КОД ИБ

ИТОГИ

ТРЕНДЫ КИБЕРАТАК НА РИТЕЙЛ 2024

ПО ДАННЫМ SOC МАГНИТ

ОЛЕГ ЛАЛАЕВ
Руководитель управления информационной безопасности
ПАО Магнит

КОД ИБ

ИТОГИ

Какие новые кибератаки в тренде в 2024?

КОД ИБ

ИТОГИ

Никакие!

Directed by
ROBERT B. WEIDE

КОД ИБ

ИТОГИ

КОД ИБ

ИТОГИ

Старые виды атак никуда не делись!

КОД ИБ

ИТОГИ

DDoS

КОД ИБ

ИТОГИ

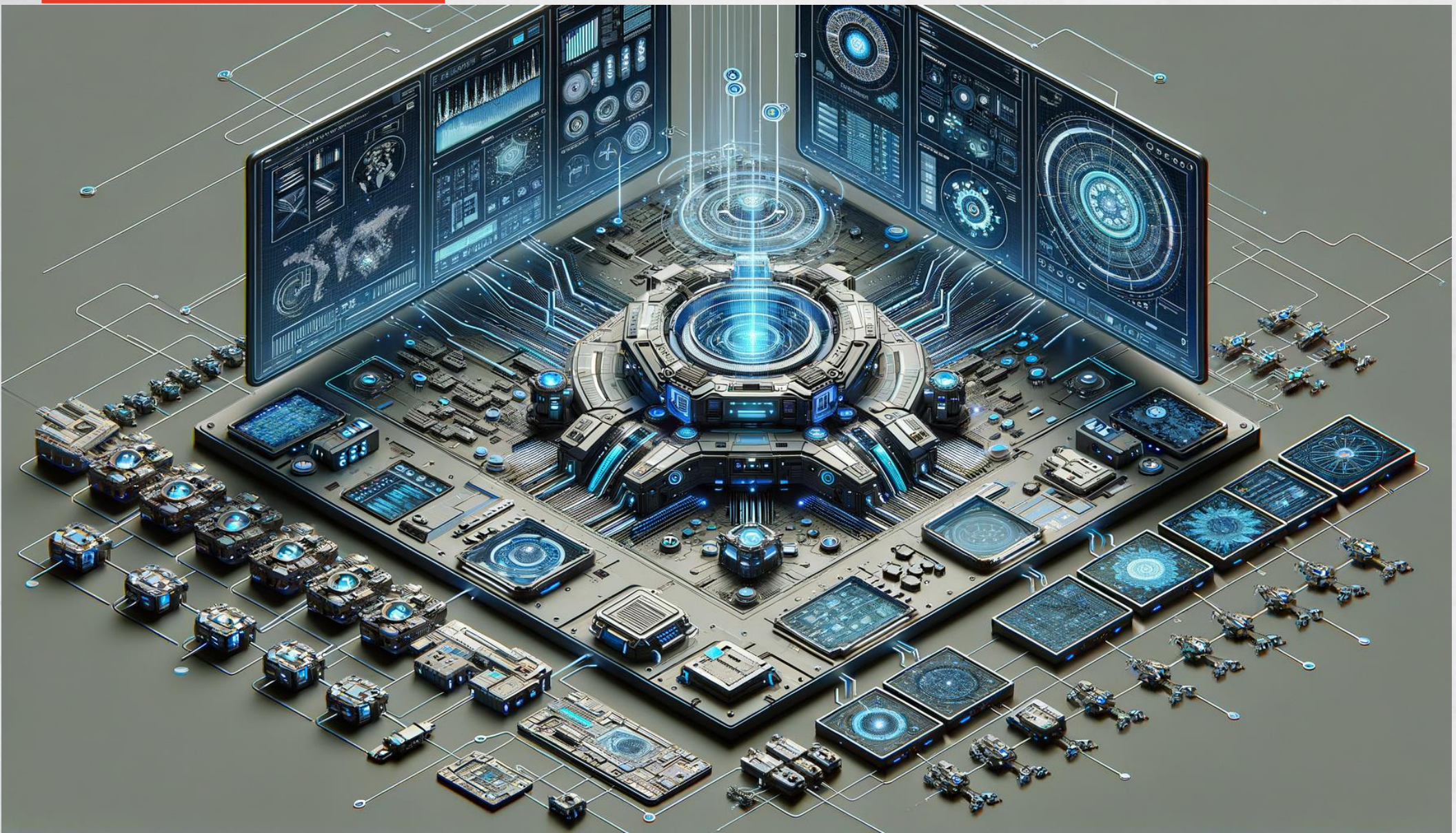
Комбинированные DDoS атаки

- L7 атаки (http запросы направленные на исчерпание производительности серверов), в сочетании с TCP flood и UDP flood на терабиты
- Одновременно атака идет на множество доменов третьего уровня, позволяя успешно загасить те домены, которые по какой-то причине не были заведены за DDoS

КОД ИБ

ИТОГИ

Bot Attacks



КОД ИБ

ИТОГИ

- Умные боты направленные на программу лояльности, кража бонусов с карт и перепродажа
- Боты парсинга каталога
- Игровые боты для дампа промокодов или достижения других целей в игре

КОД ИБ

ИТОГИ

Phishing

КОД ИБ

ИТОГИ

- Сообщения в ТГ от руководства компании
- Письма от руководства компании
- Письма от гос органов

КОД ИБ

ИТОГИ

Fraud

КОД ИБ

ИТОГИ

- Участие в онлайн опросах
- Акции, скидки, конкурсы
- Refund средств по доставке
- Продажа промокодов

