4RAYS by SOLAR

КАКИЕ БЫВАЮТ ЗНАНИЯ О КИБЕРУГРОЗАХ И КАК ИХ ПРИМЕНЯТЬ

2025

4RAYS by SOLAR

Самопроверка на знания о киберугрозах

Вопрос 1. Solar 4RAYS подробно разобрали популярный инструмент для DDoS-атак, который распространяется в Telergam. Как назывался инструмент?

- ☐ DDOSIM
- ☐ Pyloris
- ☐ Sloworis
- ☐ Gorgon

Вопрос 2. Как называется популярная техника сокрытия коммуникации между ВПО и серверами управления, о которых в октябре писали эксперты Solar 4RAYS?

- ☐ DDR
- ☐ SRS
- ☐ PPR
- ☐ FBI

Вопрос 3. Эксперты Solar 4RAYS рассказывали о методе распаковки ВПО, упакованного с помощью популярного пакера. О каком пакере идет речь?

- ☐ Strontium
- ☐ Obsidium
- ☐ Hafnium
- ☐ Ziromium
- ☐ Polonium

Вопрос 4. Как назывался легитимный инструмент, который группировка Gambling Zealot использовала для проведения атаки, расследованной Solar 4RAYS?

- ☐ T-Rex
- ☐ Velociraptor
- ☐ AmmyAdmin
- ☐ TeamViewer

Вопрос 5. В одном из кейсов, расследованных Solar 4RAYS, группировка Obstinate Mogwai применяла уязвимость в распространенной технологии. Что это была за технология?

- ☐ Почтовый сервер
- ☐ VPN
- ☐ Среда .Net
- ☐ ActiveX

Ответы: Gorgon, DDR (Dead Drop Resolver), Obsidium, Velociraptor, Среда .Net

4RAYS by SOLAR

Инструменты, которые применяют группировки

APT-группировки обладают практически неограниченными ресурсами и постоянно совершенствуют свои тактики, техники и процедуры, чтобы быть на шаг впереди стороны защиты.

Примеры:

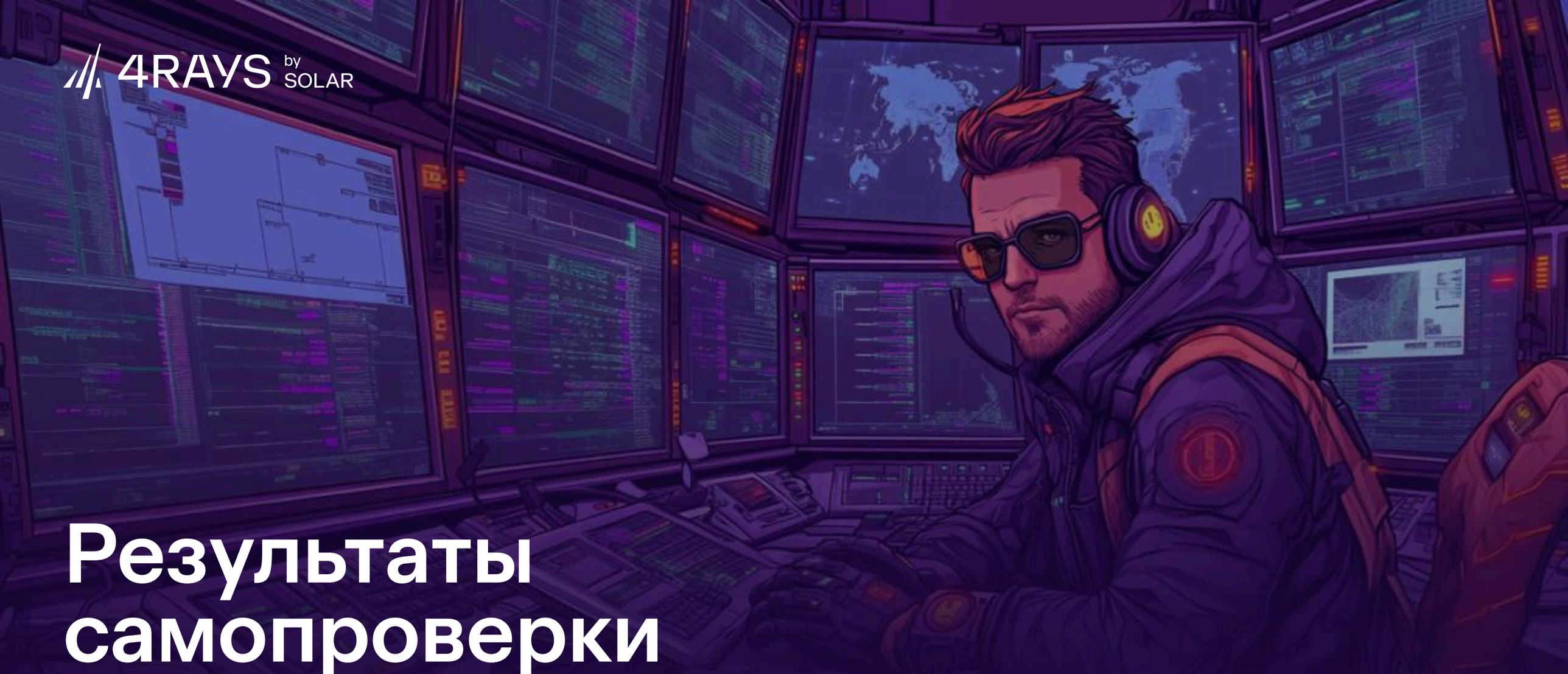
Решения для туннелирования трафика, которые позволяют обойти файрволы и организовать связь там, где ее не должно быть:

- gsocket (gs-netcat)
- ngrok
- nhas reverse ssh
- revsocks
- resocks
- chisel
- neo-regeorg

Различные RAT-утилиты, предоставляющие удаленное управление хостом жертвы:

- Bulldog backdoor (go-red)
- Facefish rootkit
- Kitsune rootkit
- Sliver
- CobInt
- Cobalt Strike
- Mythic
- DFK RAT
- Trochilus RAT
- Donnect
- Dimano RAT

4RAYS by SOLAR



Результаты самопроверки

Если вы ответили верно менее, чем на 5 вопросов, то вероятно вы не получаете все знания об актуальных киберугрозах.

Как применять знания о киберугрозах

1

Обеспечьте мониторинг угроз

Интегрировать актуальные IoC и TTP в SIEM/SOAR и TI-платформы для автоматического обнаружения и реагирования на угрозы.

2

Анализируйте киберландшафт

Отслеживать активность APT и других группировок в регионе, чтобы прогнозировать возможные атаки и адаптировать защиту.

3

Выявляйте следы компрометации

Регулярно проверять инфраструктуру на наличие следов взлома, используя DFIR-методики для быстрого выявления и нейтрализации атак.

4RAYS by SOLAR

Хотите получать знания о самых опасных угрозах в режиме реального времени?

Solar TI Feeds – потоки данных (фидов) об актуальных угрозах.

- Широта и уникальность баз данных угроз в РФ
- Интеграция с СЗИ и кастомизация срезов
- Повышение скорости расследования благодаря полному контексту киберугроз
- Знания о вредоносных кампаниях в режиме реального времени

Получите непрерывное усиление SOC с помощью уникальных фидов для раннего обнаружения и реагирования на угрозы.

Узнать о фидах

W: RT-SOLAR.RU/SOLAR-4RAYS

T: 8 (800) 302-85-23