Техники и тактики киберпреступников

Отчет Solar JSOC CERT

rt-solar.ru
rt.ru

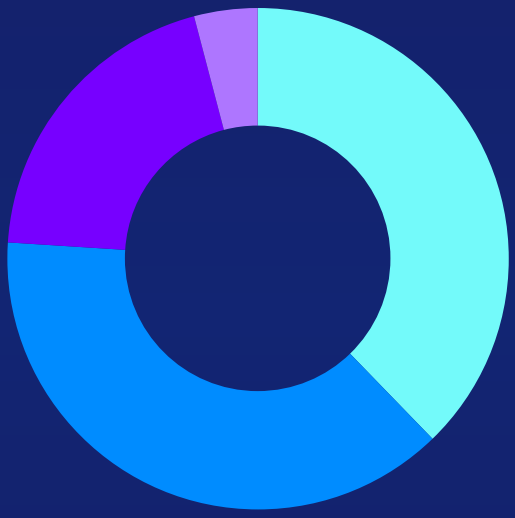
Ростелеком
Солар

Об отчете

Отчет построен на расследованиях, проведенных командой Solar JSOC CERT с марта 2022 по март 2023 г. Он содержит общую информацию обо всех типах инцидентов и данные об основных техниках и тактиках злоумышленников. Всего за отчетный период было разобрано 40 инцидентов, связанных с проникновением в ИТ-инфраструктуру различных компаний и организаций.

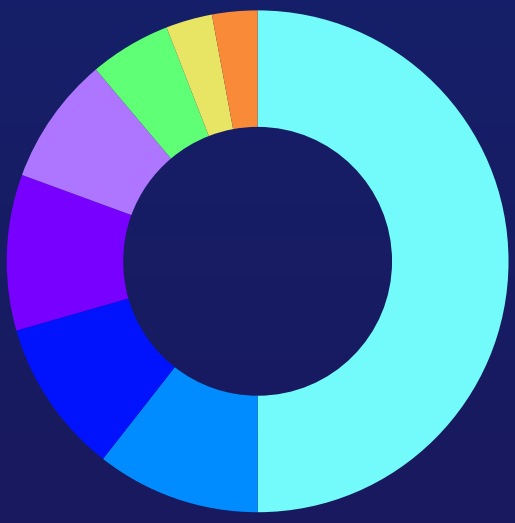
Мы выбрали 3 основных тактики, на которых базируется большинство правил детектирования вредоносной активности в различных средствах защиты информации.

Ключевые цели атакующих



- 38% Шифрование инфраструктуры для получения денежного вознаграждения
- 38% Хактивизм
- 20% Взлом инфраструктуры с целью кибершпионажа APT-группировками
- 4% Остальное

Отраслевая принадлежность пострадавших организаций



- 51% Госсектор
- 10% Промышленность
- 10% Сельское хозяйство
- 10% Телеком
- 8% Торговля и услуги
- 5% Энергетика
- 3% НКО
- 3% Финансы

Ключевые цифры

72%

кейсов связано с проникновением хакеров в инфраструктуру через известные уязвимости

