Искусственный интеллект на страже безопасности.

Обнаружение компьютерной атаки моделями машинного обучения решения ViPNet TDR

Светлана Старовойт

БОЛЬШОЙ МОСКОВСКИЙ ТЕХНО infotecs ФЕСТ

ML-модели в IDS NS и TIAS

Обнаружение сгенерированных доменных имен

DGA

Обнаружение фишинговых доменных имен

FDA

Обнаружения вредоносного ПО в TLS-трафике.

JA3

Обнаружение вредоносной активности в событиях в TIAS

SID-Chain

Новые сценарии в NS

Построение графа взаимодействия

Просмотр содержимого PCAP-файлов

Отображение информации об узлах на графе потоков

Новые сценарии в TIAS

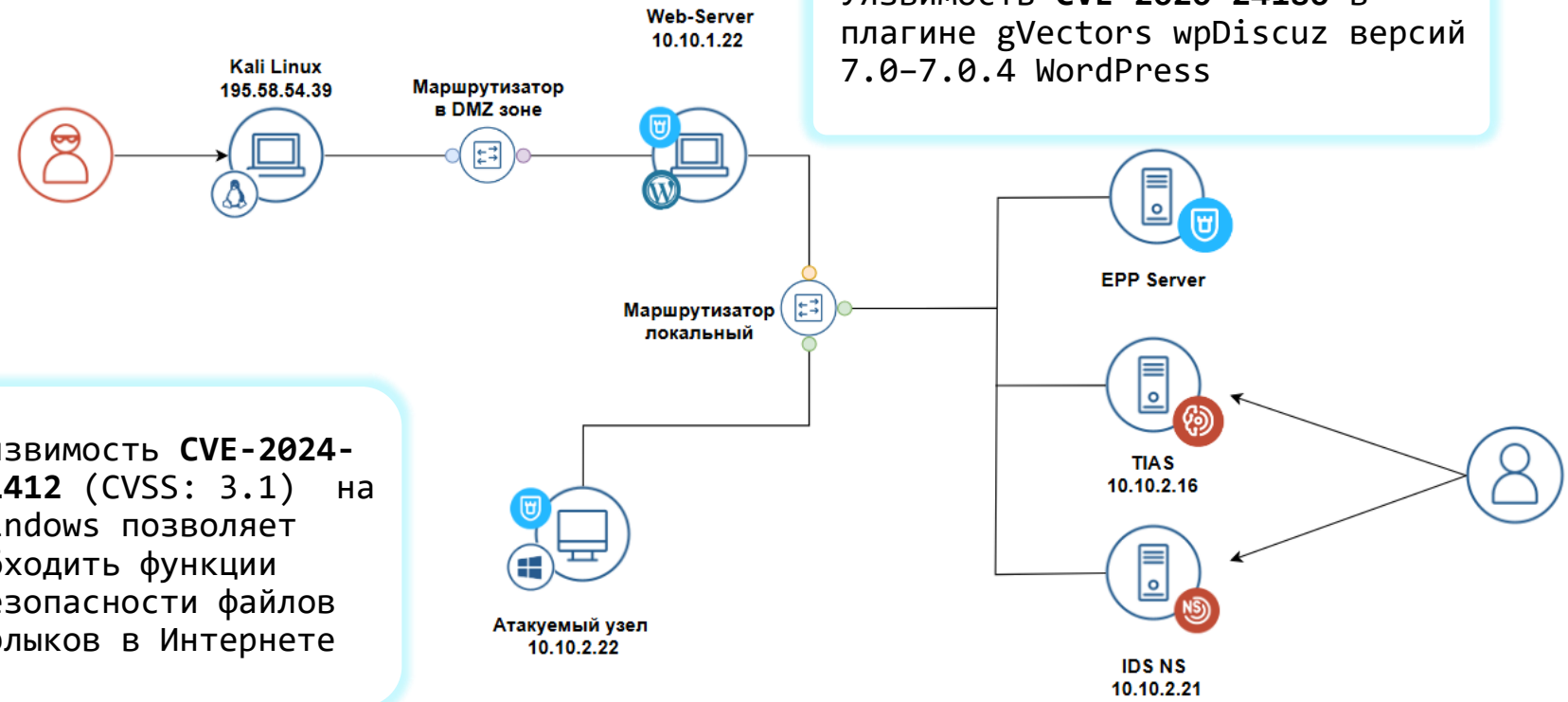
Горизонтальное распространение инцидентов

Связывание инцидентов

Новый алгоритм метаправил

Схема стенда

Уязвимость **CVE-2020-24186** в плагине gVectors wpDiscuz версий 7.0–7.0.4 WordPress



Уязвимость **CVE-2024-21412** (CVSS: 3.1) на Windows позволяет обходить функции безопасности файлов ярлыков в Интернете

Описание атаки

Шаг 1. Фишинг на Windows (CVE-2024-21412)

