www.cyberok.ru
info@cyberok.ru

Сравнение систем класса External Attack Surface Management

Пушкин Максим,

специалист направления
развития экспертизы CyberOK

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Оглавление

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Введение

В современном мире практически любая организация имеет собственный ресурс в Интернете, который может предоставлять клиентам различные возможности. Сам ресурс может представлять из себя небольшой лендинг с прайс-листом и контактной информацией, интернет-магазин, портал или форум.

С ростом количества таких ресурсов и увеличением вычислительной мощи компьютеров количество кибератак неуклонно растёт, о чем свидетельствуют некоторые цифры:

- В мире за первый квартал 2023 года совершается на 7% больше кибератак, чем за аналогичный период 2022 года[i].
- В РФ эксперты отмечают рост кибератак на 60% в первом квартале 2023 года в сравнении с 2022[ii].
- «Лаборатория Касперского» зафиксировала увеличение в 2 раза количества атак с применением фишинга за 2022 год по сравнению с 2021[iii].
- По данным «PT-Солар» в 2022 году веб-атаки составляли примерно 11% от всех типов инцидентов, а для инцидентов с высокой долей критичности — 85%[iv].
- Согласно The DFIR report[v] — 7,7% от всех способов получения злоумышленником первоначального доступа к системе составила эксплуатация уязвимостей на публичнодоступных ресурсах.

Помимо атак, связанных с эксплуатацией уязвимостей на самих ресурсах, серьезной проблемой остается наличие уязвимостей в ПО, установленном на узлах, имеющих выход в Интернет:

- Согласно отчёту Google, в более чем половине случаев атак на облачные системы стал использоваться перебор (brute force) учетных данных[vi], также злоумышленники при атаках на облачные системы эксплуатировали уязвимости в программном обеспечении в 36,7% случаев.
- «Positive technologies» в отчёте за 2022 год приводит следующую статистику: «Число успешных атак, направленных на веб-ресурсы организаций, увеличилось на 56%. Если в 2021 году веб-ресурсы компаний становились объектами атак в 17% случаев, то в 2022 году доля таких инцидентов составила 22%»[vii].
- Расследование массовых взломов 1С-Битрикс компании СайберОК показало, что злоумышленники могут годами использовать известные уязвимости для доступа к системам[viii].

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Актуальность

Стоит выделить некоторые причины, по которым атаки на ресурсы, имеющие прямой выход в Интернет, становятся возможными:

1) Неправильная конфигурация сетевого доступа и недостатки конфигурации приложений

Некоторые устройства, реализующие серверные протоколы, не должны иметь выход в Интернет или должны быть доступны только с помощью VPN. Пренебрежение этим принципом может позволить злоумышленникам, при обнаружении такого устройства, нарушить производство, что повлечет за собой как репутационные, так и финансовые потери.

К этой же категории можно отнести общедоступные страницы сайтов, содержащие конфигурационную информацию, панели для администраторов или описание API, доступ к которым должен быть ограничен.

Согласно данным «Paloalto»[ix] в 2022 году четверть проблем, связанных с общедоступными ресурсами, заключалась в открытых RDP-серверах, 17% из которых были с открытыми страницами входа для администраторов.

2) Устаревшее ПО

Обновления для различных компонентов, с помощью которых разработано веб-приложение, зачастую содержат исправления уязвимостей.

Ярким примером может служить случай, произошедший в мае 2023 года: массовый дефейс веб-ресурсов, использующих CMS «1С-Битрикс: Управление сайтом». Массовые взломы были проведены загодя, начиная с 2022 года через известные уязвимости (включая CVE-2022-27228), а целями атакующих являлись все не обновлённые версии «1С-Битрикс: Управление сайтом». Своевременное обновление данного ПО могло бы предотвратить компрометацию большей части ресурсов.

3) Новые уязвимости

Ежемесячно в популярном программном обеспечении экспертами выявляются новые уязвимости, позволяющие злоумышленникам, действующим удалённо, получать доступ к конфиденциальной информации.

В случае объемной инфраструктуры в организации, отслеживать и контролировать вручную все версии ПО, новые уязвимости и конфигурацию сети может быть непросто.

Для того, чтобы упростить эту задачу, могут использоваться сервисы для управления поверхностью атаки (далее — ASM-сервисы[1]). Поверхность атаки, согласно определению Национального Института Стандартов и Технологий США[x], представляет собой совокупность точек

[1] ASM — Attack Surface Management

на границе системы, системных элементов или среды, к которым злоумышленник может попытаться получить доступ, воздействовать на них или извлечь из них данные.

ASM-сервисы предоставляют результаты пользовательских запросов в виде IP-адресов, доменов, связанных с этими адресами, информацию об открытых портах и запущенных сетевых службах. Некоторые ASM-сервисы анализируют версии программного обеспечения, установленного на исследуемом хосте и предоставляют информацию о потенциальных уязвимостях[xi].