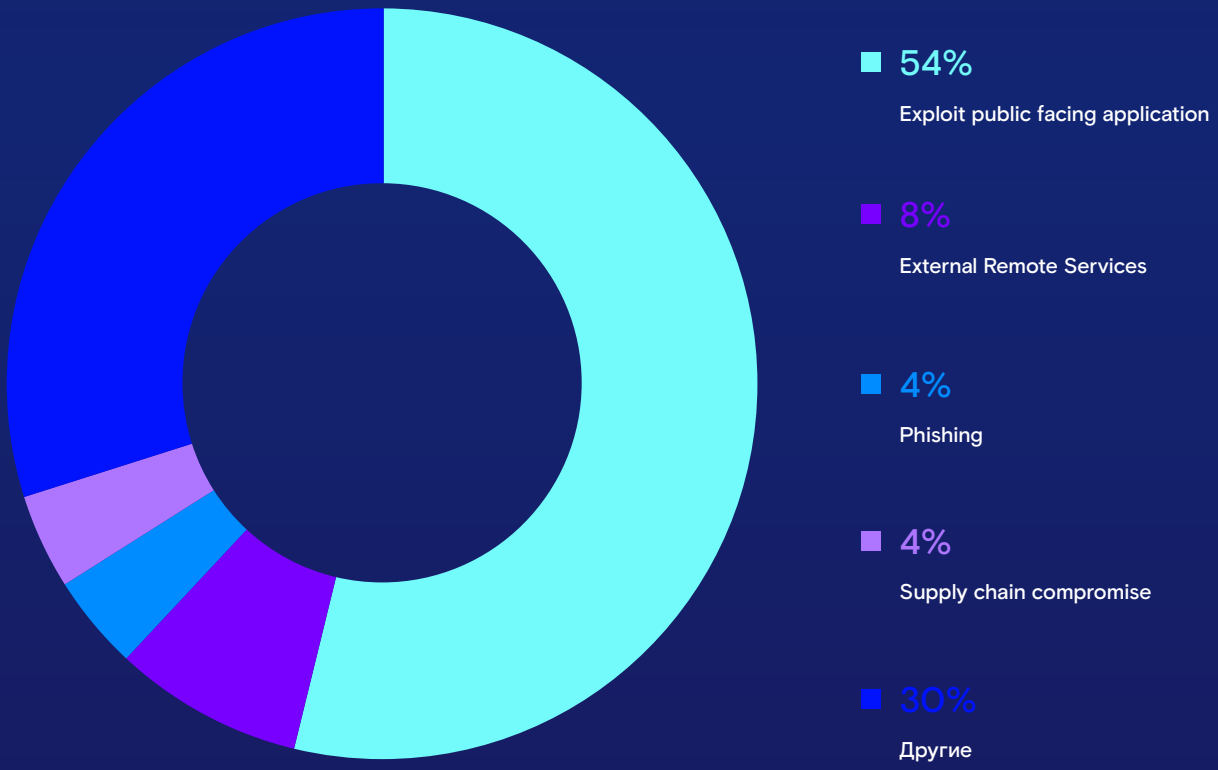
7 дней

в среднем требовалось хакерам для достижения конечной цели атаки

в 5 раз

за год выросло число атак хактивистов

Первоначальный доступ получен через



Шифрование инфраструктуры с целью получения денежного вознаграждения

С атаками подобного типа столкнулись компании из самых разных отраслей, включая госсектор, сельское хозяйство, ритейл, высшее образование, благотворительность.

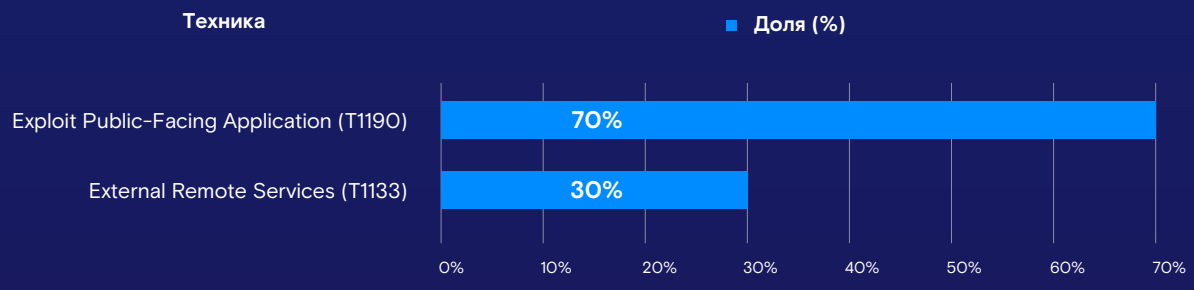
Инструментарий, используемый злоумышленниками для шифрования систем внутри инфраструктуры

- Phobos
- VoidCrypt
- Cring
- Spook
- BitLocker
- Conti

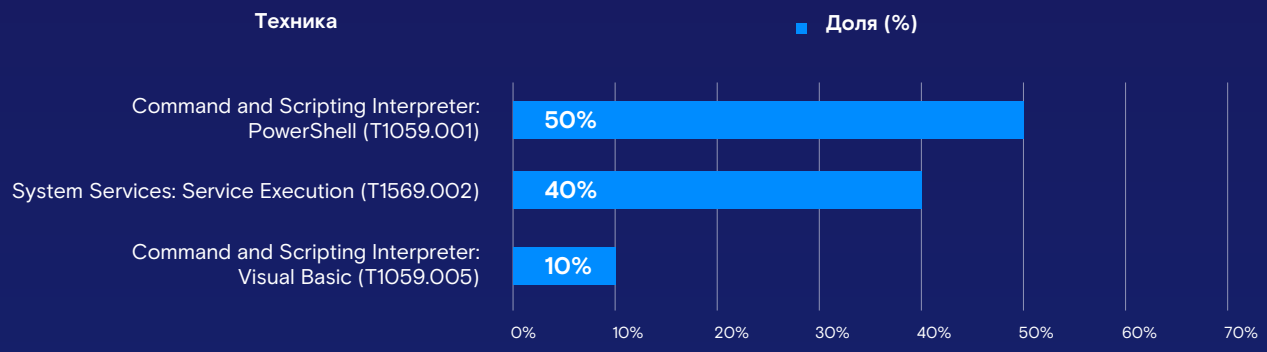
Дополнительно используемый инструментарий

- Cobalt Strike
- Mimikatz
- NLBrute
- Ligolo-ng
- FRPC
- Impacket
- Sysinternals Suite

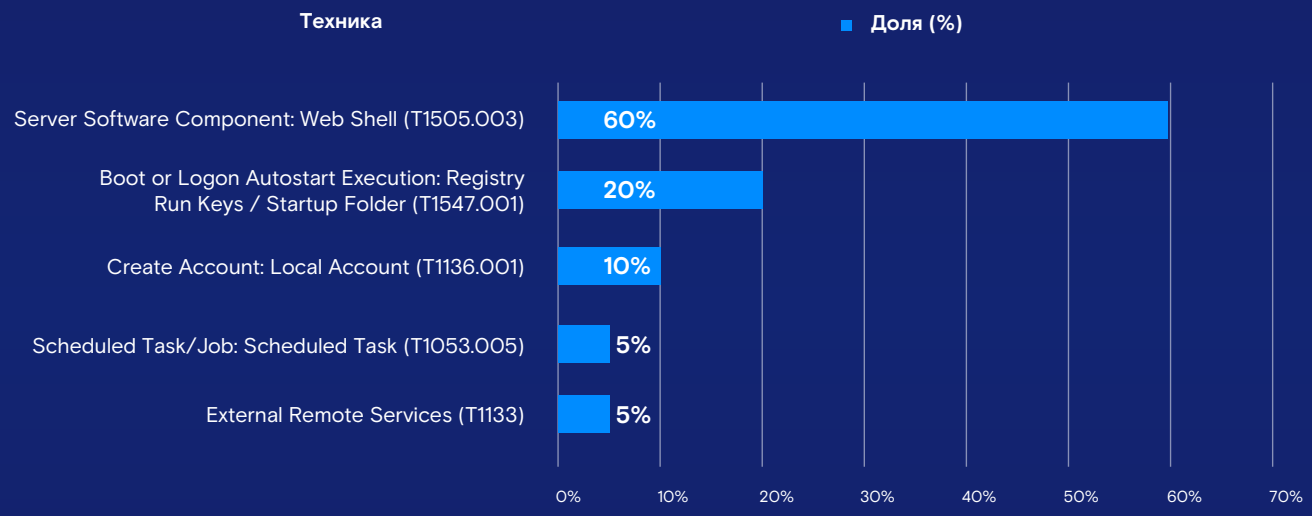
Initial Access (Первичный доступ)



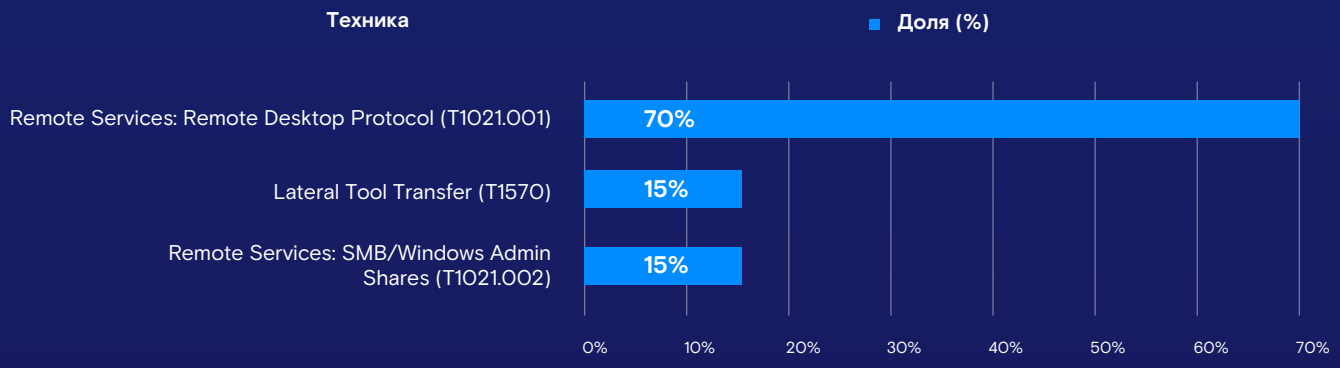
Execution (Исполнение)



Persistance (Закрепление)



Lateral Movement (Горизонтальное передвижение)



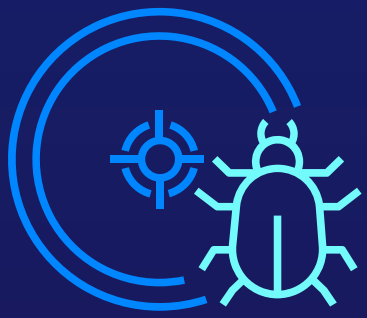
В большинстве (70%) проектов первоначальный доступ в инфраструктуру был реализован через уязвимости в сервисах, доступных из интернета. Самой частой уязвимостью такого типа является ProxyLogon (критическая уязвимость в Microsoft Exchange Server).

Она позволяет реализовать сразу два вектора:

- быстро получить доступ к переписке пользователей (в том числе уровня топ-менеджмента) для ее дальнейшей публикации или шантажа с требованием выкупа;
- проникнуть в инфраструктуру и развивать атаку уже внутри сети жертвы.

Несмотря на простоту эксплуатации и широчайшее распространение MS Exchange как продукта, многие компании не спешат закрывать уязвимость на периметре, чем и пользуются злоумышленники.

В целом объем расследуемых Solar JSOC CERT инцидентов с использованием шифровальщиков остался на уровне 2020–2021 годов. Единственное отличие заключается в том, что в 2022 году в этой категории нами не было замечено инцидентов, начинавшихся с фишинговых писем. Это может быть связано с тем, что с начала СВО компании оперативно настроили базовое антивирусное ПО, которое защитило их от массовых вредоносных рассылок.

