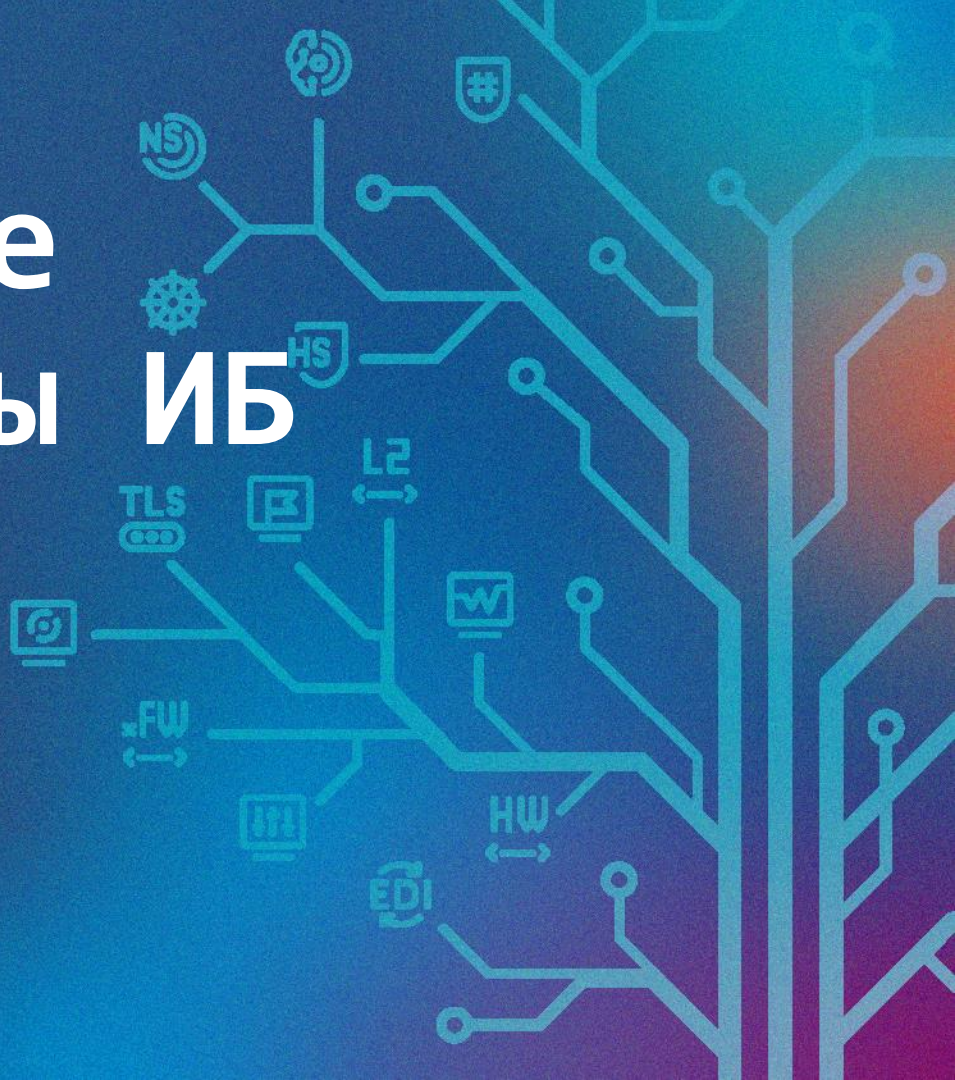
Реагирование на инциденты ИБ

Лихацких Иван

infotecs



С чего начать реагировать на инцидент?

1. **NIST SP 800-61 "Computer Security Incident Handling Guide**

   ("Руководство по обработке инцидентов компьютерной безопасности«)

2. **ГОСТ Р 59710-2022**

   «Защита информации. Управление компьютерными инцидентами. Общие положения»

3. **ГОСТ Р 59712-2022**

   «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты»

NIST SP 800-61 "Computer Security Incident Handling Guide

Содержит этапы:

- Подготовку
- Идентификацию
- Сдерживание
- Ликвидацию
- Восстановление работы
- Пост-анализ случившегося

Подготовка:

Политика реагирования на киберинциденты

Индивидуально для каждой конкретной организации

1. Утверждение о вовлеченности руководства компании в процесс реагирования на киберинциденты и понимание его важности на всех уровнях компании;
2. Организационная структура и распределение ролей, ответственности, полномочий и уровней принятия решений;
3. Формы отчетности и отправки уведомлений.

ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения»

Рисунок 2 — Стадии управления компьютерными инцидентами

Реагирование на майнер

Подготовка: проверить: актуальность баз антивируса, все ли модули АВЗ включены. Убедиться в наличие журналов (логов) с DNS, Proxy серверов, МЭ и др. СЗИ. Убедиться в наличие точек восстановления системы (System Restore), бэкапы.

Идентификация: Обычный вирус-майнер (Trojan) или скрытый майнер (криптоджекинг)? Установить источник распространения вируса.

Сдерживание: Если АРМ подключен к корпоративной сети, то нужно локализовать площадь заражения.

Ликвидация: Провести антивирусную проверку, проверить работу браузера

Восстановление: Проверить работу ОС и ПО (Windows Event) на наличие проблем и ошибок. Переустановить ПО, драйвера или откатится на точку восстановления

Пост анализ: Разработать и внедрить комплекс мер защиты.

Реагирование на майнер

На первом этапе, помимо стандартных рекомендаций по защите оконечных устройств от вредоносного ПО, мы советуем настроить сетевое оборудование, межсетевые экраны или средства контроля доступа в Интернет на блокирование доступа к адресам сайтов по майнингу.

Поэтому я бы рекомендовал регулярно отслеживать рейтинги пулов для майнинга, которые свободно можно найти в Интернете. Назову только несколько имен:

suprnova[.]cc,
nanopool[.]org,
zpool[.]ca,
coinmime[.]pl,
eth.pp[.]ua,
zcash.flypool[.]org,
dwarfpool[.]org,
p2pool[.]org,
bitclubnetwork[.]com,
miningrigrentals[.]com,

Реагирование на майнер

К сожалению, надо признать, что исключить полное блокирование доступа к пулам для майнинга мы не можем – они появляются постоянно и отслеживать их бывает непросто…

С помощью слежения за портами, которые использует ПО для майнинга для взаимодействия с пулами и командными центрами. К таким портам можно отнести:

- 3333 (bitcoin)
- 3336 (litecoin)
- 8333 (bitcoin)
- 8545 (Ethereum),
- 9333 (litecoin)
- 9999 (Dashcoin),
- 10034 (ypool.net)
- 22556 (Dogecoin),

Реагирование на майнер

Помимо контроля портов, присутствует возможность обнаружения протоколов, используемых майнерами, например, популярными Bitcoin и Litecoin. Достаточно создать правило для контроля взаимодействия по данным протоколам и вы будете всегда знать, кто в вашей сети занимается майнингом (осознанно или даже не зная, что его компютер участвует в пуле для майнинга), независимо от того, с каким узлами и по каким портам идет взаимодействие. Аналогичная функция присутствует и в ViPNet IDS/ xF/ HW5, позволяющей распознавать и классифицировать больше тысячи приложений, включая и майнинговые.

Реагирование на майнер

Система обнаружения вторжений **ViPNet IDS** обладает рядом сигнатур для обнаружения работы как легальных майнеров, так и вредоносного кода, задействующего функции майнинга.