КОД ИБ

ИТОГИ

Ransomware

КОД ИБ

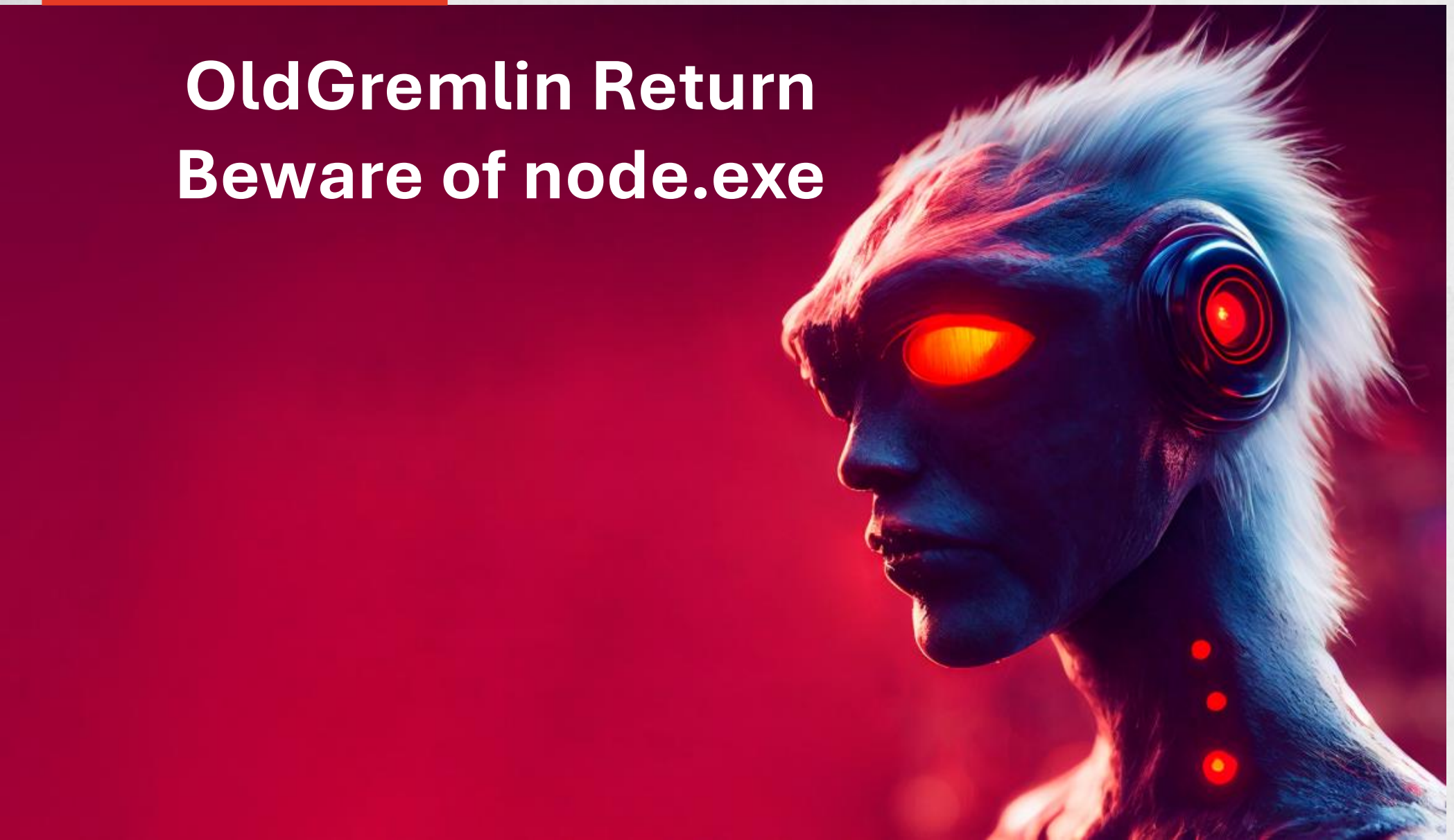
ИТОГИ

- Blackbit
- Lockbit
- Shadow (тот же lockbit + endurance wiper)

КОД ИБ

ИТОГИ

OldGremlin Return
Beware of node.exe

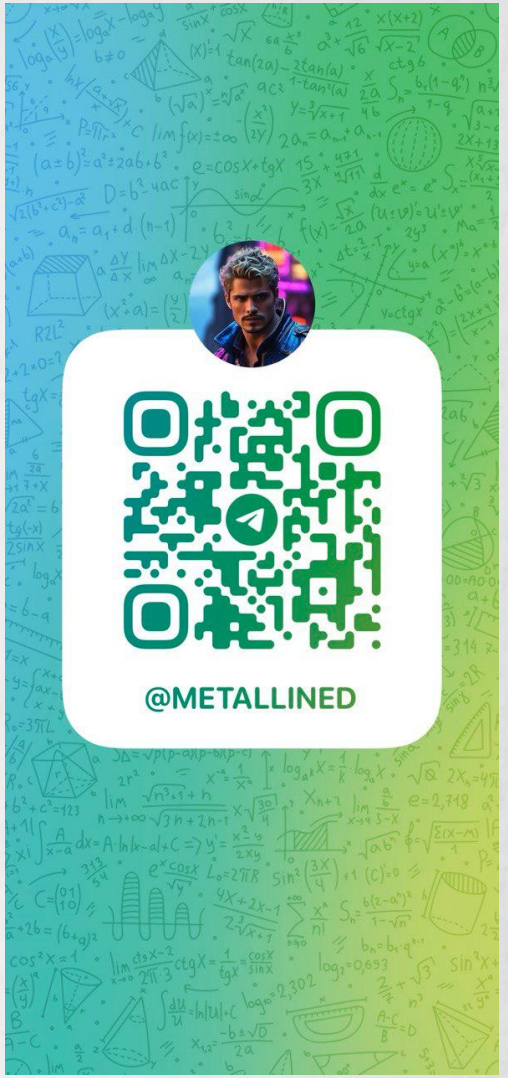


КОД ИБ

ИТОГИ

Тренды не поменялись

- DDoS
- Bot Attacks
- Phishing
- Fraud
- Ransomware



Лалаев Олег
Руководитель Информационной безопасности ПАО Магнит
Email: Oleg@metallined.ru
TG: @metallined