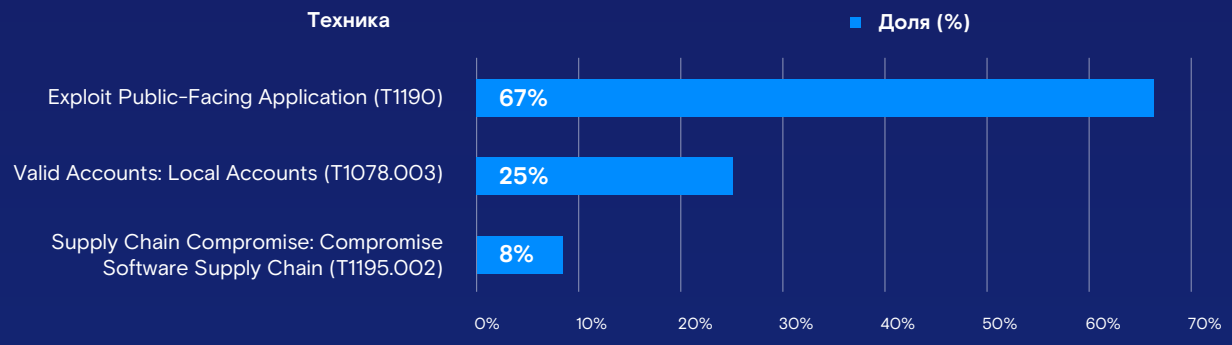


Хактивизм

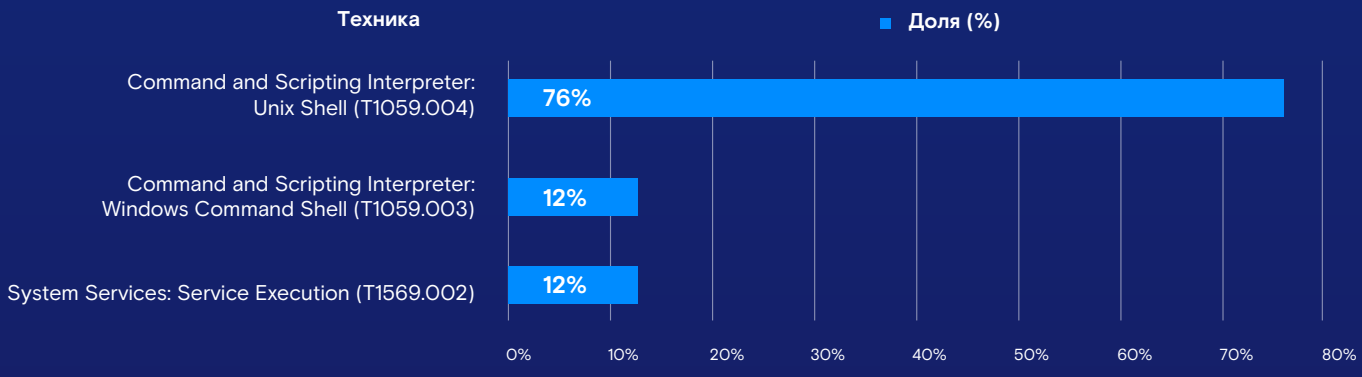
Дополнительно используемый инструментарий

- Cobalt Strike
- Mimikatz
- Impacket
- AnyDesk

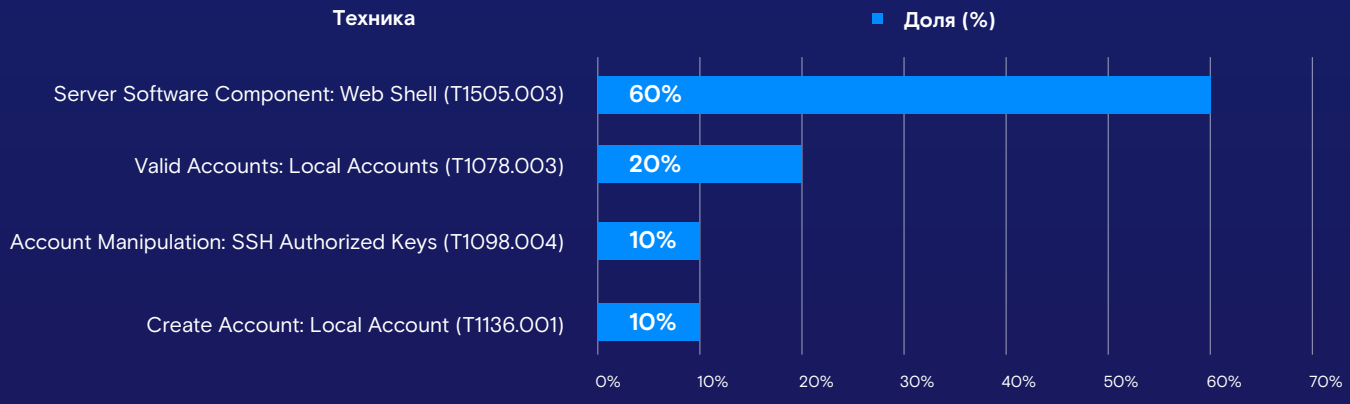
Initial Access (Первичный доступ)



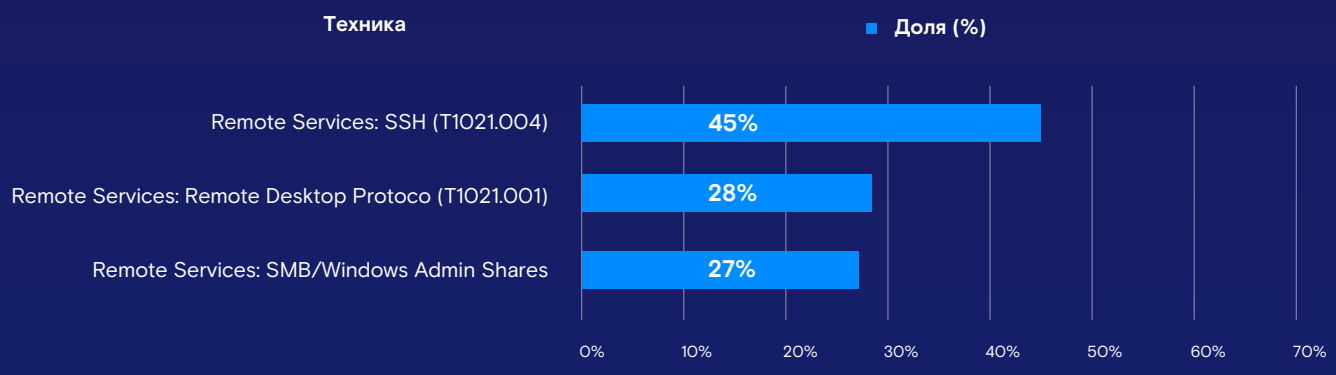
Execution (Исполнение)