TA0001 Первоначальный доступ

T1566.002 Целевой фишинг со ссылкой

Шаг 2. Установление meterpreter-сессии с Windows

TA0011 Организация управления

T1071 Протокол прикладного уровня

Шаг 3. Сканирование сети в DMZ зоне

TA0007 Обнаружение

T1046 Изучение сетевых служб

Шаг 4. Эксплуатация уязвимости CVE-2020-24186 Wordpress с плагином wpDiscuz

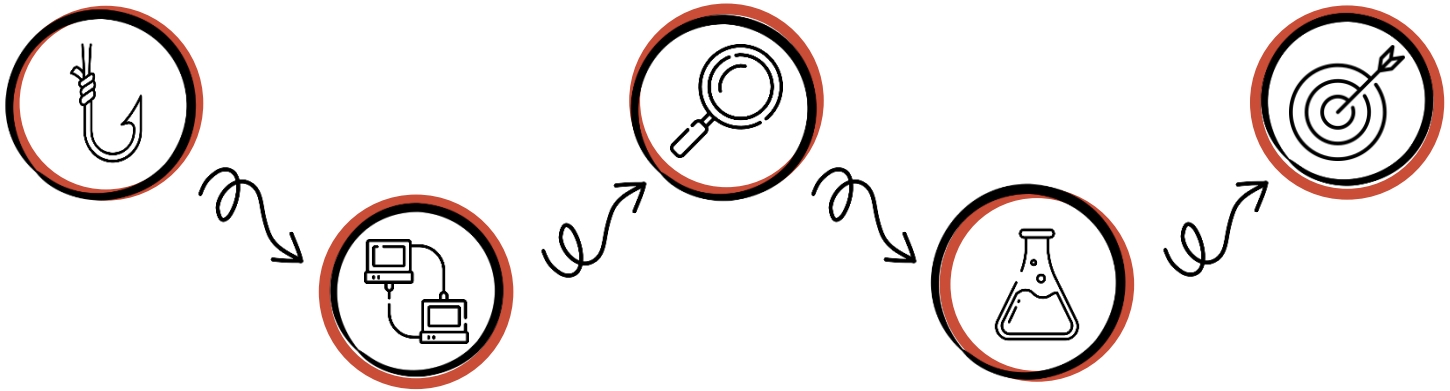
TA0001 Первоначальный доступ

T1190 Эксплуатация уязвимостей публичных приложений

Шаг 5. Кража данных

TA0010 Эксфильтрация данных

T1041 Эксфильтрация по каналу управления



ВНИМАНИЕ!

Компьютерная атака воспроизводится в демонстрационных целях.

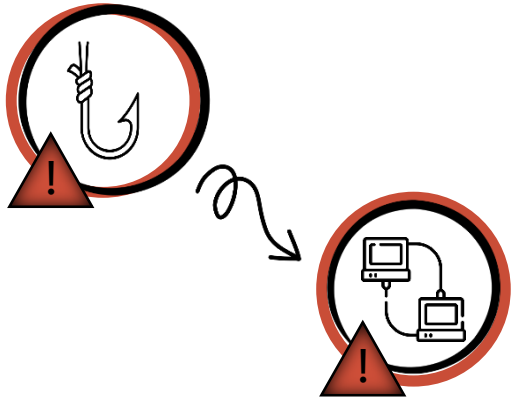
Мы не призываем и не обучаем вас атаковать компьютерные системы.

И помните: киберпреступления караются законом.

Отслеживание последовательной атаки компонентами TDR

Шаг 1. Фишинг на Windows (CVE-2024-21412)

Обнаружены обращения к фишинговому доменному имени ML-моделью AntiPhishing (IDS NS)



Шаг 2. Установление meterpreter-сессии с Windows

Обнаружено обращение к сгенерированным доменным именам ML-моделью DGA (IDS NS)

Обнаружена нежелательная программа в зашифрованном трафике методом Malware JA3 (IDS NS)

Регистрация сигнатурных инцидентов в TIAS

Эксплуатация уязвимости CVE-2024-21412 (тип метаправила «Последовательность событий»)

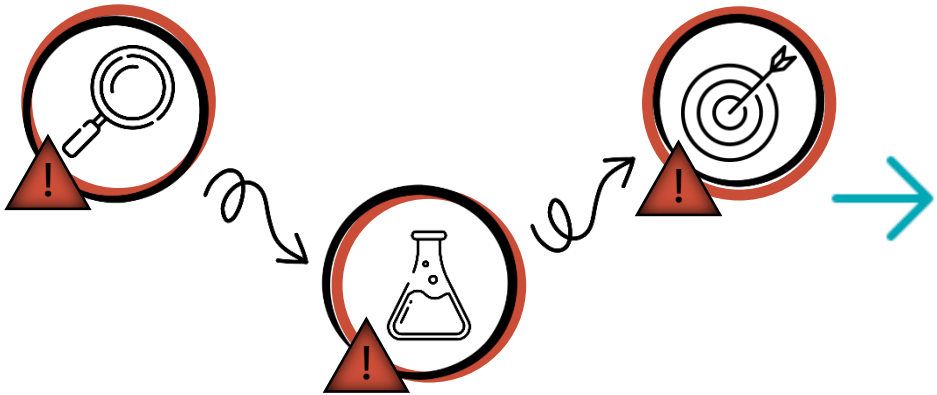
Обращение к фишинговому доменному имени (тип метаправила «ML-событие»)

Отслеживание последовательной атаки компонентами TDR

Шаг 3. Сканирование сети в DMZ зоне

Шаг 5. Кража данных

Обнаружено аномальное увеличение исходящего трафика ML-моделью TVA



Шаг 4. Эксплуатация уязвимости CVE-2020-24186 Wordpress с плагином wpDiscuz

Регистрация сигнатурных событий в IDS NS и ViPNet EPP

Регистрация эвристического инцидента в TIAS

Классификатором обнаружена подозрительная активность (модель SID-Chain)

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA
NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ
GLOBAL DIGITAL SPACE
CISOCLUB
РУТОКЕН
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
АВАНГАРД
AR integ
АТБ ЭЛЕКТРОНИКА
infotecs {/-cademy}
merlion
УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС