«Ростелеком-Солар»: пирамида боли Threat Intelligence в жизни коммерческого SOC

Владимир Дрюков
Директор центра противодействия кибератакам Solar JSOC

Ростелеком
Солар

Solar JSOC

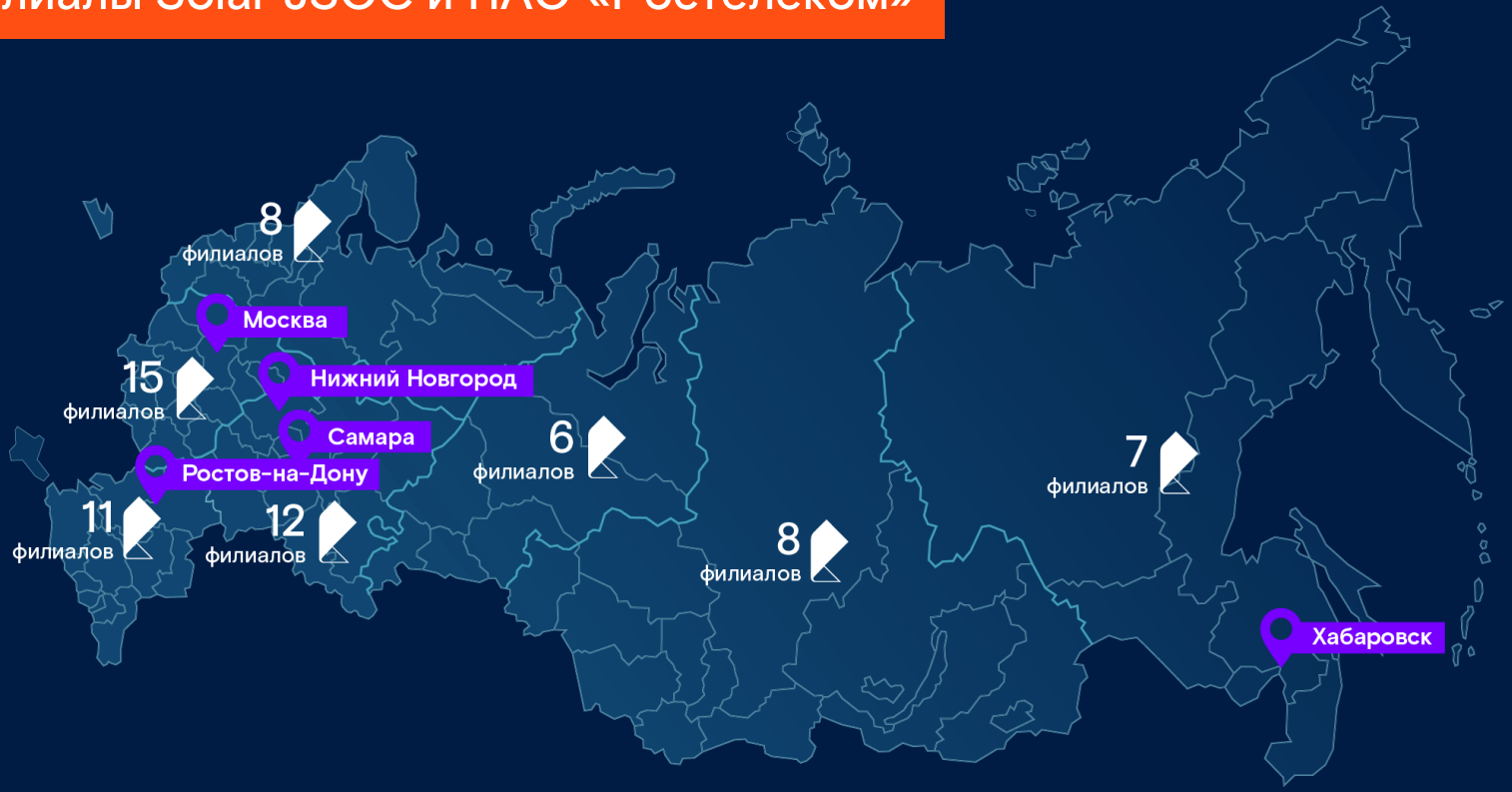
№1
на рынке SOC
В России

350+
экспертов
кибербезопасности

140+
клиентов из всех
отраслей экономики

110+
млрд анализируемых
событий ИБ в сутки

Филиалы Solar JSOC и ПАО «Ростелеком»