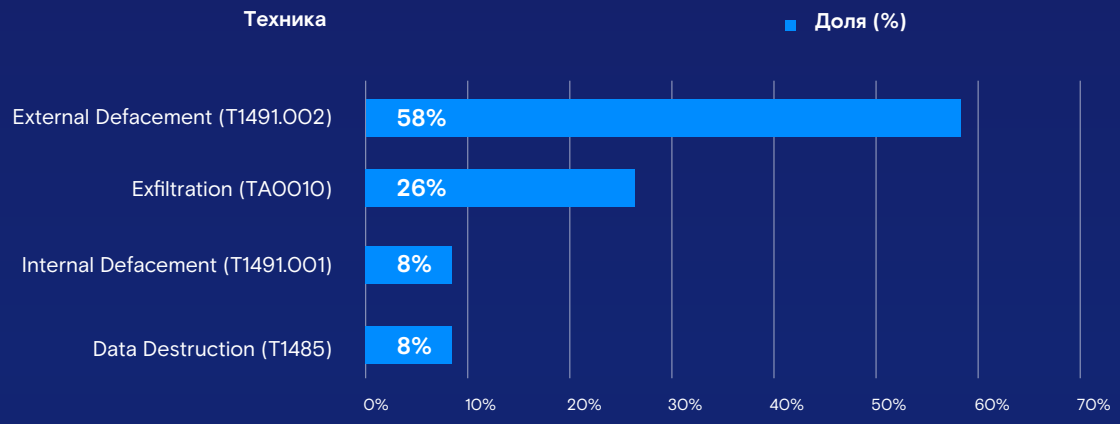
Persistance (Закрепление)



Lateral Movement (Горизонтальное передвижение)



Impact (Достижение цели)



Хактивизм – главный тренд 2022 года. С технической точки зрения (используемый инструментарий, тактики и техники) инциденты данной категории не отличались особой сложностью, однако их было в 5 раз больше в сравнении с предыдущим годом. К IV кварталу 2022 года количество таких атак начало снижаться. Мотивация хактивистов стала падать, а часть тех, кто остался, начали повышать свою квалификацию и объединяться под началом профессионалов.

Согласно нашей статистике, чаще всего с атаками хактивистов сталкивались госсектор, финансы, телеком и энергетика. Как правило, это были популярные организации, известные широкой общественности, атаки на которые могут вызвать резонанс.

Как и в кейсах с шифрованием, подавляющее большинство атак начиналось с эксплуатации уязвимостей в веб-сервисах. В частности, в наших расследованиях мы встречали взломы таких популярных сервисов, как Exchange, WowzaStreamingEngine, Horizon, Apache, Oracle WebLogic Server, Bitrix, Joomla, Drupal. Далее следовал дефейс сайта, безвозвратное шифрование (без требования выкупа) и кража данных.

Взлом инфраструктуры с целью кибершпионажа APT-группировками

Предполагаемый список обнаруженных нами группировок

- APT27
- APT41
- APT10
- Lazarus Group

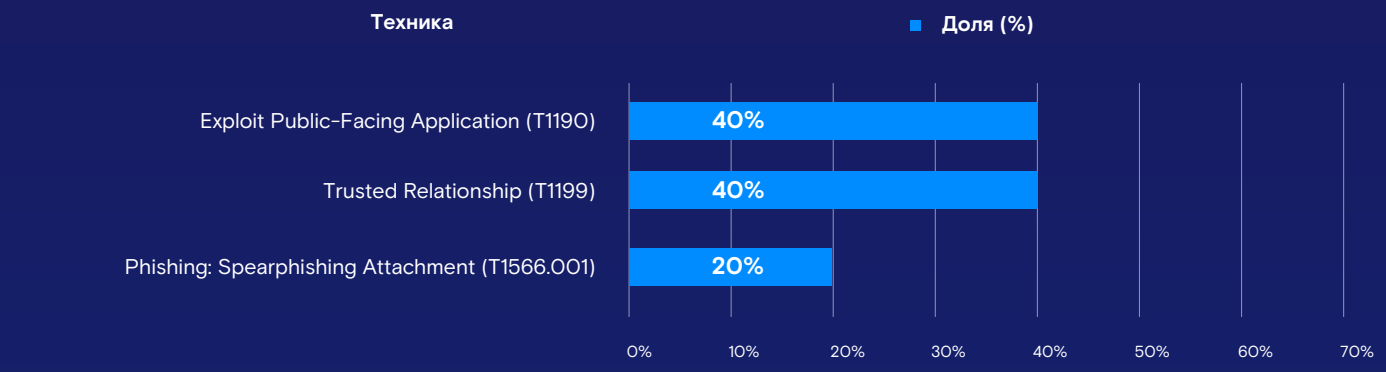
Вредоносный инструментарий, используемый указанными группировками в инцидентах

