

Обнаружение и предотвращение атак при помощи ViPNet EndPoint Protection.

Разбор поведения злоумышленника по MITRE ATT&CK

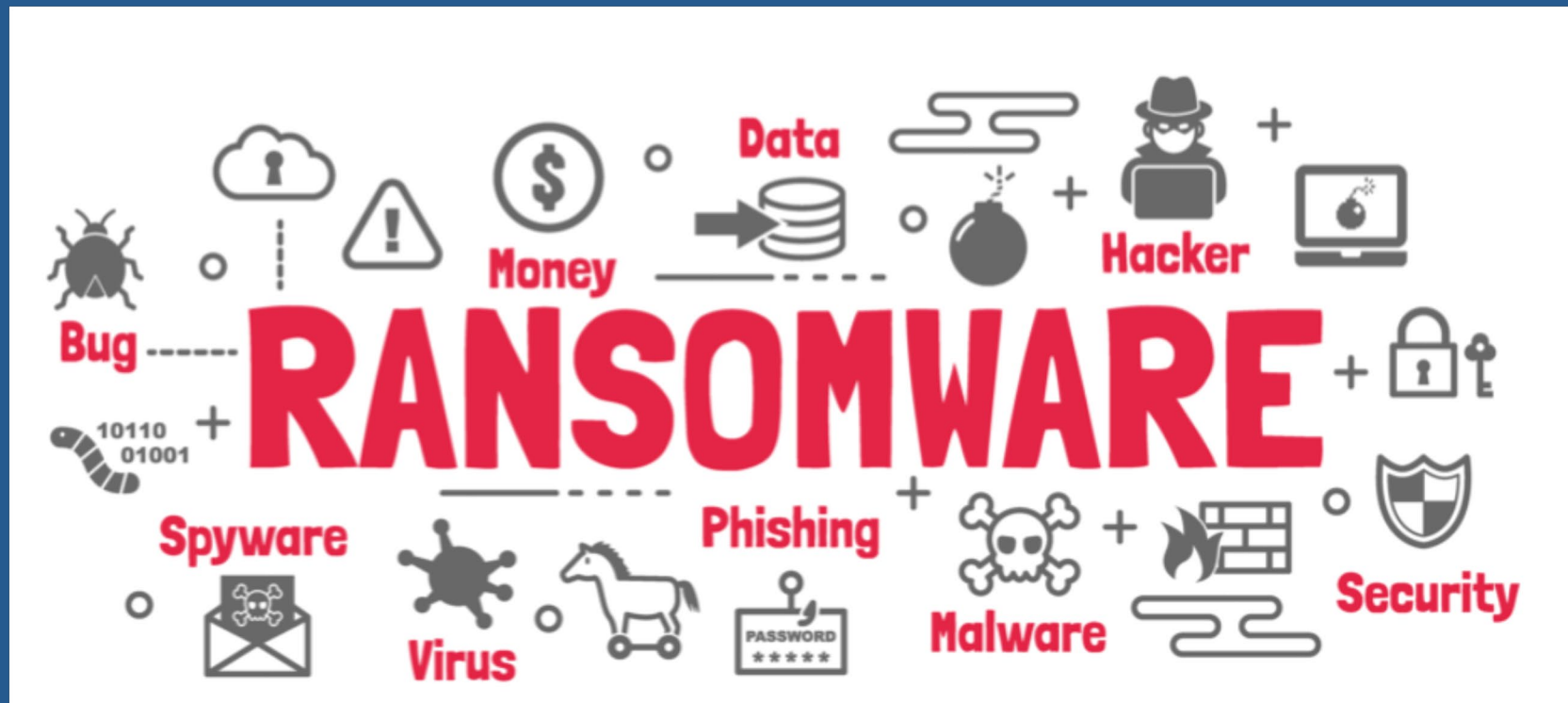
Кадыков Иван
Руководитель продуктового направления

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

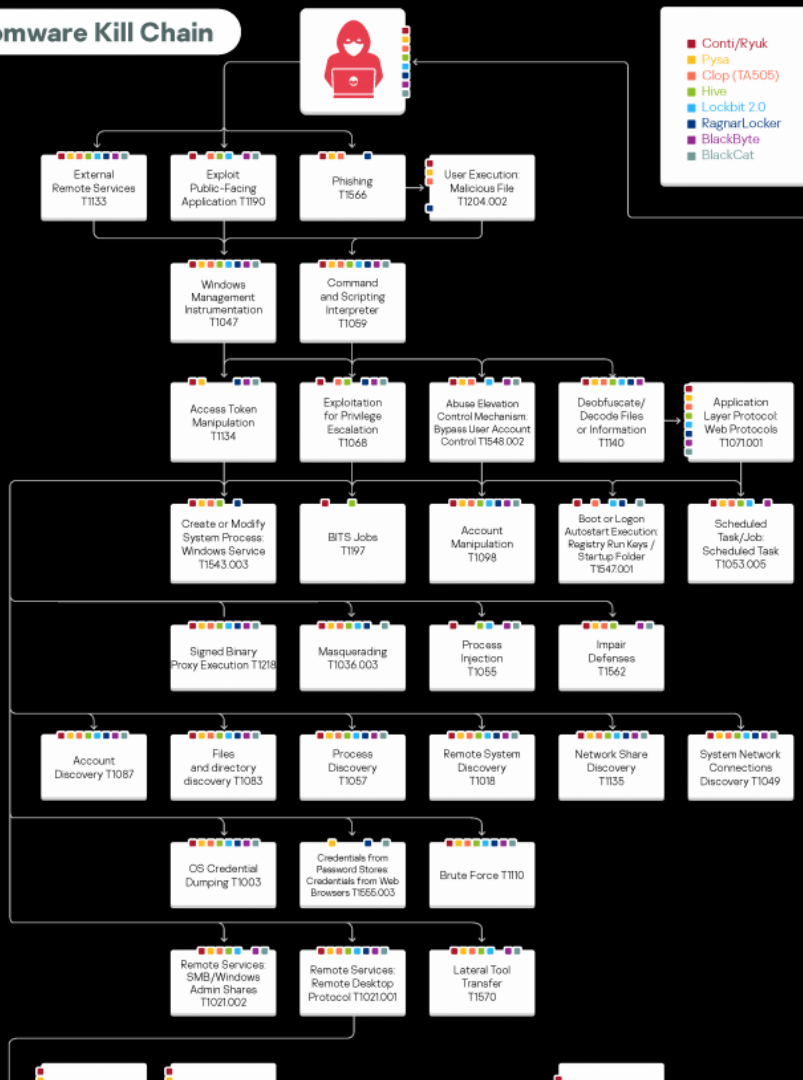
Adversary
Tactics
Techniques
&
Common
Knowledge