Методология, ожидаемые результаты

В статье представлены результаты анализа по заданным критериям для сравнения ASM-сервисов. Определены слабые и сильные моменты, возможности, принципы работы и специфика различных ASM.

В фокус исследования попали системы отобранные по географическому признаку: в выборку вошли представители США, Кореи, Армении и Китая: **SHODAN**, **CENSYS**, **CRIMINAL IP**, **NETLAS**, **HUNTER.HOW**.

Для сравнения применялся ряд критериев:

- периодичность сканирования;
- количество сканируемых портов, поддерживаемых протоколов и проб сетевых сервисов;
- общее количество обнаруживаемых устройств и сетевых сервисов;
- выявление ошибок конфигурации и уязвимостей, с присвоенным идентификатором CVE (Common Vulnerabilities and Exposures);
- качественные характеристики.

Результаты исследования, проведенного экспертами CyberOK, могут помочь определиться с выбором ASM-системы для решения той или иной задачи.

1.1 Сравнение ASM по периодичности сканирования

Актуальность данных является важнейшим фактором при использовании ASM-систем. Своевременное обновление результатов сканирования узлов компаний, имеющих выход в Интернет, помогает быстрее выявить и исправить уязвимости, и, как следствие, снизить вероятность успешных атак на инфраструктуру этой компании. Актуальность данных в ASM-системах, в свою очередь, обеспечивается систематическим сканированием сети.

SHODAN сканирует весь Интернет не реже 1 раза в неделю, но дополнительно можно использовать API этого сервиса для сканирования в любой нужный момент — подробная информация об этом представлена на официальном сайте сервиса[xii].

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Для получения информации о периодичности сканирований сервиса **CRIMINAL IP** были проанализированы узлы, расположенные в разных странах (РФ, США, Германия). Рассматривалась даты обновлений информации для популярных открытых портов (80, 443, 22 и т.д.).

NETLAS обладает возможностями выполнения запросов и получения результатов сканирований в рамках выделенных временных диапазонов. Один временной диапазон соответствует одному периоду сканирования Сети, пример диапазонов можно увидеть на скриншоте сервиса:

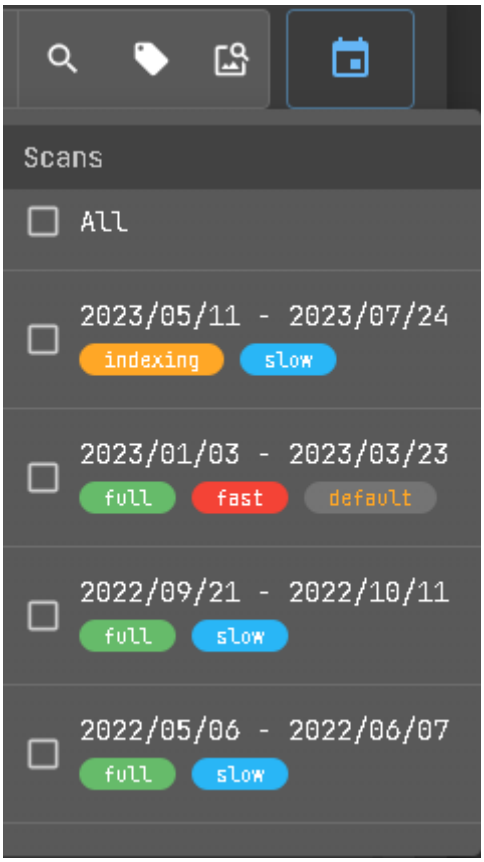


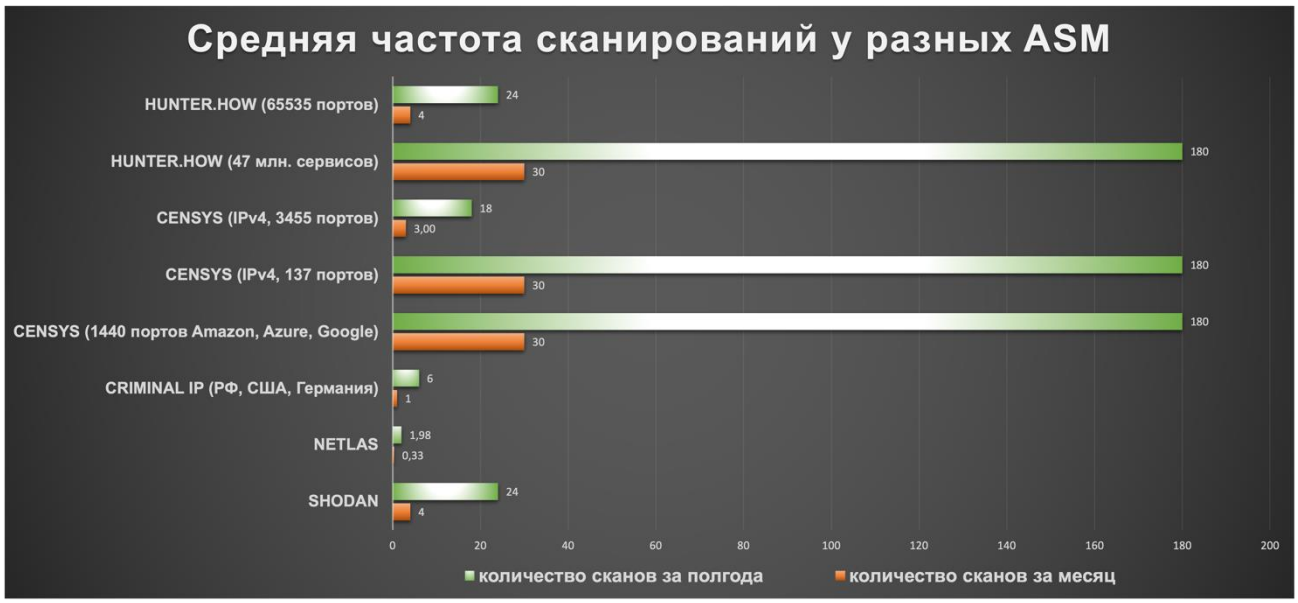
Рисунок 1.