- PlugX
- Light Shadowpad
- Mirage
- Microcin
- GhOst Rat
- MATA Framework

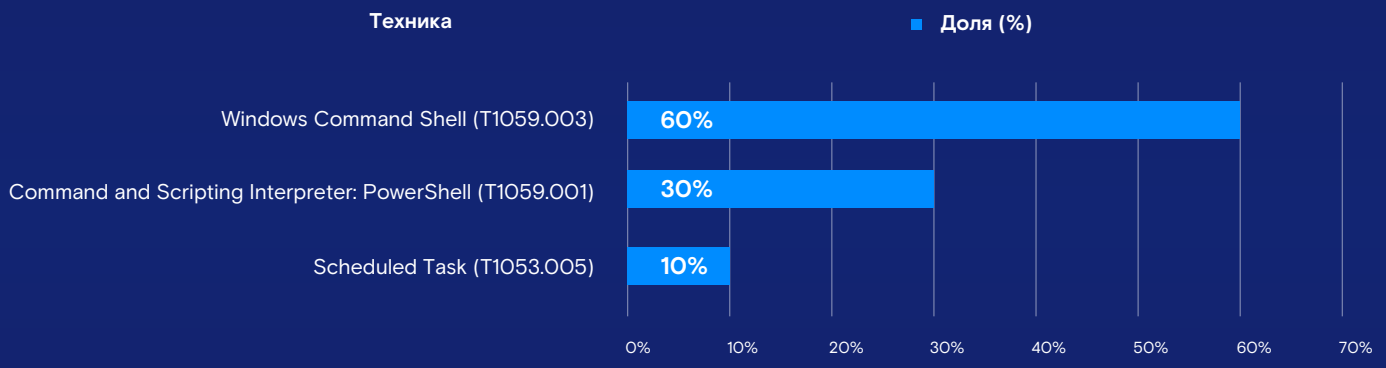
Дополнительно используемый инструментарий

- Impacket
- Mimikatz
- Cobalt Strike
- SharpHound
- noPac
- SMBScan
- Nbtscan
- EarthWorm
- Rubeus
- Go-SOCKS5
- Rssocks

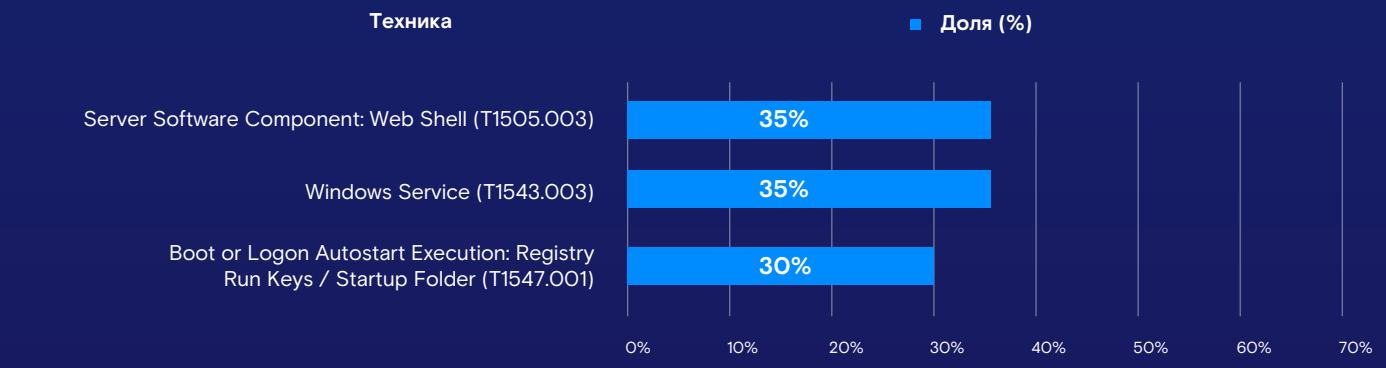
Initial Access (Первичный доступ)