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	Later 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 (5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Later 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)	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)	Domain Policy Modification (2)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Domain Trust Discovery	Data from Information Repositories (2)	Failback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	Valid Accounts (4)	Shared Modules	Event Triggered Execution (15)	Escape to Host	Execution Guardrails (1)	Modify Authentication Process (4)	File and Directory Discovery	File and Directory Discovery	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)	Software Deployment Tools	User Execution (3)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites	System Services (2)	Windows Management Instrumentation	System Services (2)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hide Artifacts (7)	Network Share Discovery	Hide Artifacts (7)	OS Credential Dumping (8)	Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
				Impair Defenses (7)	Impair Defenses (7)	Hijack Execution Flow (11)	Network Sniffing	Impair Defenses (7)	Password Policy Discovery	Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
				Indicator Removal on Host (6)	Indicator Removal on Host (6)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	Peripheral Device Discovery	Data from Removable Media	Protocol Tunneling	Transfer Data to Cloud Account	Service Stop
				Scheduled Task/Job (7)	Scheduled Task/Job (7)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	Permission Groups Discovery (3)	Data Staged (2)	Proxy (4)	Transfer Data to Cloud Account	System Shutdown/Reboot
				Valid Accounts (4)	Valid Accounts (4)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	Process Discovery	Input Capture (4)	Remote Access Software	Transfer Data to Cloud Account	
				Hijack Execution Flow (11)	Hijack Execution Flow (11)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	Query Registry	Man in the Browser	Traffic Signaling (1)	Web Service (3)	
				Implant Internal Image	Implant Internal Image	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	Remote System Discovery	Man-in-the-Middle (2)	Web Service (3)		
				Modify Authentication Process (4)	Modify Authentication Process (4)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	System Information Discovery	Screen Capture			
				Office Application Startup (6)	Office Application Startup (6)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	System Location Discovery	Video Capture			
				Pre-OS Boot (5)	Pre-OS Boot (5)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)	System Network Configuration				
				Scheduled Task/Job (7)	Scheduled Task/Job (7)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)					
				Server Software Component (3)	Server Software Component (3)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)					
				Traffic Signaling (1)	Traffic Signaling (1)	Impair Defenses (7)	Network Sniffing	Impair Defenses (7)					
						Indirect Command Execution	Network Boundary						
						Masquerading (6)							
						Modify Authentication Process (4)							
						Modify Cloud Compute Infrastructure (4)							
						Modify Registry							
						Modify System Image (2)							
						Network Boundary							