По информации с официального GITHUB-репозитория сервиса[xiii], **HUNTER.HOW** ежедневно сканирует все 65 535 портов пространства IPv4 и с той же периодичностью обновляет данные сканирований свыше 40 млн. сервисов.

CENSYS в своём сервисе сосредоточен на задачах глобального сканирования популярных портов, сканирования облачных провайдеров (таких как Amazon, Google и Azure), глобального сканирования наименее популярных портов (3455 портов на пространстве IPv4) и сканирования всех портов пространства IPv4 с низкой фоновой скоростью. Подробная информация об этом представлена на официальном сайте сервиса[xiv].

На основании полученных результатов можно сделать вывод, что наиболее высокая периодичность сканирования всего Интернета осуществляется ASM-сервисами **SHODAN** и **HUNTER.HOW**. Однако остальные ASM-системы обладают и могут предоставлять особые возможности и более специализированные результаты сканирований.

Таблица 1. Периодичность сканирования



1.2 Сравнение ASM по количеству обнаруживаемых ими устройств и сетевых сервисов

Поскольку при обработке пользовательского запроса ASM-системы не производят сканирование всей сети, а лишь выполняют поиск по сохранённым результатам, важной характеристикой является количество обнаруженных сетевых сервисов и узлов во время регулярного сканирования всего Интернета. Информация о количестве обнаруживаемых сетевых сервисах представлена в Таблице 2. В Таблице 3 представлена информация о количестве обнаруженных в РФ сетевых сервисах. В Таблице 4 представлена информация о количестве обнаруженных в РФ узлах.

Важно заметить, что в контексте этого раздела «сетевой сервис» означает запись в базе данных (БД) с результатами сканирования ASM, которую можно найти поисковым запросом. Некоторые ASM разделяют на разные записи в БД сетевые сервисы, которые доступны по разным URI (иногда даже URL), поэтому полученные значения не полностью однородны.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Таблица 2. Количество обнаруживаемых сетевых сервисов в мире

ASM	Количество обнаруженных сетевых сервисов	Комментарии
shodan	~958,5 млн	Данные получены с помощью запроса «*».
netlas	~905,7 млн (~121 млн узлов)	Данные получены с помощью запроса «*».
criminal ip	~713,9 млн	Были взяты iso коды стран , после чего для каждого кода был выполнен запрос типа «country: {код}» из которого извлекалась информация о количестве результатов.
censys	~749,4 млн сервисов (~353,9 млн узлов)	Данные получены с помощью запроса «*».
hunter.how	~2,2 млрд сервисов (~268,9 млн узлов)	Данные получены с помощью запроса «ip=="1.0.0.0/0"».

Таблица 3. Количество обнаруживаемых сетевых сервисов в РФ

ASM	Количество обнаруженных сетевых сервисов	Комментарии
shodan	11,5 млн	Данные получены с помощью запроса «country:RU».
netlas	18,8 млн	Данные получены с помощью запроса «geo.country:"RU"».
criminal ip	12,8 млн	Данные получены с помощью запроса «country:RU».
censys	~11,8 млн	Поскольку система предоставляет результаты, уникализированные по IP, количество сетевых сервисов было получено следующим образом: суммировалось количество ТОП-20 сервисов для этого же запроса.
hunter.how	~21,6 млн	Данные получены с помощью запроса «ip.country='Ru'».

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Таблица 4. Количество обнаруживаемых устройств в РФ

ASM	Количество обнаруженных сетевых сервисов	Комментарии
netlas	~3,7 млн	Данные получены от разработчиков
censys	5 млн	Данные получены с помощью запроса «location.country=`Russia`»
hunter.how	~6,6 млн	Данные получены с помощью запроса «ip.country='Ru'».

Анализ таблицы показывает, что по количеству обнаруженных сетевых сервисов в мире лидирует Hunter.how, а по количеству узлов — Censys. По количеству обнаруживаемых сетевых сервисов и узлов в РФ лидирует Hunter.how. Такой результат говорит о том, что вероятность найти уязвимые узлы выше при использовании именно этого сервиса.

1.3 Категории протоколов

Поскольку цель ASM-системы заключается не только в обнаружении устройства в сети, но и в определении потенциальных уязвимых мест, важными первичными задачами являются:

- обнаружение открытых портов;
- определение сетевых протоколов;
- определение программного обеспечения (ПО).

Для определения программного обеспечения системы класса ASM отправляют сетевые запросы, которые условно можно разделить на два типа:

- стандартные запросы, соответствующие сетевому протоколу;
- нестандартные запросы, специфичные для определённого ПО.

Из-за того, что под термином «протокол» различные системы подразумевают разные понятия, следует дать определения терминам, которые используются в рамках данной статьи:

- Пробы протоколов — способ определения протоколов прикладного уровня модели OSI (The Open Systems Interconnection model), путём отправки соответствующего стандартного сетевого запроса.
- Пробы сетевого сервиса — совокупность стандартных и нестандартных сетевых запросов.

Так как количество обнаруживаемых открытых портов, проб сетевых сервисов и поддерживаемых протоколов является хорошей сравнительной характеристикой ASM-систем, была получена информация об этих параметрах для рассматриваемых систем. Результаты представлены в Таблице 5.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Таблица 5. Поддерживаемые протоколы и количество сканируемых портов

ASM	Количество сканируемых портов, проб сетевых сервисов и поддерживаемых протоколов	Комментарии
Shodan	1237 портов	Данные о портах получены с помощью модуля Python. shodan.Shodan(api_key).ports().
	194 сетевых сервиса	Данные о сетевых сервисах получены с помощью модуля Python и CLI: - CLI: shodan scan protocols; - Python lib: shodan.Shodan(api_key).protocols().
	44 протокола	Протоколы были получены из сетевых сервисов.
Netlas	>1000 портов	Данные о портах были получены с помощью интерфейса системы, была выполнена группировка результатов запроса «*» по полю «port». Поскольку в группировке Netlas представляет не более 1000 результатов, можно оценивать лишь нижнюю границу количества определяемых системой портов.
	37 сетевых сервисов	Данные о сетевых сервисах были получены с помощью интерфейса системы, была выполнена группировка результатов запроса «*» по полю «protocol».
	29 протоколов	Протоколы были получены из сетевых сервисов.
Criminal ip	3463 портов	Данные о сканируемых портах и поддерживаемых сетевых сервисах были получены с помощью группировки по полям service и port для результатов запроса «country: US», далее были получены результаты группировки по запросу «country: RU», результатом является мощность объединения этих двух множеств.
	51 сетевой сервис	
	29 протоколов	Протоколы были получены из сетевых сервисов.
Censys	3500 портов	Информация о сканируемых портах была получена с официального сайта[xv]
	110 сетевых сервисов	Данные о поддерживаемых сетевых сервисах были получены с помощью API: /api/v2/metadata/hosts.
	37 протоколов	Протоколы были получены из сетевых сервисов.
Hunter.how	65535[2] портов	Информация о сканируемых портах была получена из официального github-репозитория системы.
	не определено	Информация о поддерживаемых сетевых сервисах и протоколов не публикуется на официальных ресурсах системы и не может быть получена с помощью интерфейса.
	не определено	

[2] Данное число не отражает количество обнаруживаемых портов — только сканируемых

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

На основании полученного результата можно сделать вывод о том, что наибольшее количество обнаруживаемых портов представлено ASM-системой Censys, а наибольшее количество проб сетевых сервисов и поддерживаемых протоколов — системой Shodan.

Большее количество поддерживаемых протоколов делает ASM-систему более гибкой, позволяет находить более критичные и менее защищённые устройства. Ярким примером служат ПЛК (Программируемые Логические Контроллеры) в системах АСУ ТП (Автоматизированные Системы Управления Технологическим Процессом): данные устройства предназначены для работы в реальном времени и, в силу того, что приоритетным для них является быстродействие и способность обрабатывать большие объемы данных, при разработке прошивок для них, механизмам защиты уделяется меньше внимание. В то же время, уязвимый ПЛК может иметь выход в Интернет, что позволяет злоумышленнику проэксплуатировать уязвимость и нарушить процесс производства. Другими примерами «ценных находок» для злоумышленника являются контроллеры управления материнскими платами или медицинское оборудование.

1.4 Определение продуктов

Также немаловажной функциональностью систем класса ASM является возможность точного определения различного ПО и стека технологий, который использует это ПО. Для сравнения систем по этому критерию было выполнено следующее:

- выбраны несколько типов ПО;
- выбраны несколько представителей каждого типа ПО (при выборе ориентировались на то, что ПО распространено на территории РФ, список критичных уязвимостей ПО регулярно пополняется и эти уязвимости достаточно часто успешно эксплуатируются злоумышленниками);
- для каждого выбранного ПО были сформированы запросы, позволяющие найти это ПО, используя несколько методов поиска. Текст запросов можно посмотреть в расширенной таблице.

1.4.1 Простой поиск

Самым простым методом поиска для получения информации об исследуемых системах является полнотекстовый поиск по всем данным, которые содержатся в БД с результатами сканирований. Наиболее частая реализация такого метода поиска — это поиск вхождения запрашиваемого текста в сохраненных баннерах ответов сетевых сервисов и в теле HTML-страниц. Такой поиск не отличается особой точностью и подходит только для определения порядка числа сетевых сервисов, использующих искомое ПО и ознакомления со структурой собираемых данных.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

В Таблице 6 представлены продукты, а также количество уникальных записей в БД, которые нашёл каждый из сервисов. Запросы для их поиска в каждом из ASM-сервисов находятся в расширенной таблице.

Примечание:

- В hunter.how нельзя выполнить поиск без указания полей, поэтому поиск выполнялся по полю «web.body».
- В результатах, полученных из Censys и hunter.how, в скобках отражено количество уникальных узлов.

Таблица 6. Количество уникальных сетевых сервисов для простых запросов

	Shodan	**Netlas**	**CriminalIP**	**Censys**	**HunterHow**
Fortinet fortigate	479	1779	1480	3914	796 (421)
Cisco ASA VPN	193	3	901	6	7500 (3700)
Grafana	107	212	1799	14787 (12952)	37800 (13600)
Zabbix	464	4339	3168	7265 (3792)	16800 (4600)
Atlassian Jira	88	80	1295	3600 (1196)	7100 (1500)
Atlassian Confluence	566	18	536	2542 (1014)	4500 (1500)
Redmine	162	3582	4999	4949 (1906)	17000 (2800)
MS Exchange Server	10386	266	17111	5620 (5345)	-
Postfix	72350	119446	43065	59152 (55732)	-
Exim	163903	186475	89992	71963 (72041)	-

1.4.2 Поиск с использованием меток

ASM-сервисы для удобства пользователей могут сами отмечать некоторые сканируемые ресурсы определенными метками/тегами. Алгоритм, по которому сервисы определяют продукты, зачастую неизвестен, однако поиск с использованием таких кодовых слов способен показать более релевантные результаты.

В Таблице 7 представлены продукты, а также количество уникальных записей в БД, которые нашёл каждый из сервисов. Запросы, составленные с использованием соответствующих меток для их поиска в каждом из ASM-сервисов, можно посмотреть в расширенной таблице.

Таблица 7. Количество уникальных сетевых сервисов для запросов с использованием меток продуктов или технологий

	Shodan	Netlas	CriminalIP	Censys	HunterHow
Fortinet fortigate	328	-	48	4872 (3921)	131 (160)
Cisco ASA VPN	2875	9663	5	15690 (5298)	9200 (4600)
Grafana	696	-	-	7094 (3840)	21800 (4800)
Zabbix	2412	4254	-	5531 (2591)	11700 (3200)
Atlassian Jira	767	1647	-	1948 (795)	3300 (678)
Atlassian Confluence	477	1535	-	985 (313)	3800 (857)
Redmine	2047	3481	-	4195 (1482)	11600 (2400)
MS Exchange Server	13152	93050	14753	28170 (10480)	30500 (11000)
Postfix	70049	119411	75700	54616 (53399)	101300 (64000)
Exim	156732	186432	126631	71741 (70890)	163000 (62800)

1.4.3 Углубленный поиск

Наиболее точным методом поиска является поиск по уникальным признакам ПО. Для того, чтобы получить эти признаки, необходимо проанализировать несколько результатов для разных ресурсов. В случае веб-приложений, такими признаками могут быть хэш-код файла «favicon.ico» или специфичное содержимое HTTP-заголовка. Результаты при таком поиске получаются наиболее точными и, зачастую, более полными.

В Таблице 8 представлены продукты, а также количество уникальных записей в БД, которые нашёл каждый из сервисов. Запросы, составленные с использованием некоторых специфичных признаков для их поиска в каждом из ASM-сервисов, можно посмотреть в расширенной таблице.

Таблица 8. Количество уникальных IP для запросов по поиску популярных продуктов

	Shodan	Netlas	CriminalIP	Censys	HunterHow
Fortinet fortigate	1818	2769	597	584 (518)	3100 (1200)
Cisco ASA VPN	6462	7396	5834	6506 (4275)	8400 (2300)
Grafana	2714	3760	1009	6185 (3423)	22500 (4800)
Zabbix	2434	4229	1875	3661(1622)	2700 (1100)
Atlassian Jira	636	2023	1026	867 (2147)	3200 (624)
Atlassian Confluence	397	1482	460	921 (311)	4600 (1000)
Redmine	2075	2958	4726	3752 (1327)	12800 (2000)

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

1.5 Обработка уязвимостей

Помимо определения открытых портов и программного обеспечения на исследуемом узле, существует возможность получать конкретные версии самого программного обеспечения, а также версии операционных систем. Помимо этого, возможен сбор используемых технологий и метаинформации. В свою очередь, совокупность определённых признаков может служить основанием полагать, что исследуемый сервис подвержен уязвимости. Таким образом, умение ASM-системы верно идентифицировать уязвимости является неоспоримым преимуществом этой системы над другими.

1.5.1 Общая информация

В Таблице 9 представлена информация о формате обработки уязвимостей различными ASM-системами.

Таблица 9. Общая информация по обработке уязвимостей

ASM	Работа с уязвимостями
Shodan	Уязвимости отмечаются флагом verified (True/False). Verified: False — проставляется по метаданным, например, в случае, если версия какого-либо ПО является уязвимой, все уязвимости для этой версии присваиваются узлу с меткой unverified. Топ-10 уязвимостей в РФ с таким флагом представлены на Рисунке 2. Shodan может верифицировать уязвимости и отмечать их Verified: True. Топ-10 уязвимостей с таким флагом представлены на Рисунке 3. На официальных ресурсах системы подробностей о процессе верификации не предоставляется.
Netlas	Система отмечает уязвимости согласно версиям программного обеспечения[xvi].
Criminal IP	Отсутствует возможность группировки данных по CVE.
Censys	Сервис не определяет уязвимости.
Hunter.how	Сервис не определяет уязвимости.

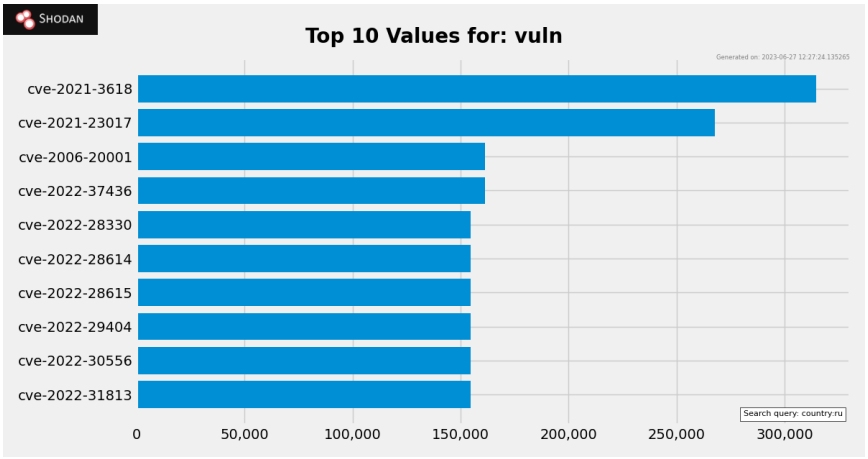


Рисунок 3. Инфографика системы Shodan для поля vuln

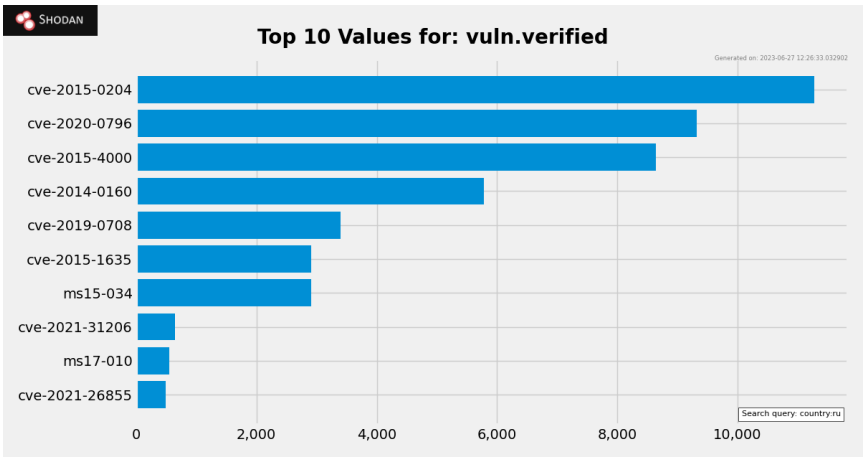


Рисунок 4. Инфографика системы Shodan для поля vuln.verified

-	15933231
CVE-2022-31630	1694637
CVE-2022-31628	1686639
CVE-2022-31629	1686639
CVE-2017-8923	1463464
CVE-2020-11579	1032126
CVE-2019-9637	928186
CVE-2019-9638	928186
CVE-2019-9639	928186
CVE-2019-9641	928186
CVE-2015-9253	911679

Рисунок 5. Инфографика системы Netlas для поля cve.name

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

1.5.2 Насколько «врут» ASM'ы

Очевидно, что при оценке уровня защищённости узла гораздо важнее качество, а не количество. Было проведено исследование, показывающее насколько точным является определение уязвимостей в ASM-системах.

Из всех уязвимостей, отмечаемых системой Shodan как vuln_verified=True, были выбраны критичные, активно эксплуатируемые в последние несколько лет и определяемые на узлах в РФ. В качестве одного из источников таких уязвимостей был выбран ресурс CISA (Cybersecurity & Infrastructure Security Agency) «Known Exploited Vulnerabilities Catalog»[xvii]. Для того, чтобы проверить является ли узел действительно уязвимым, использовались активные сетевые проверки, которые не оказывают вредоносного воздействия, но, при этом, определяют уязвимость с высокой степенью достоверности.

Для каждой такой уязвимости в Shodan были выполнены запросы типа «country:RU vuln:{CVE-....-....} vuln_verified=True». Для результатов, которые вернул сервис, запускалась соответствующая активная проверка. После этого подсчитывалось количество результатов до её запуска и после. Результаты представлены в Таблице 10.

Таблица 10. Точность определения уязвимостей Shodan (поиск по РФ)

Уязвимость	Количество найденных	Количество после активной проверки	Доля уязвимых
CVE-2021-26855	372	108	0,29
CVE-2021-34473	453	400	0,88
CVE-2021-43798	139	133	0,95
CVE-2017-7269	65	62	0,95
CVE-2022-36804	16	1	0,06
CVE-2015-2080	5	0	0
CVE-2021-41277	6	6	1
CVE-2019-1652	2	0	0
CVE-2019-1653	2	1	0,5
CVE-2019-11510	1	1	1

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Для Netlas проводился аналогичный эксперимент.

Таблица 11. Точность определения уязвимостей netlas (поиск по РФ)

Уязвимость	Количество найденных	Количество после активной проверки	Доля уязвимых
CVE-2022-36804	39	1	0,03
CVE-2021-42013	166	3	0,02
CVE-2018-7600	156	0	0
CVE-2019-16759	2	0	0
CVE-2020-17496	2	0	0
CVE-2019-3396	22	0	0

В CriminalIP информация об уязвимостях сетевого сервиса отражается в поле vulnerability. На момент проведения исследования, ни одна уязвимость из списка, подготовленного нами для этого эксперимента, не была обнаружена в поле vulnerability.

Таким образом можно сделать вывод, что качество выявления уязвимостей в современных ASM оставляет желать лучшего. Большое количество ложно-положительных срабатываний не позволяет сфокусироваться на устранении наиболее актуальных проблем.

1.6 Сравнение предоставляемой информации

В данном разделе представлено сравнение рассматриваемых ASM-систем с точки зрения пользователя.

1.6.1 Сравнение по техническим характеристикам

В Таблице 12 представлены данные о том, какую информацию об узле предоставляют системы, какие есть возможности для группировки результатов, а также возможности API.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Таблица 12. Сравнение систем по техническим характеристикам

Параметр сравнения \ ASM		**shodan**	**netlas**	**criminalip**	**censys**	**hunter.how**
При поиске отображает		Сервис	Сервис	Сервис	Хост	Сервис
Обработка хоста	При переходе отображает	Хост	Хост	Хост	Хост	Хост
	Имеются связанные домены (для узла)	Да	Да, + url	Есть, не для всех	Да (вкладка explore)	Да
	Whois	Частично (организация, ISP, ASN (номер))	Да (ASN, сеть, организация, abuse)	Да (ASN, ASN name, организация)	Да (ASN, сеть, abuse, даты изменений)	Да (ASN, ASN name, организация)
	Уязвимости	Да, без привязки (только номер CVE + описание)	Да, с привязкой к продукту и порту	Да, с привязкой к продукту, вендору и порту	Нет	Нет
	Скриншот страницы	Есть, не для всех	Нет	Да	Нет	Нет
	Подсчёт уровня защищенности узла	Нет	Нет	Да	Нет	Нет
	Историческая информация	Да (в CLI: shodan host — history [IP])	Да, можно выполнять поиск по разным сканам	Да	Да (историческая информация есть не для всех узлов), есть возможность сравнения событий	Да (в запросе можно указать временной период за который показывать результаты)
Группировка результатов		Да, с помощью /search/facet можно группировать по различным параметрам	Да	Да, можно сгруппировать только по ASN, стране, порту, продукту, сервису	Да	Частично (есть статистика по топ-10 странам/городам, портам, протоколам, приложениям/ продуктам. При этом запросы не тратятся и можно менять фильтры)
Возможности API	Отдельный API для информации по хосту	Да	Да	Да	Да	Нет
	API для поиска	Да	Да	Да	Да	Да
	Отдельный API для количества результатов	Да	Да	Нет (количество возвращается в ответе при поиске)	Нет (количество возвращается в ответе при поиске)	Нет
	API для группировки	Да	Да	Да	Нет	Нет
	API для запроса скана узла/ сети	Да (на вход — IP/сеть)	Нет	Да (на вход — домен), есть возможность приватного скана	Нет	Нет
	Особенности	-	Отдельные API для сертификатов, whois.	-	Отдельный API для сертификатов	-
Доп. возможности		Есть CLI, модуль для Python.	Есть CLI, модуль для Python и многих языков программирования или фреймворков.	-	Есть модуль для Python и платформы Node.js	-
Теги		c2, cdn, cloud, compromised, cryptocurrency, database, devops, doublepulsar, eol-os, eol-product, honeypot, ics, iot, malware, medical, onion, proxy, self-signed, scanner, starttls, tor, videogame, vpn	Теги представляют собой софт/вендоров	Admin, CDN, ChatBot, Cloud, CMS, Cobalt Strike, Codec, Data Leak, Database, DevOps, DMP, Docker, E-Government, Elastic Beanstalk, Embeded, Firewall, Hardware, Honeypot, IoT, IP Camera, IPSEC VPN, KVM, LMS, LNMP, Malicious, Mining, Monitoring, NAS, NoSQL DB, PBX, Platform, PLC, Printer, Sandbox, SCADA, SCM, Simbox, Splunk, SSL VPN, Steam, Switch, Torrent, Webmap, Wifi	Как таковых тегов нет, но определяются версии софта (и сам софт). Могут проставляться метки (Labels): SSH -> Remote Access	Для каждого результата есть вкладка «App/Product»
Определение версий		Да	Да	Да	Да	Да, достаточно подробное определение версий, при поиске можно отфильтровать нужную версию нужного продукта (только ТОП-10 продуктов). При этом в подробном окне версии отображаться не будут (только продукты).
Присутствует ли raw-ответ		Да, для информации по конкретному хосту	При поиске (в responses) для каждого результата есть raw-ответ	Нет	Да, для информации по конкретному хосту. Представляется как в JSON, так и в формате таблицы	Нет