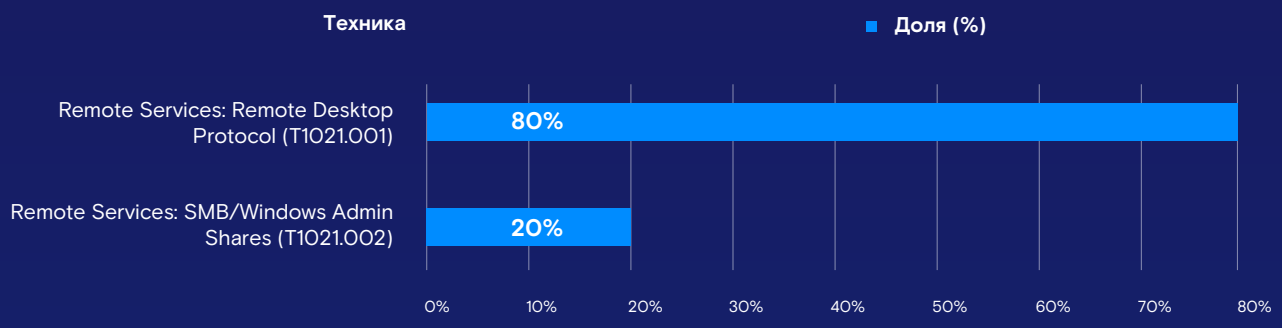
Execution (Исполнение)



Persistance (Закрепление)



Lateral Movement (Горизонтальное передвижение)



Основными целями APT-группировок стали органы госвласти.

В целом инциденты, связанные с проникновением APT-группировок в инфраструктуры компаний, остаются на уровне предыдущих лет. Также сохраняется разнообразие способов получения первичного доступа.

Особенностью 2022 года является то, что расследований, связанных с проникновением в инфраструктуру через подрядные организации, стало больше, чем через заражение классическим фишинговым письмом. В начале года злоумышленники активно атаковали наиболее незащищенных подрядчиков и через них добирались до изначальных целей. После небольшого затишья был новый всплеск подобных атак, связанный с тем, что основные цели хакеров – КИИ – значительно повысили свою защищенность и злоумышленникам пришлось вновь искать слабые места через подрядчиков.

Выводы

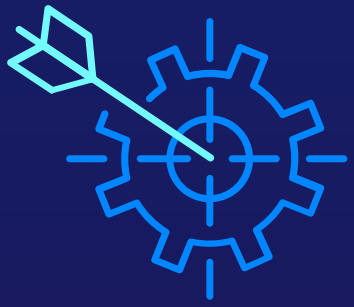
- Помимо основной активности (шифрования или майнинга), злоумышленники массово размещали манифесты, относящиеся к СВО. В итоге в 5 раз выросло количество атак, связанных с хактивизмом.

- Самые популярные векторы проникновения в инфраструктуру жертвы – эксплуатация уязвимостей (часто известных уже несколько лет), атаки через подрядчиков (supply chain и trusted relationship), компрометация данных пользователей, фишинг.

- Скорость атак изменилась драматически. Если раньше от входа злоумышленника в инфраструктуру до взлома и кражи денег или данных проходили месяцы, то сейчас для достижения цели хакерам в среднем требуется 7 дней.

- Менее профессиональные хакеры стали объединяться под началом злоумышленников с высокой квалификацией, а различные инструменты для реализации атак все чаще бесплатно распространяются на форумах в даркнете или в ТГ-каналах.

- Выросла активность проправительственных APT-группировок. Их интересы уже давно не ограничиваются федеральными и региональными органами власти. Мы встречаем их в инфраструктурах энергетических компаний и даже СМИ. В то же время на фоне постоянных кибератак сотрудники ИБ-служб стали внимательнее относиться к инцидентам, что позволило гораздо оперативнее выявлять более профессиональных злоумышленников и их передвижение по сети.



Ростелеком
Солар

rt.ru
rt-solar.ru

Email:
solar@rt-solar.ru

Телефон:
+7 (499) 755-07-70