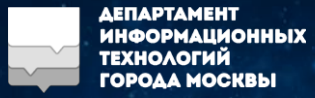
ПАО «Ростелеком»

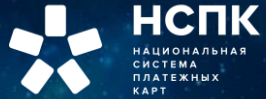
Филиалы Solar JSOC

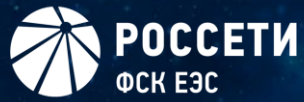
Ростелеком
Солар

У Solar JSOC более 140 клиентов

Тинькофф Банк







Администрация Волгоградской области

Министерство ИТ и связи Хабаровского края

Региональный центр кибербезопасности Самарской области

Ростелеком
Солар

Экосистема сервисов Solar JSOC

Мониторинг и анализ инцидентов ИБ

- Мониторинг инцидентов ИБ
- Анализ сетевого трафика (NTA)
- Защита конечных точек (EDR)
- Мониторинг бизнес-систем
- Мониторинг АСУ ТП

Расследование и реагирование на инциденты ИБ

- Управление процессами реагирования на киберинциденты (IRP)
- Разработка плейбуков для реагирования
- Incident Response
- Техническое расследование инцидентов ИБ

Комплексный контроль защищенности

- Тест на проникновение
- Red Teaming
- Комплексный анализ защищенности
- Социотехническое исследование
- Анализ рисков и обследование инфраструктуры
- Оценка зрелости технической защиты

Анализ угроз и внешней обстановки

- Киберразведка
- Threat Hunting (Solar JSOC CERT)
- Крупнейшая в России база Threat Intelligence