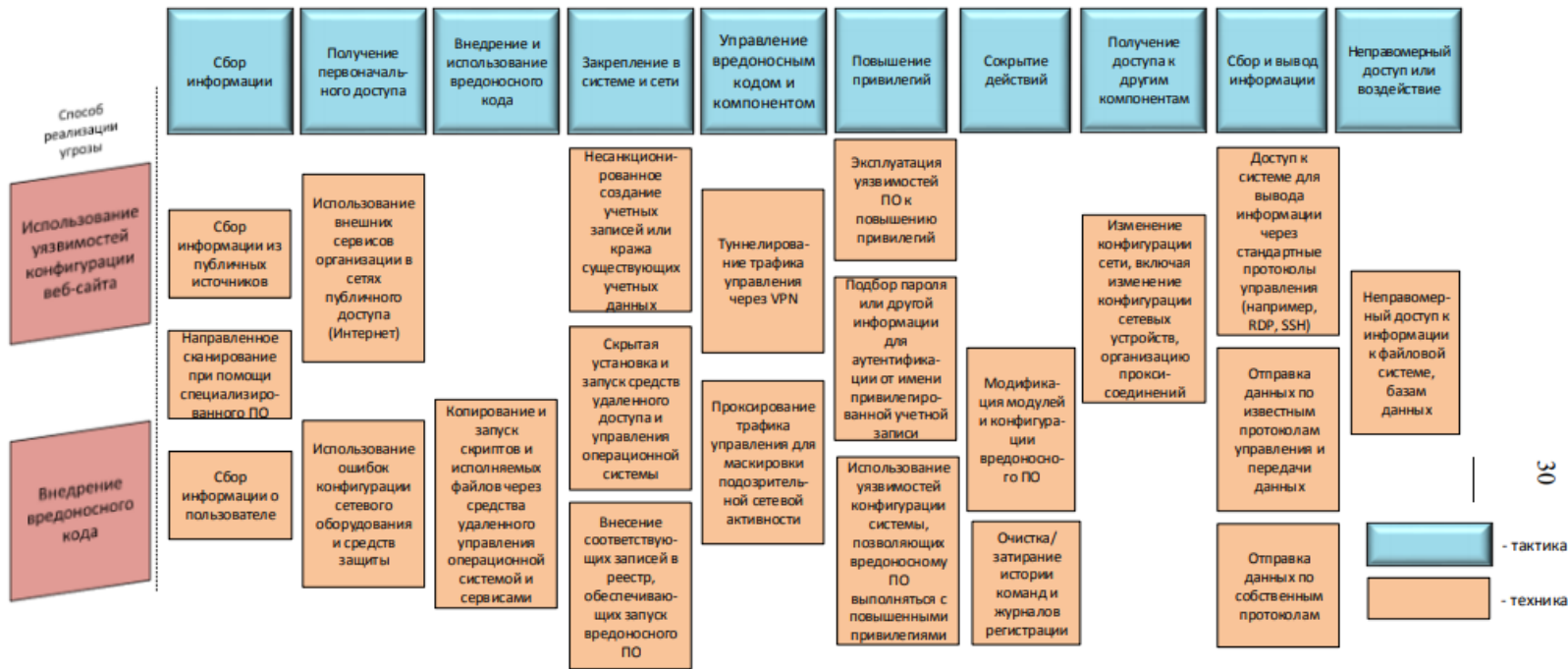
Тактики, техники и процедуры Ransomware- группировок

Исследования
А0 «Лаборатория Касперского»

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

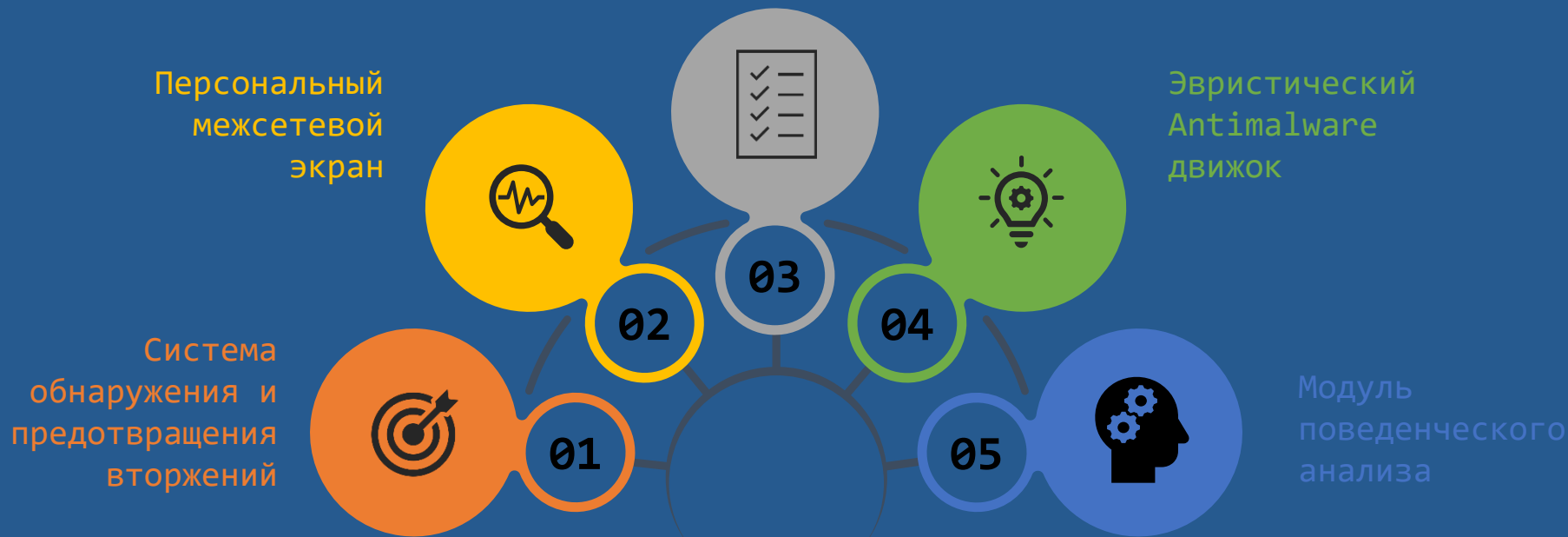
«Методика оценки угроз безопасности информации». ФСТЭК России

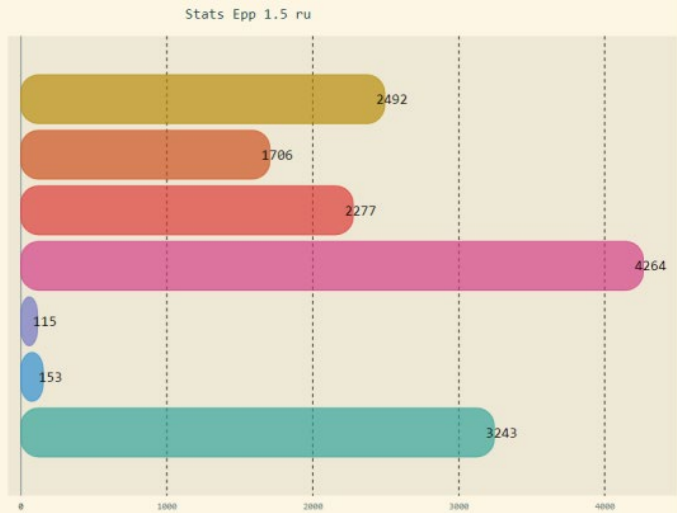
Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию



VIPNet EndPoint Protection

Контроль приложений

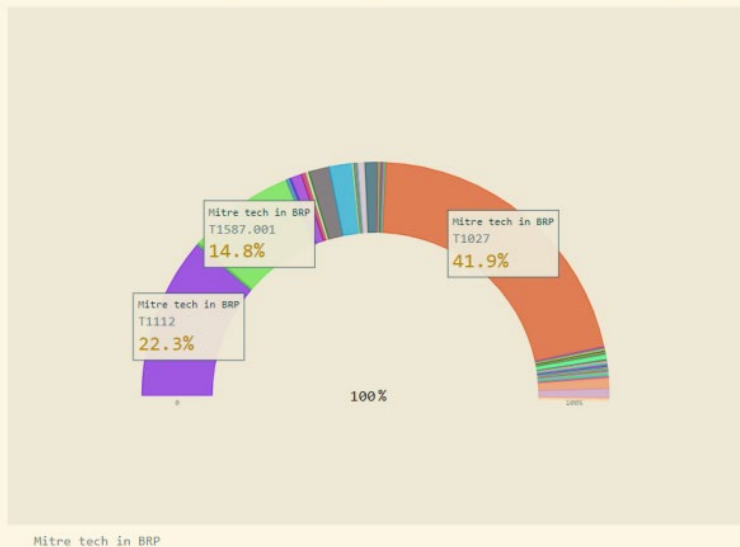




Небольшая статистика

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! 😊 😊 😊



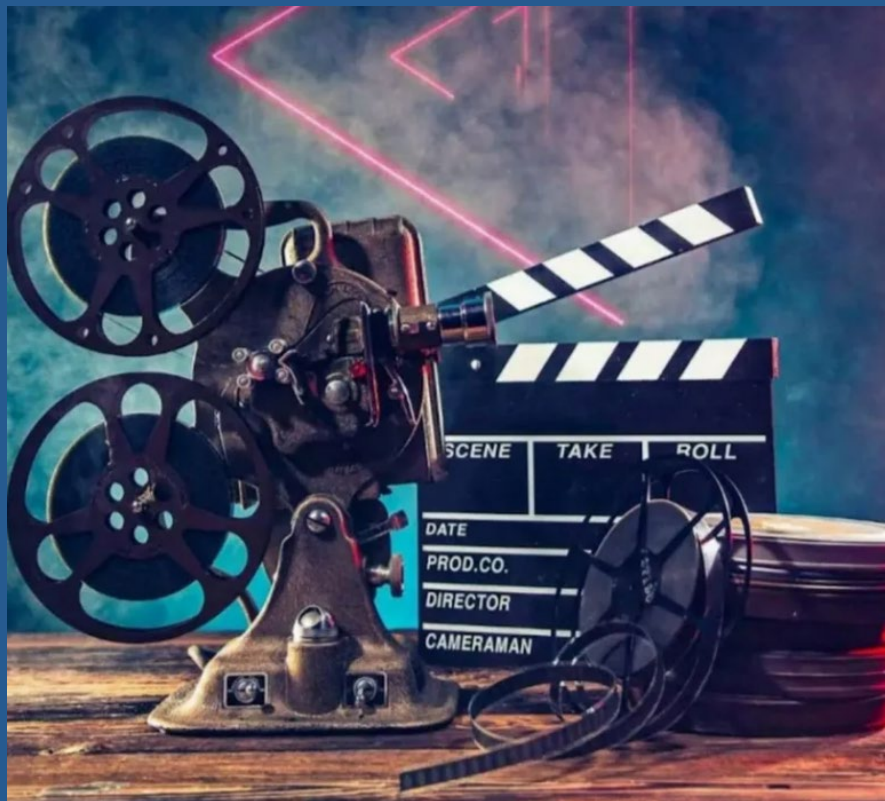
Сценарий 1. Атака через уязвимость в Log4j. Запуск произвольного кода или приложения

Что за атака?

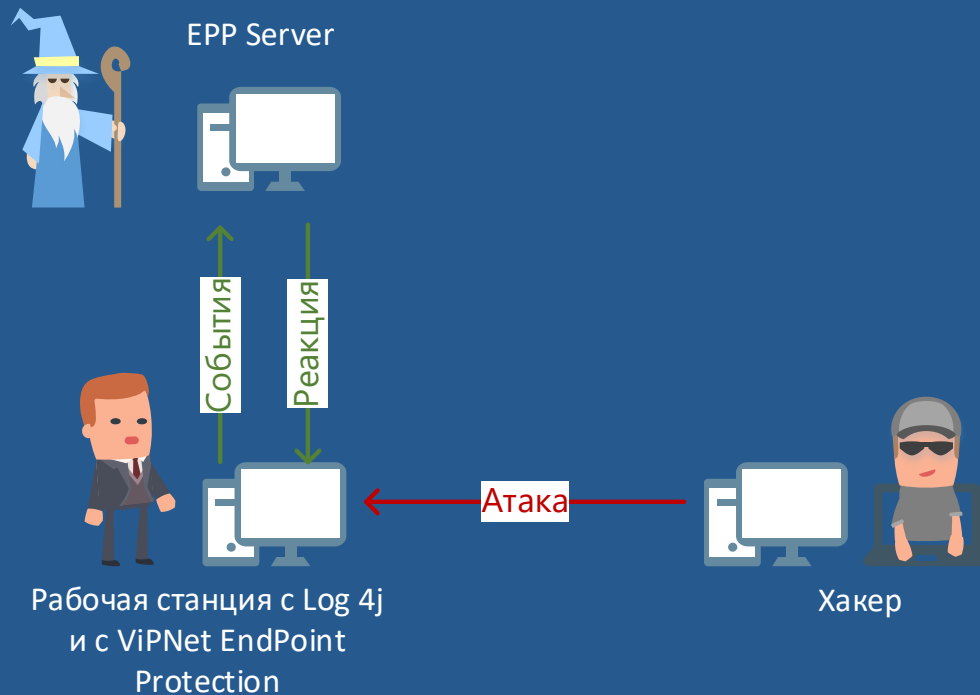
- Злоумышленник будет использовать известную уязвимость в Log4j, точнее CVE-2021-44228.
- Суть атаки – работающий Log4j позволяет запустить любую программу или команду на сервере, при помощи Java Naming and Directory Interface (JNDI).
- Запустим калькулятор через cmd.



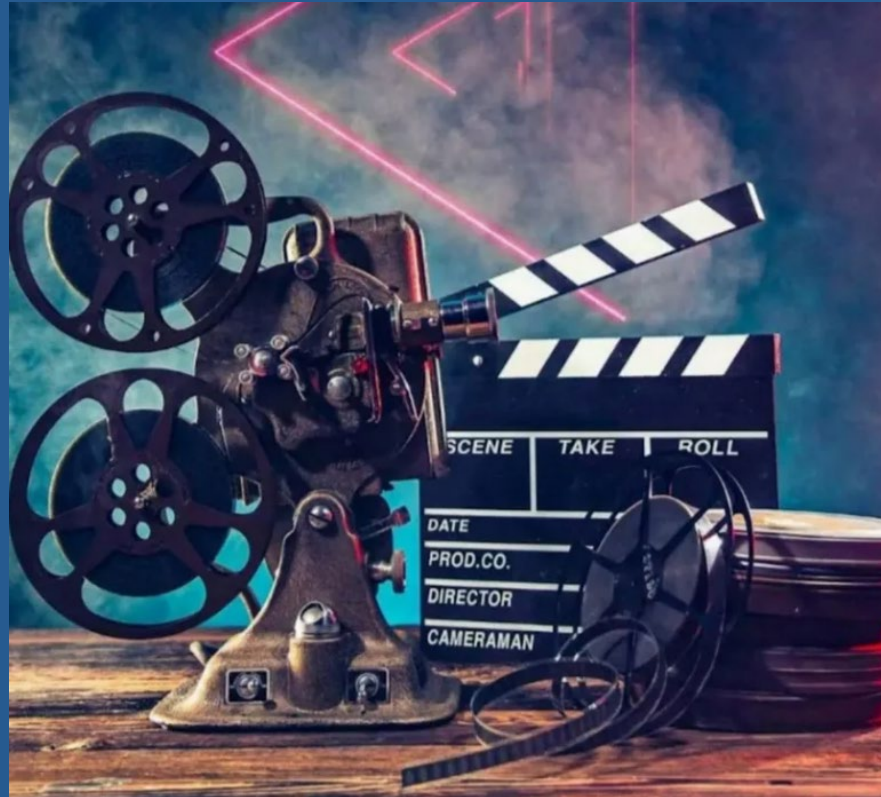
Демонстрируем атаку!



