Как изменились действия злоумышленников в 2020 году

Артем Кильдюшев
Руководитель группы пресейла Solar JSOC
компании «Ростелеком-Солар»

Ростелеком
Солар

Что анализировали?

1. Выявленные инциденты у клиентов в рамках сервисов Solar JSOC
2. Инциденты, расследуемые командой Solar JSOC CERT
3. Информация, собранная на honeypot
4. Информация, полученная в рамках информационного обмена

Ростелеком
Солар

Киберпреступники постоянно совершенствуются

+40%

рост атак на получение контроля над инфраструктурой организации

55,4%

событий ИБ удается выявить лишь с помощью сложных интеллектуальных средств защиты или анализа событий

По данным Solar JSOC, 2019 г.

63%

всех атак являются целенаправленными

По данным Positive Technologies, 2020 г.

1 из 5

ВПО, доставляемое с фишингом, имеет встроенный инструментарий обхода песочницы

По данным Solar JSOC, 2019 г.

17%

компаний способны эффективно сопротивляться кибератакам

По данным Accenture, 2020 г .

207 дней

среднее время обнаружения компанией взлома ее инфраструктуры

По данным Ponemon Institute, 2020 г.

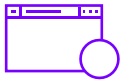
Ростелеком
Солар

Киберландшафт-2020

Рост квалификации злоумышленников

Усложнение инструментария

Повышение темпа использования новых уязвимостей



Длительное присутствие в инфраструктуре

Итог: расслоение подходов злоумышленников к атакам на инфраструктуру

Уровни злоумышленников

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
1	Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
2	Киберхулиган/ Энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
3	Киберкриминал/ Организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, социнжиниринг
4	Кибернаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
5	Группировки, спонсируемые государствами	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные "закладки"

Ростелеком
Солар

Общие тренды

Атаки на периметр

- Брутфорсы RDP
- Взлом WEB

Фишинг

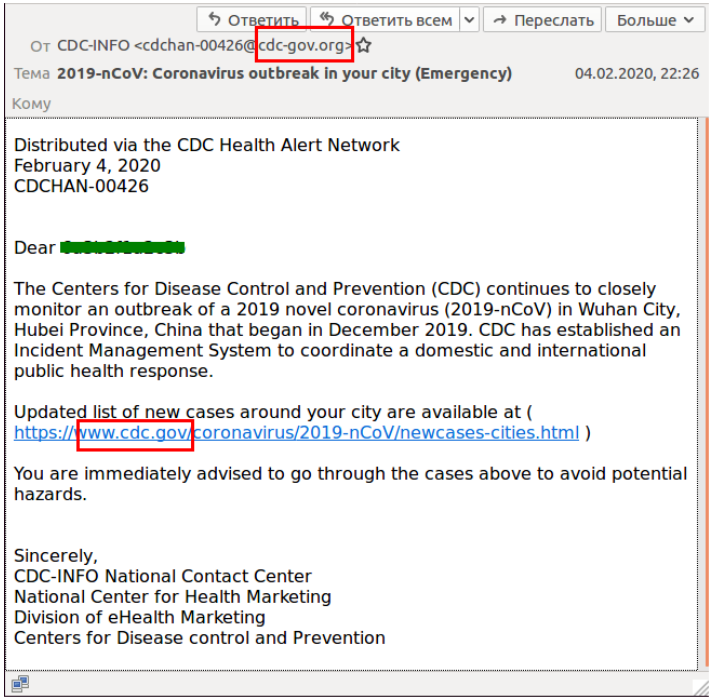
- Использование тематики Covid-19 в APT и массовых рассылках

Атаки на удаленных пользователей

- Компрометация данных VPN
- Взлом и заражение домашних устройств

Атаки на supply chain

- Jump server – единые точки входа подрядчиков в инфраструктуру
- Прямой взлом подрядчика


