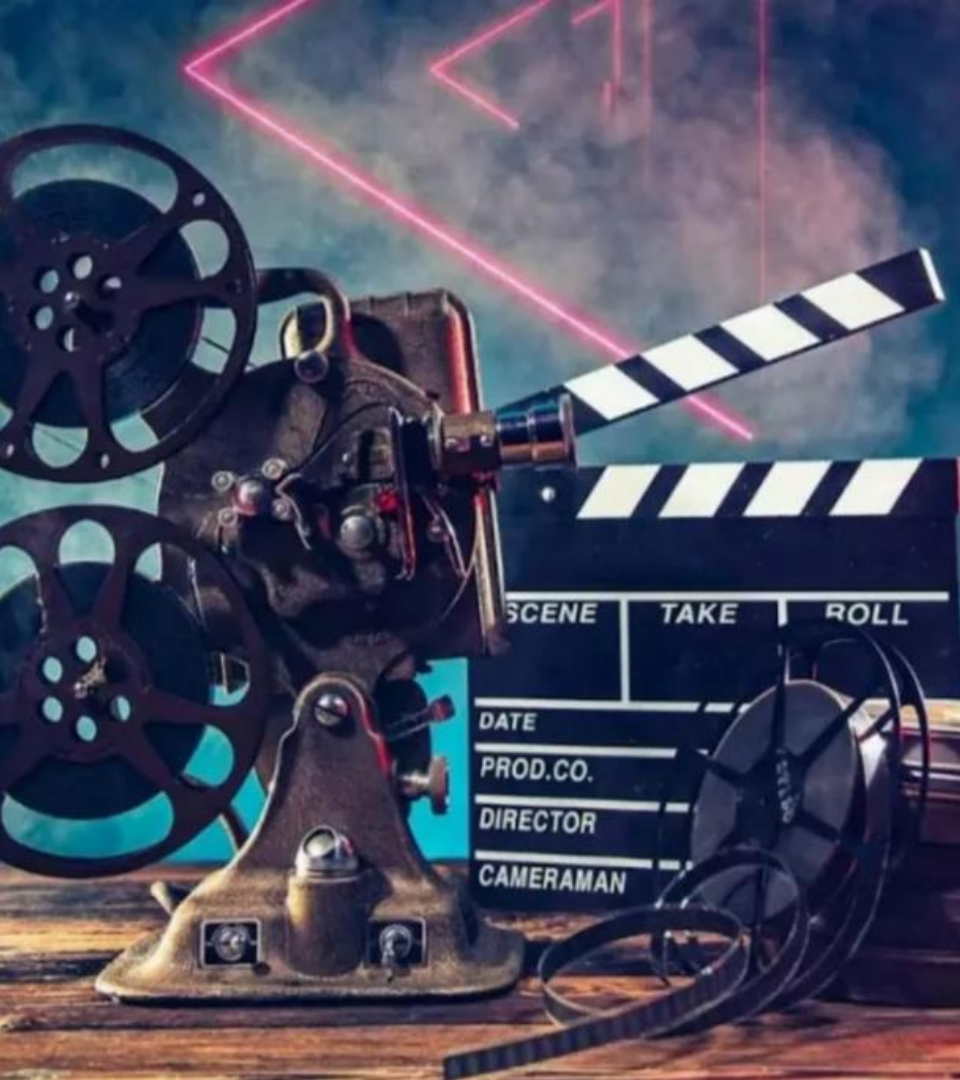
### Минимальный

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



### Отключен

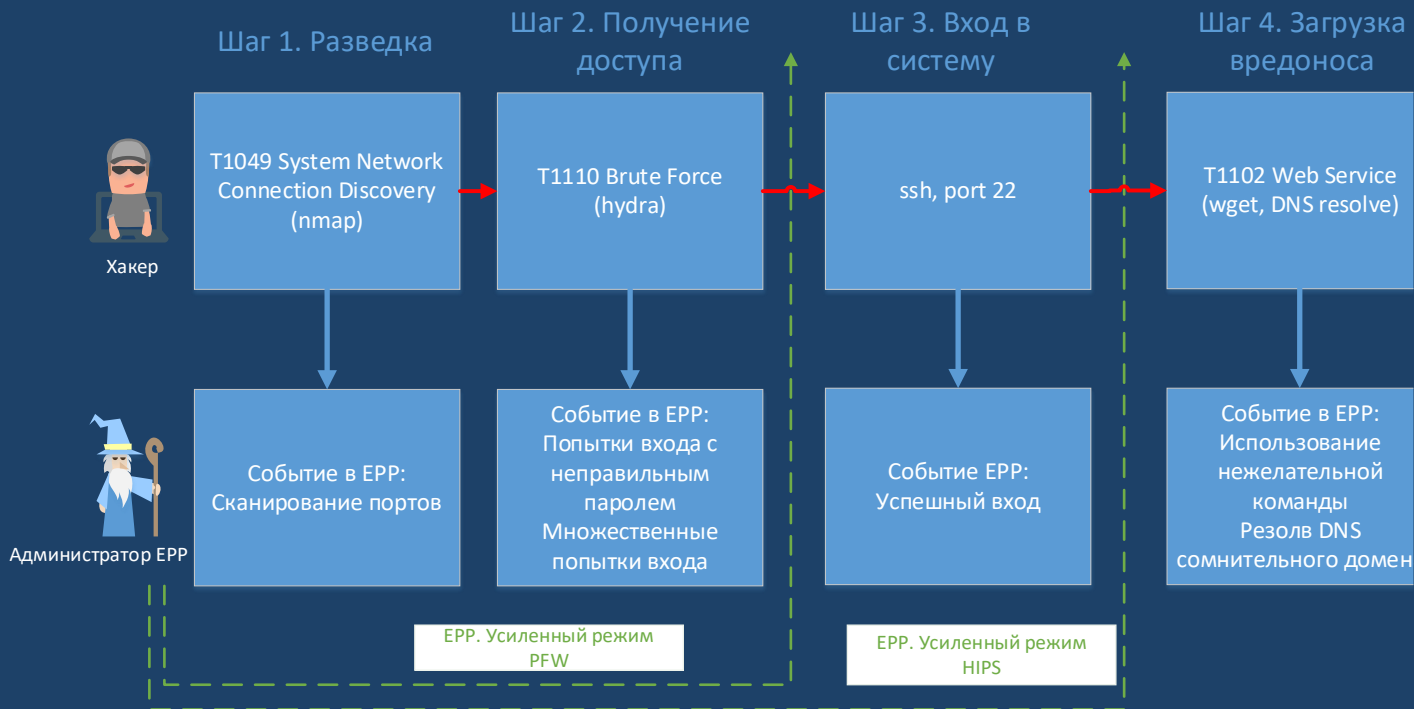
Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.



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)