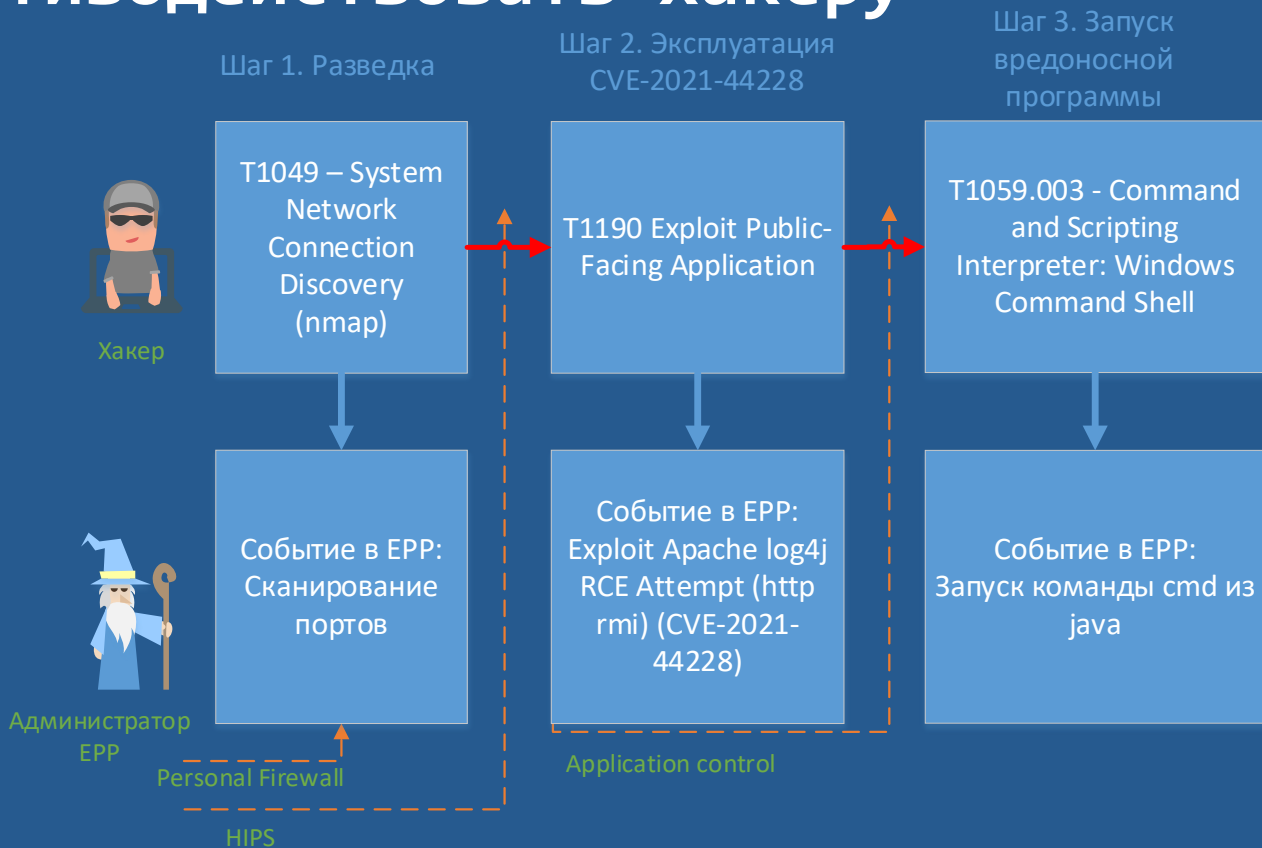
В инфраструктуре появился ViPNet EndPoint Protection



Повторно атакуем, с включенным ViPNet EndPoint Protection



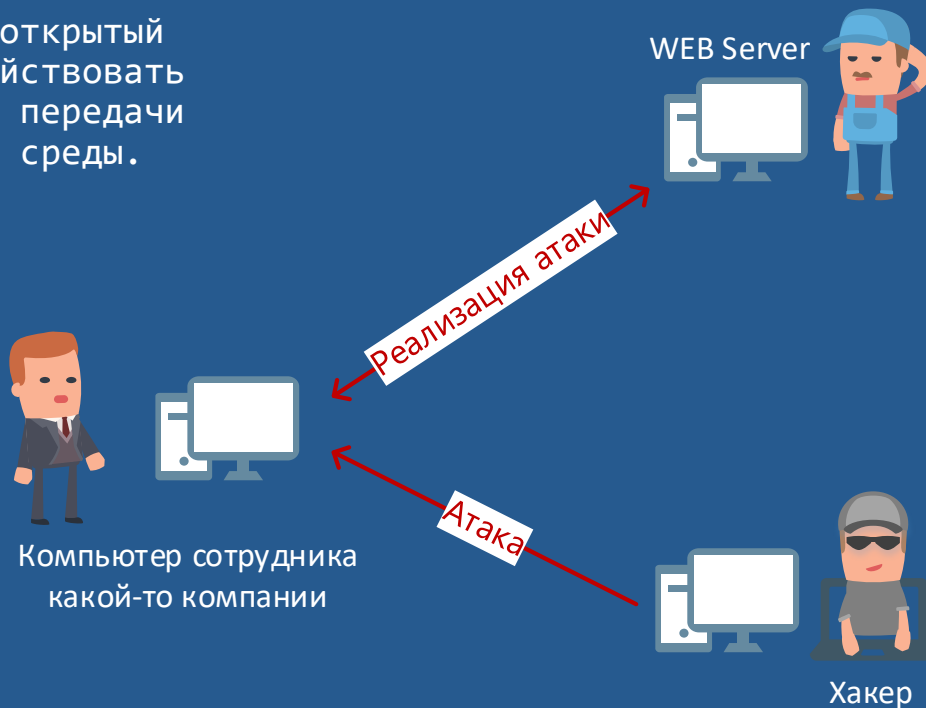
Пошаговый разбор. Как противодействовать хакеру