Ответить | Ответить всем | Переслать | Больше

От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

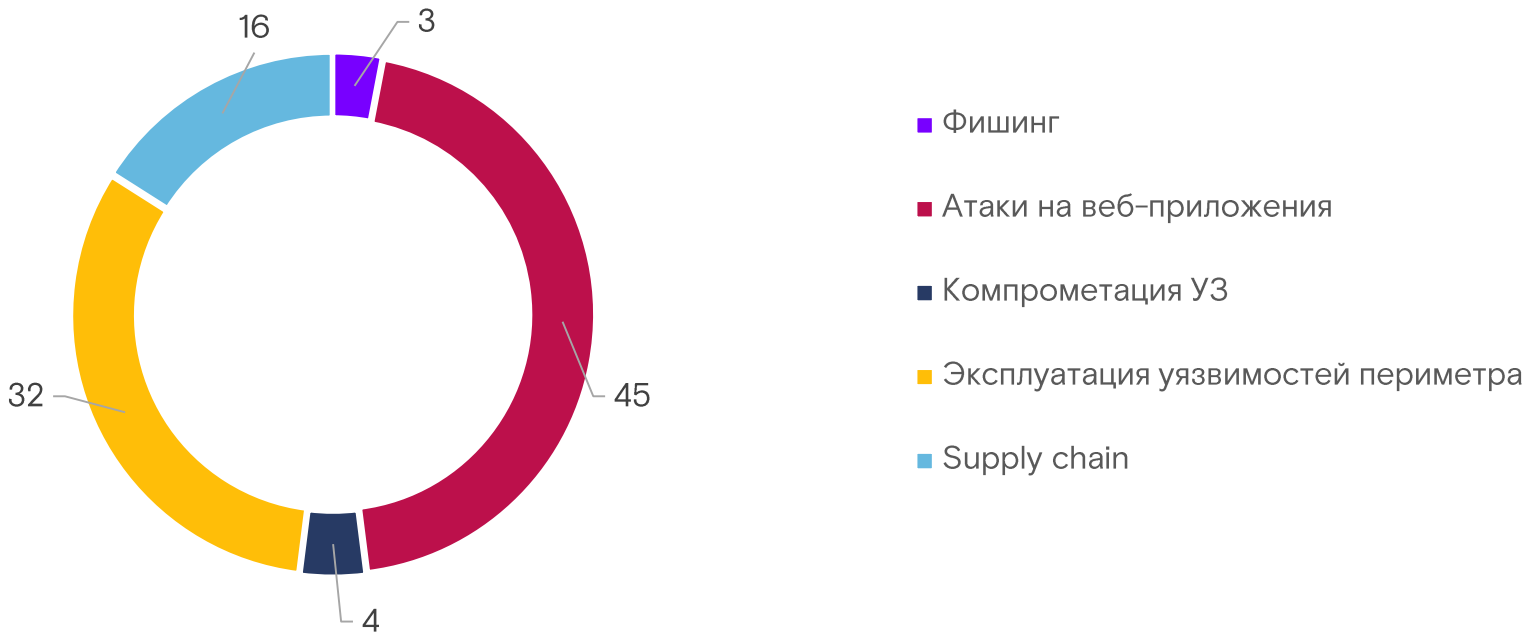
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Ростелеком
Солар

Статистика по группировкам среднего уровня

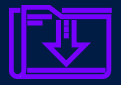
Ростелеком
Солар

Статистика по группировкам высокого уровня



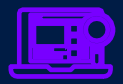
Ростелеком
Солар

Основные техники закрепления и распространения

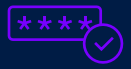


Механизмы автозагрузки

Системные службы

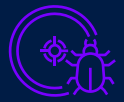


Формирование собственных драйверов



Использование удаленных сервисов

Pass the Ticket / Pass the Hash



Использование WMI для работы ВПО

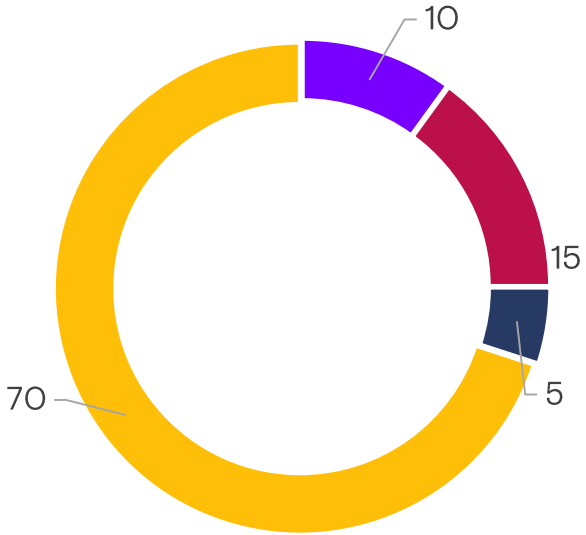
Использование ОС для работы инструментария BITS-задач