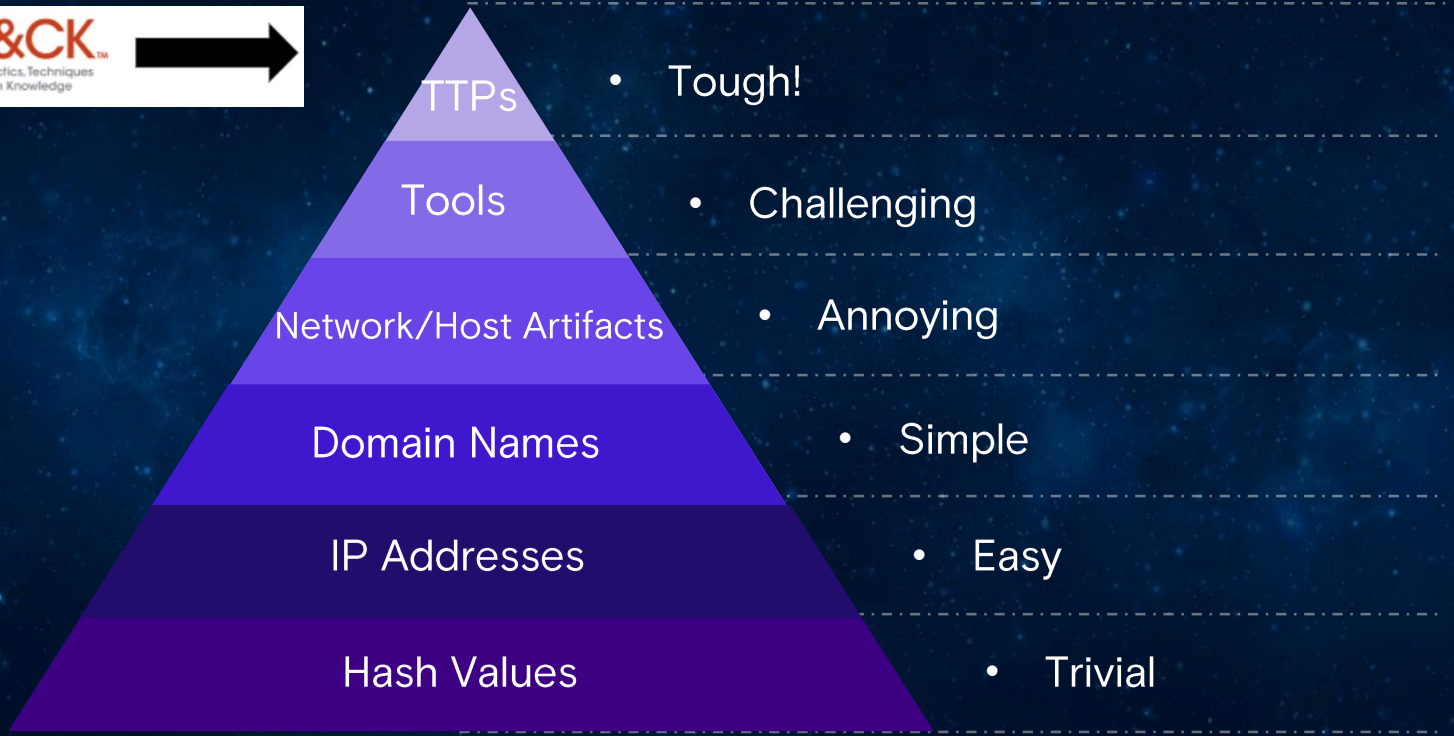
Построение SOC и его частных процессов

- Построение SOC
- Консалтинг

Ростелеком
Солар

Пирамида боли Threat Intelligence

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge



Источник: http://detect-respond.blogspot.com/

Ростелеком
Солар

Базовые IoC

- Индикаторов очень много
- Они легко и просто изменяются:
  - Новые IP или домены – пара дней
  - Email – 3 секунды
  - Hash, process – пересборка ВПО
- Индикаторы являются признаками конкретной атаки, а не группировки

Добавлены в мониторинг новые индикаторы IoCs:	IP-адрес	**+ 12 345**
	FQDN/URI	**+ 2 356**
	Реестр	**+ 34**
	File Hash	**+ 145**
	Email	**+ 1 257**
	Process	**+ 48**
Добавлено новых exit-нод TOR-сети:		**+ 256**

Ростелеком
Солар

Практическая работа с индикаторами

Тип индикатора	Источник детектирования	Типовые способы работы	Стоит учесть
IP-адрес	FW	Блокировка высоковероятных, мониторинг всего	Хостинги и облака
FQDN/URI	Proxy, UTM	Блокировка высоковероятных, мониторинг всего	Массовый https
Реестр	EDR, Sysmon	Мониторинг, если получится	Почти всегда – малое покрытие
File Hash	Информация от антивируса, EDR, Sysmon, некоторые DLP	Мониторинг, если получится	Почти всегда – малое покрытие
Email	Mail security	Блокировка + мониторинг	
Process	EDR, Sysmon	Мониторинг, если получится	Почти всегда – малое покрытие

Ростелеком
Солар

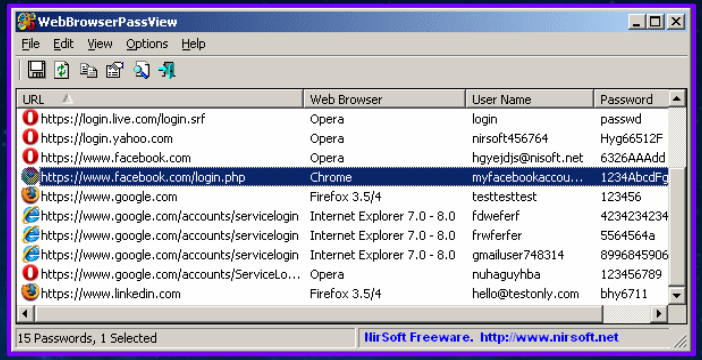
Но с профессионалами все гораздо сложнее

	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»

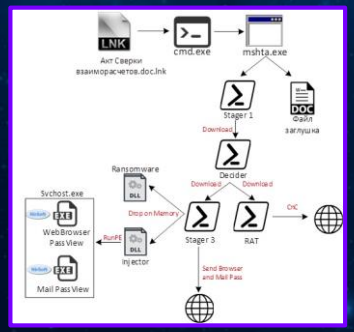
Ростелеком
Солар

Старые идеи. Новые механики

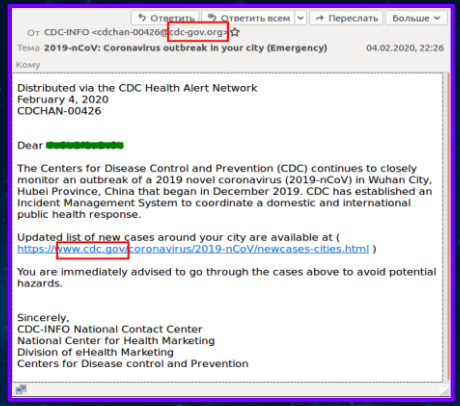
1



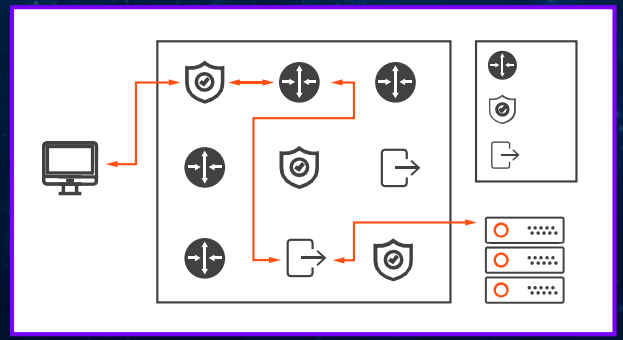
2



3



4



Ростелеком
Солар

«Ростелеком» и НКЦКИ выявили серию масштабных кибератак на российские органы государственной власти