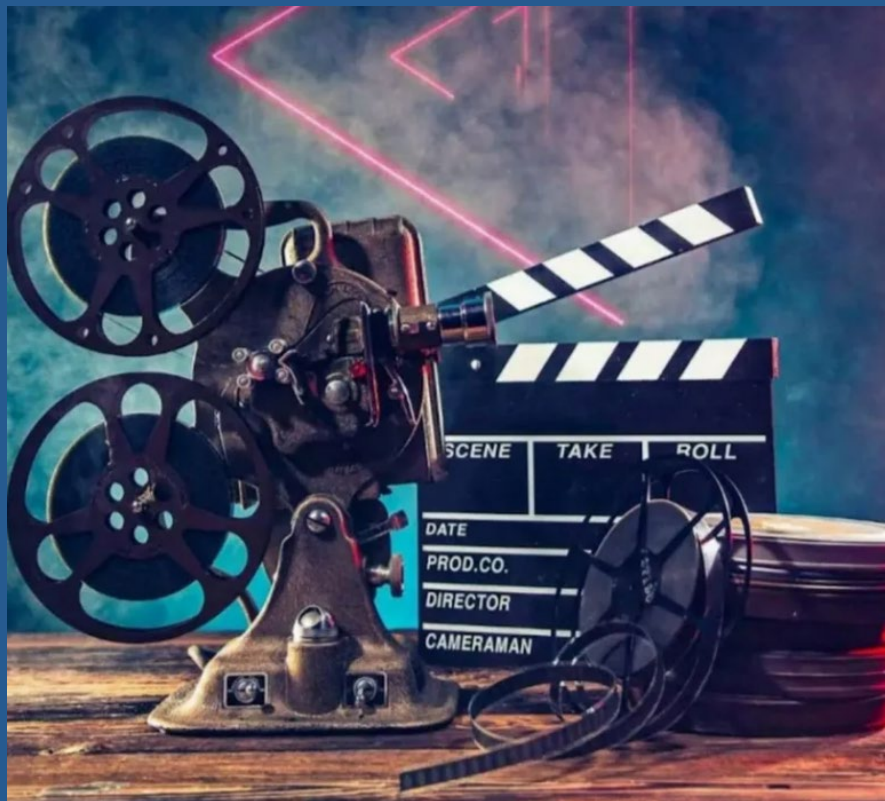
Сценарий 2.
Загрузка вредоносной
программы через открытый
порт 22 (ssh)
с использованием Resolve
DNS.

Что за атака?

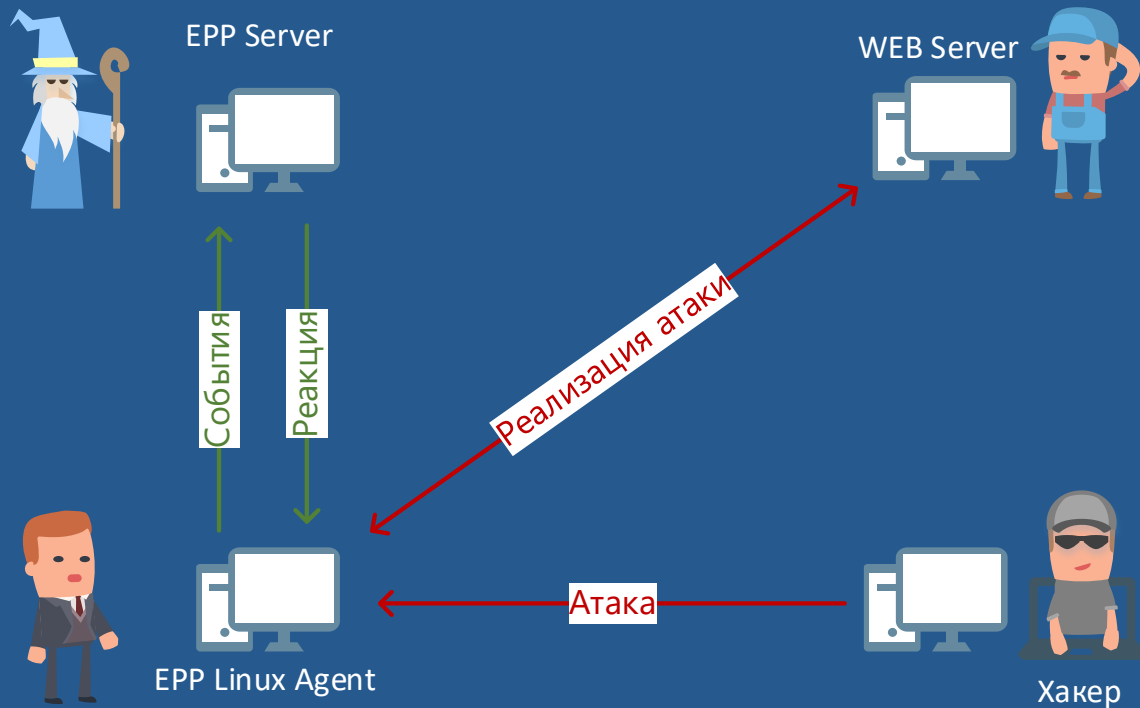
- Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб-службу для передачи данных в/из корпоративной среды.