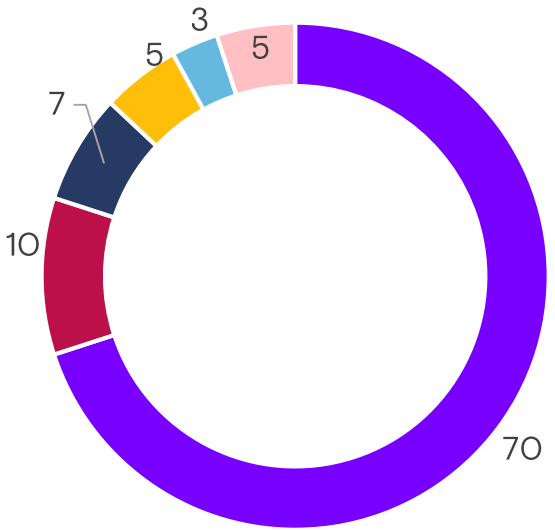
Использование планировщика задач

Эксплуатация уязвимостей удаленных сервисов

Ростелеком
Солар

Техники закрепления

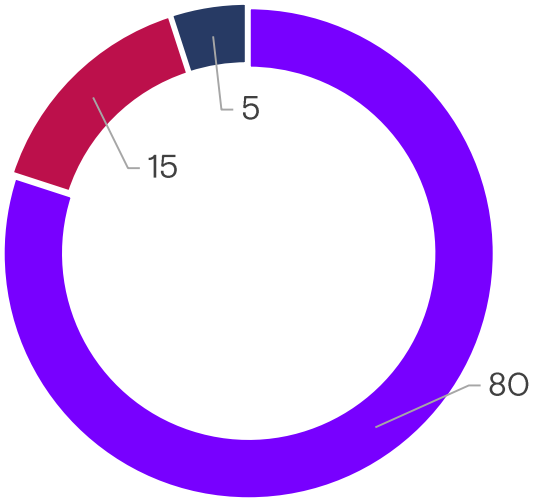


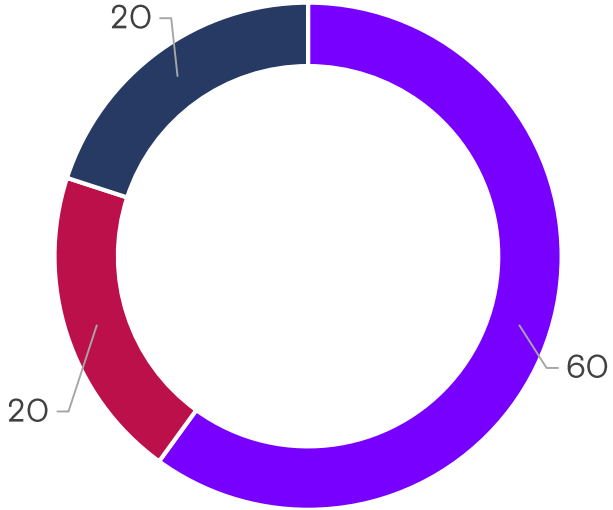


- Системные службы
- Использование BITS-задач
- Формирование собственного драйвера
- Использование планировщика задач
- Механизмы автозагрузки
- Использование WMI

Ростелеком
Солар

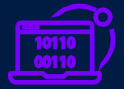
Техники распространения





- Использование удаленных сервисов
- Pass the Ticket / Pass the Hash
- Эксплуатация уязвимостей удаленных сервисов