Например, она может выглядеть так:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN
W32/BitCoinMiner.MultiThreat Subscribe/Authorize Stratum Protocol Message";
flow:established,to_server; content:"{|22|id|22|"; depth:10; content:"|22|method|22
3A| |22|mining."; within:100; content:"|22|params|22|"; within:50;
pcre:"/\x22mining\x2E(subscribe|authorize)\x22/"; classtype:trojan-activity;
reference:url,talosintelligence.com/;
reference:url,www.btcguild.com/new_protocol.php;
reference:url,mining.bitcoin.cz/stratum-mining; sid:1000501; rev:1;)
```

Реагирование на шифровальщика

Подготовка: проверить АВЗ, резервные копии «3-2-1»,
План реагирования, Управление обновлениями.
Сегментирование «яйца по разным корзинкам».

Идентификация: АВЗ (Sandbox), IDS/IPS, EDR, NGFW, SIEM.
Сообщение в НКЦКИ/ФинЦЕРТ.

Сдерживание: Если АРМ подключен к корпоративной сети,
то нужно локализовать площадь заражения.

Ликвидация: Провести антивирусную проверку/ переустановка систем

Восстановление: Резервные копии

Пост анализ: Оценка действиям, работа над ошибками

Реагирование на шифровальщика

infotecs

Методы защиты:

1. "Белый список" сайтов куда разрешен доступ. Желательно прописать сайты в локальный DNS-сервер.
2. "Белый список" разрешенных для запуска приложений. Можно в редакторе реестра (запускается Win+R и ввести regedit и OK) в ветке HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer создать DWORD параметр RestrictRun со значением 1, затем в этой же ветке создаем раздел RestrictRun, а имена исполняемых файлов прописываем в этом же разделе в строковых параметрах в формате: имя параметра = номере по порядку (1,2,3); значение = имя исполняемого файла. В ОС Linux на отдельные диски выносятся точки монтирования /bin /usr/bin (если нестандартный софт, то добавить в этот список), а для остальных разделов ставиться флаг монтирования noexec.

Реагирование на шифровальщика

infotecs

Бэкап данных