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

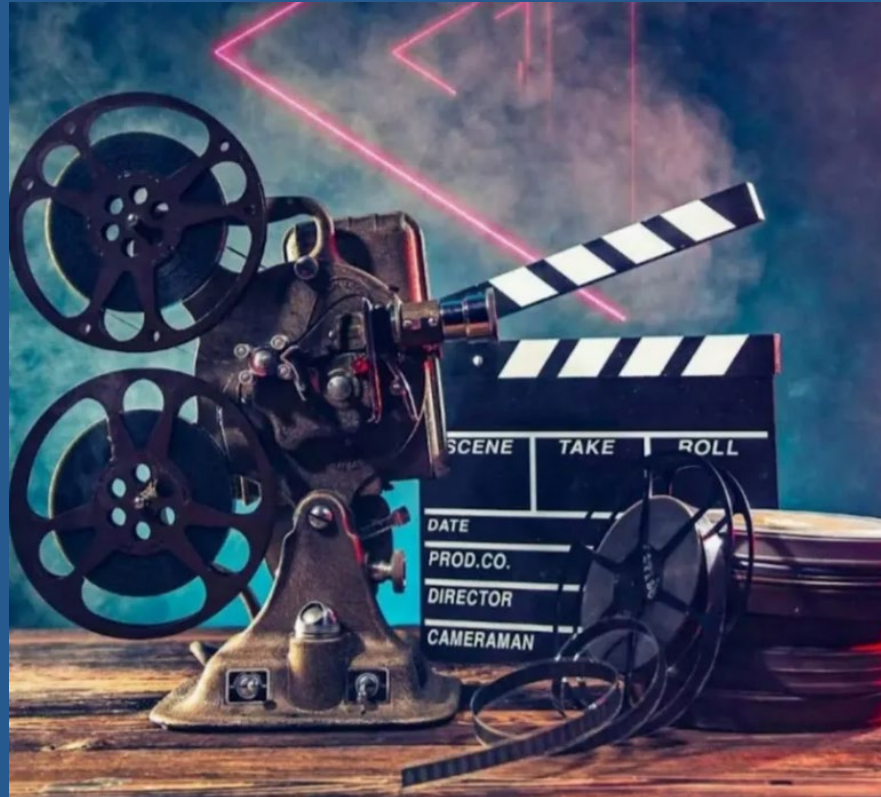
Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.



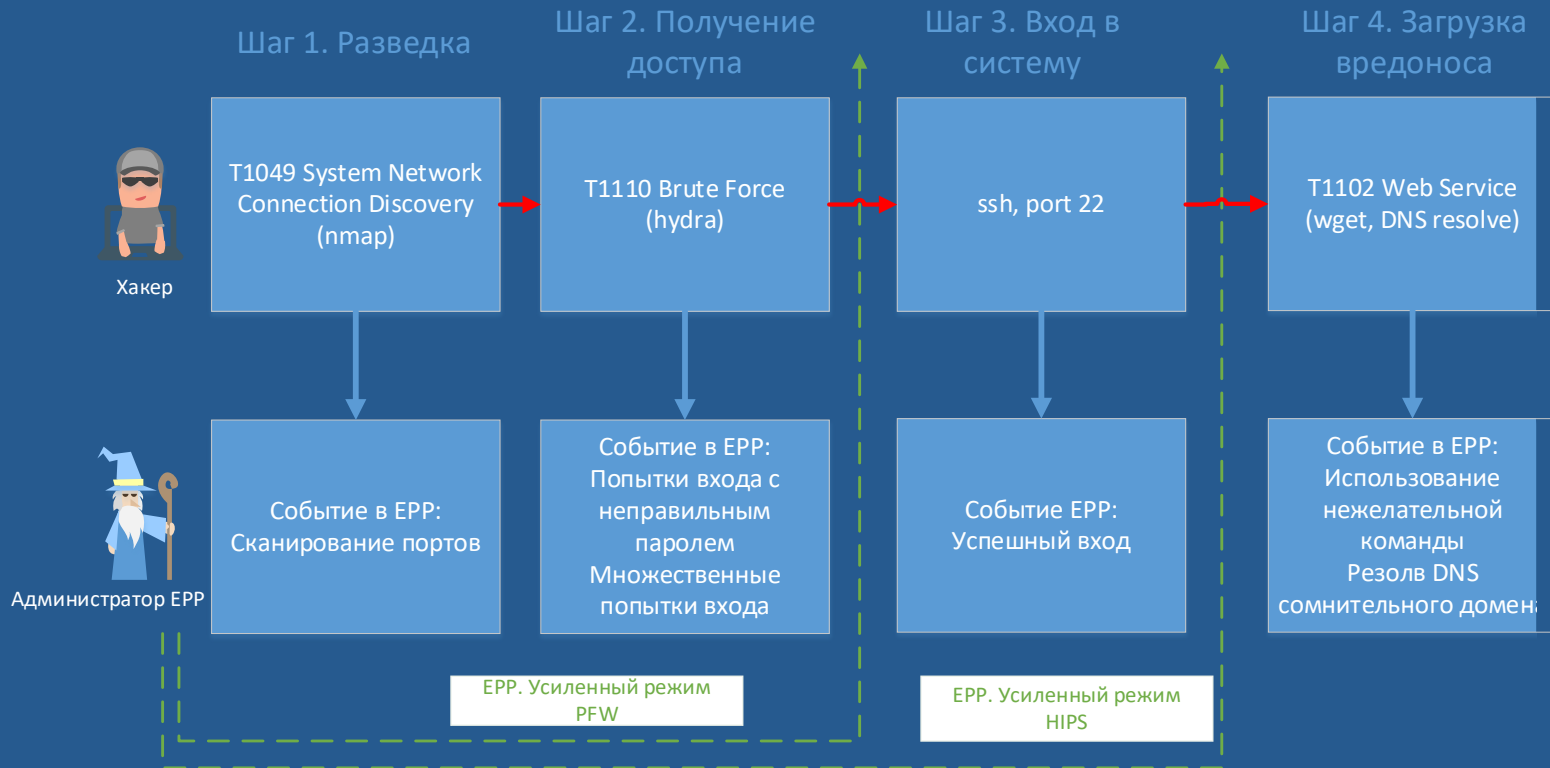
Отключен

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

Повторно атакуем, с включенным ViPNet EndPoint Protection



Пошаговый разбор. Как противодействовать хакеру



ТЕХНО infotecs
2022 ФЕСТ

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363