Подходы к реализации



Самописное бинарное ВПО

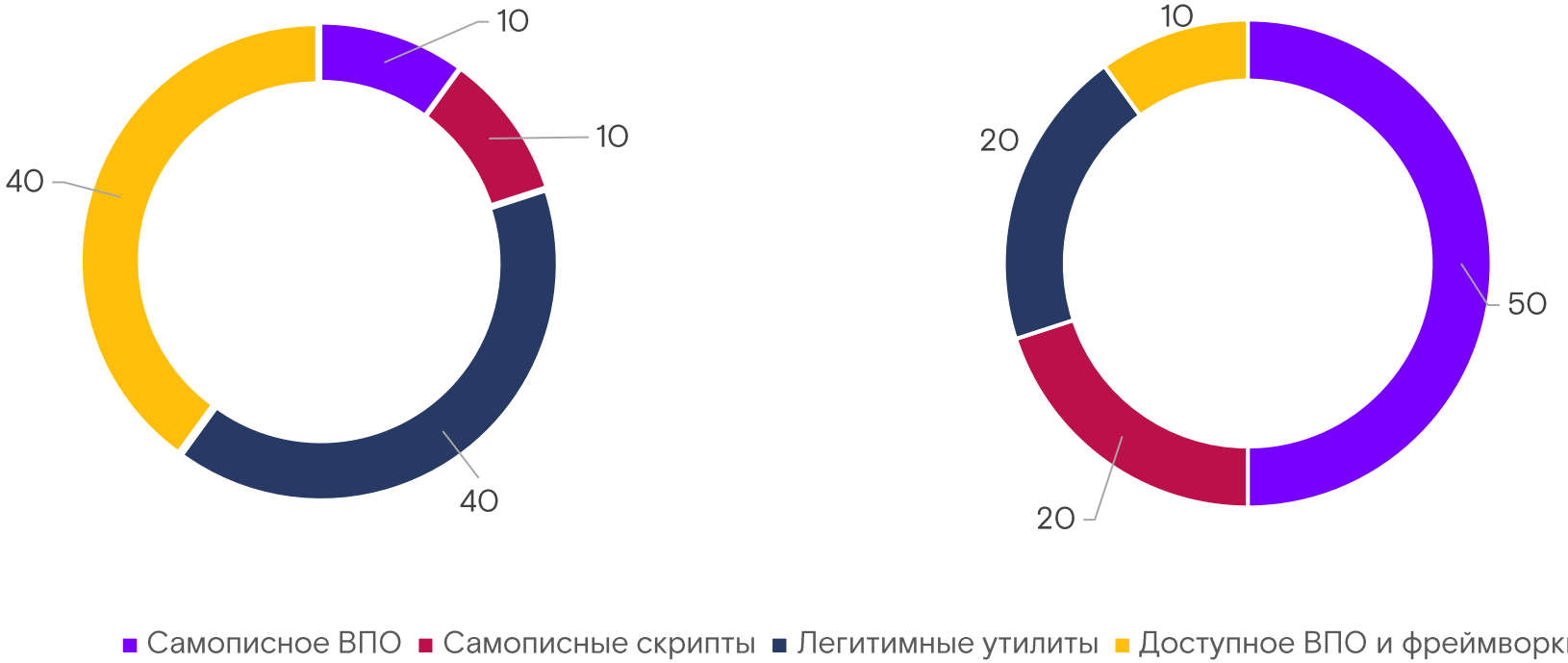
Использование легитимных утилит

Самописные скрипты

Инструменты для анализа защищенности, доступное ВПО

Ростелеком
Солар

Подходы к реализации



Ключевые цели инфраструктуры злоумышленников среднего уровня

80% АРМ и транзитные серверы

85% Контроллер домена

75% АРМ ИТ-администраторов

65% Системы ИТ-управления инфраструктурой

40% Системы ИБ-управления инфраструктурой

45% Прикладные системы, хранящие финансовую информацию

Ростелеком
Солар

Ключевые цели инфраструктуры злоумышленников высокого уровня

85% Почтовые серверы

70% Контроллер домена

70% АРМ первых лиц и их заместителей

80% АРМ ИТ-администраторов

75% Системы ИТ-управления инфраструктурой

50% Системы ИБ-управления инфраструктурой

65% Системы документооборота

65% Серверы и технологические рабочие станции управления технологическими процессами

Ключевые выводы

Существенный рост числа атак на субъекты КИИ

Рост числа потенциально опасных утилит в открытом доступе

Необходимость в сложных системах защиты

Ростелеком
Солар

Вопросы спикеру

Артем Кильдюшев

Руководитель группы пресейла Solar JSOC
компании «Ростелеком-Солар»

Контакты
+7 (499) 755-07-70
presale@rt-solar.ru

Ростелеком
Солар