Самый эффективный способ бэкапа данных требует "в идеале" 2 флешки и 1 съемный диск, но можно обойтись и Linux-сервером в сети. "Идеальная схема" - на 1 флешку мы записываем ОС Linux, на вторую - установочник ОС Windows. Устанавливаем ОС и делаем или классическую 2-х дисковую разметку (ОС + данные) или более продвинутую 3-х дисковую (ОС + данные + раздел под резервную ОС). После "чистой" установки устанавливаем весь нужный софт и проводим все мероприятия по защите ОС. Получаем "эталонную систему"

Реагирование на шифровальщика

Метод (единственный!!!) защиты:

1. Выключаем жёстко компьютер (выдергиванием вилки из сети или 10 секундным нажатием на кнопку питания).
2. Создаем или используем загрузочную флешку с антивирусом или просто Linux.
3. Проверяем действительно ли файлы повреждены (есть 0,01% вероятность шутки).
4. Если действительно повреждены - удаляем разделы дисков.
5. Переустанавливаем/восстанавливаем ОС и скачиваем последний бэкап.

НИ В КОЕМ СЛУЧАЕ ПЛАТИТЬ НЕЛЬЗЯ!!!

Реагирование на дефэйс сайта

Подготовка: проверить АВЗ, резервные копии «3-2-1», План реагирования, Управление обновлениями. Сегментирование «яйца по разным корзинкам».

Идентификация: WAF, АВЗ, IDS/IPS, NGFW, SIEM.
Сообщение в НКЦКИ/Роскомнадзор

Сдерживание: Нужно локализовать площадь атаки.

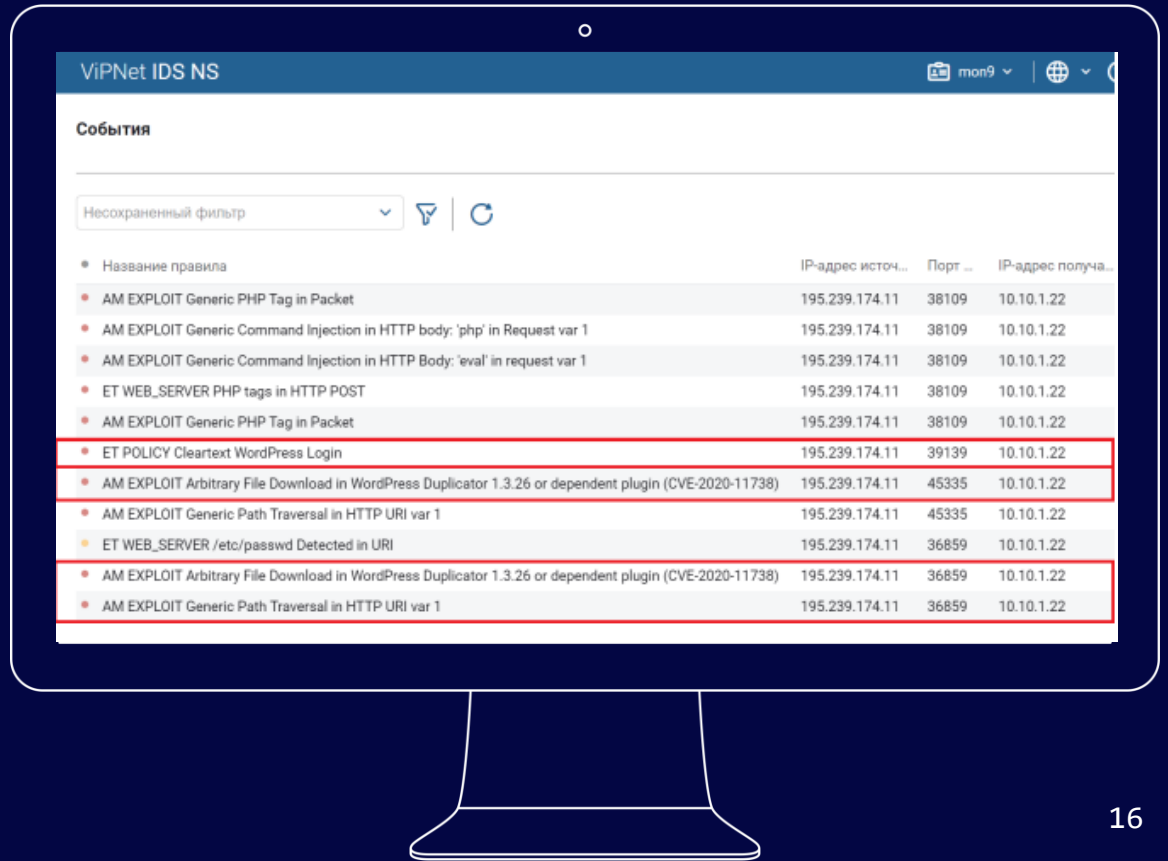
Ликвидация: Провести мероприятия по поиску и ликвидации взломанных файлов.

Восстановление: Резервные копии

Пост анализ: Оценка действиям, работа над ошибками

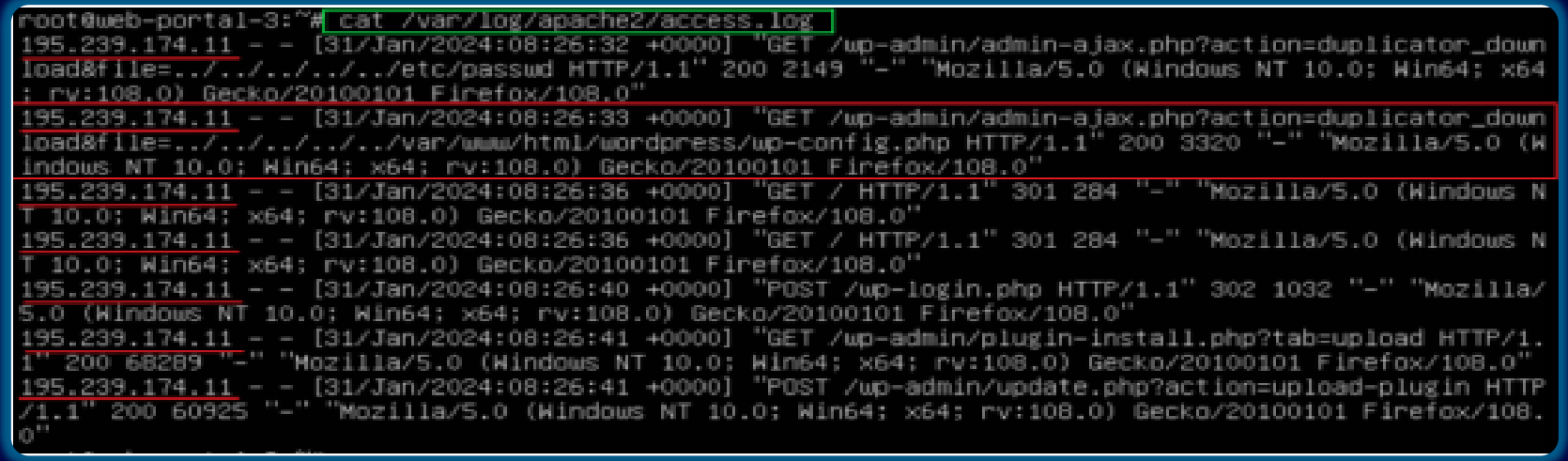
Реагирование на дефэйс сайта

Обнаружение эксплуатации уязвимости средствами обнаружения вторжений уровня сети



Реагирование на дефэйс сайта

Необходимо напомнить, что уязвимость в плагине Duplicator WordPress позволяет получить любой файл в системе, к которому имеет доступ пользователь www-data.
Для того, чтобы получить необходимый файл, нарушитель будет обращаться по ссылке: GET/wp-admin/adminajax.php?action=duplicator_download&file=../../../../../file.
Этот факт будет детектироваться в логах сервера apache2, которые можно найти по следующему пути: /var/log/apache2/access.log



Подписывайтесь
на наши соцсети,
там много интересного

Иван Лихацких
lin@infotecs.ru