12/05/21

Ростелеком
Солар

Инструментарий атаки

1 Вредоносное программное обеспечение, не детектируемое антивирусом

- 13 различных вирусных семейств разного назначения
- Более 120 уникальных образцов

2 Максимальная локализация атаки под инфраструктуру РФ

- Работа с российскими облачными сервисами с полным изучением API для взаимодействия
- Активное изучение и обход средств защиты

Ростелеком
Солар

Шаг в сторону TTP

Источники информации:
- Коммерческие APT-репорты
- Разборы атак и деятельности группировок от исследовательских компаний
- Собственные исследования

Анализ группировки или атак:
- Использование конкретных инструментов или утилит (RAT, PowerShell-скрипты, когда-то Mimikatz)
- Используемые методы закрепления (уязвимости, способы повышения привилегий)
- Подходы к lateral movement (уязвимости, нестандартные протоколы)

Инструменты выявления:
- Sysmon, EDR
- NTA, внутренний IDS

Ростелеком
Солар

Гонка за матрицей MITRE

	Категория	Tech.ID	Ссылка на описание
Process DLL Injection	Privilege Escalation	T1055	https://attack.mitre.org/techniques/T
Remote File Copy with BITSadmin	Defense Evasion, Persistence	T1197	https://attack.mitre.org/techniques/T
VShadow Code Execute	Defense Evasion, Execution	T1218	https://attack.mitre.org/techniques/T
Create Junction Folders	Persistence		https://wikileaks.org/ciav7p1/cms/pa
CLSIDs Registry Modification	Defense Evasion, Persistence	T1122	https://attack.mitre.org/techniques/T
SCM and DLL Hijacking Process	Lateral Movement		https://posts.specterops.io/lateral-m
Normal.dotm changed	Persistence		https://enigma0x3.net/2014/01/23/m
Control Panel Items	Defense Evasion, Execution	T1196	https://attack.mitre.org/techniques/T
InstallUtil	Defense Evasion, Execution	T1118	https://attack.mitre.org/techniques/T
Signed Script Proxy Execution	Defense Evasion, Execution	T1216	https://attack.mitre.org/techniques/T
DHCP Callout DLL	Defense Evasion	T1073	https://attack.mitre.org/techniques/T
DNS Server Plugin has been loaded	Defense Evasion		https://blog.3or.de/hunting-dns-serv
Compiled HTML File	Execution	T1223	https://attack.mitre.org/techniques/T
Indicator Removal on Host	Defense Evasion	T1070	https://attack.mitre.org/techniques/T
Indirect Command Execution	Defense Evasion	T1202	https://attack.mitre.org/techniques/T
Signed Binary Proxy Execution	Execution	T1218	https://attack.mitre.org/techniques/T
Change Default File Association	Persistence	T1042	https://attack.mitre.org/techniques/T
UAC Bypass Dll Hijacking File Modi	Defense Evasion	T1088	https://attack.mitre.org/techniques/T
UAC Bypass Dll Hijacking Process S	Defense Evasion	T1088	https://attack.mitre.org/techniques/T
UAC Bypass Dll Hijacking Process In	Defense Evasion	T1088	https://attack.mitre.org/techniques/T
Process execution as System	Privilege Escalation	T1068	https://attack.mitre.org/techniques/T
UAC Bypass with wusa.exe	Defense Evasion	T1088	https://attack.mitre.org/techniques/T
UAC Bypass Sysprep WinSxS	Defense Evasion	T1088	https://attack.mitre.org/techniques/T
UAC Bypass Shim Redirection	Defense Evasion	T1088	https://attack.mitre.org/techniques/T
UAC Bypass Parent Process Start	Defense Evasion	T1088	https://attack.mitre.org/techniques/T

Дорогу осилит идущий

Ростелеком
Солар

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Узнать подробнее или заказать сервис

presale@rt-solar.ru

Ростелеком
Солар