1.6.2 Сравнение по качеству UI/UX

В Таблице 13 представлено сравнение ASM-сервисов с точки зрения качества UI/UX. Удобство запросов оценивалось субъективно: так, у Shodan построение запроса интуитивно понятно, у CriminalIP — аналогично. У Netlas стоит отметить удобный интерфейс с возможностью поиска необходимого параметра — своего рода «конструктор» запросов. У Hunter.how можно выделить несколько бóльшую функциональность: например, можно сделать запрос на количество открытых портов. Censys также обладает большой функциональностью: поддерживает символы «?» и «*», спец. символы «\n», «\t», возможность поиска по CPE и т.д.

Таблица 13. Сравнение сервисов по качеству UI/UX

Параметр сравнения \ ASM	**Shodan**	**Netlas**	**CriminalIP**	**Censys**	**Hunter.how**
Удобство запросов	4,5/5	4/5	4,5/5	3,5/5	3,5/5
Функциональность запросов	3,5/5	4/5	3,5/5	4,5/5	4,5/5
Наличие подсказок для запросов	Нет	Да	Да	Да	Да
Возможность перейти по IP:Port	Да	Частично (только из responses)	Да	Да	Да
Выгрузка — количество	не более 1 млн	(зависит от подписки: бесплатная — 200, платные — 10к, 1 млн., 10 млн.)	Доступно начиная с medium подписки, формат и количество неизвестны	Результаты запроса скачать нельзя, есть raw ответ (json, таблица) и кнопка для копирования	-
Выгрузка — формат	NDJSON	JSON, CSV	Доступно начиная с medium подписки, формат и количество неизвестны	Результаты запроса скачать нельзя, есть raw-ответ (json, таблица) и кнопка для копирования	-

1.6.3 Сравнение по качеству данных

Случайным образом были выбраны 8 различных узлов для сравнения. На каждом из них открыто несколько портов, запущено несколько сетевых сервисов. Собиралась информация о том, какие порты, продукты и домены определят ASM'ы. Достоверная информация об открытых портах собиралась с помощью утилиты nmap. Корректность определения доменов проводилась с помощью отправки прямых DNS-запросов (в качестве результата возвращается IP-адрес, связанный с соответствующим доменным именем). Если сетевой порт, сервис, технология или домен были ошибочно определены ASM, то в таблице 14 эти значения выделяются красным цветом.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Таблица 14. Узлы для сравнения (данные брались со вкладок с информацией по хосту)

	Узел \ ASM	Shodan	Netlas	CriminalIP	Censys	Hunter.how
1	Порты: nmap: 11: 22 80 443 3000 8080 8088 8777 9090 9100 9411 27017	7: 22 80 443 3000 8080 8088 9100	7: 22 80 443 3000 8080 8088 27017	7: 22 80 443 8080 8088 9090 9100	10: 22 80 443 3000 8080 8088 8777 9090 9100 27017	11: 22 80 443 3000 8080 8088 8777 9090 9411 9100 27017 (результаты за последний год)
	Продукты/метки	OpenSSH 8.9p1 Ubuntu-3ubuntu0.1 Nginx Grafana (Open Source) 9.3.2 Prometheus Node Exporter 1.5.0	Ubuntu openssh (8.9p1) nginx	OpenSSH 8.9p1 Grafana+nginx Bear UI Httpd Node Exporter+httpd Prometheus Node Exporter1.5.0+httpd	OpenDSD OpenSSH 8.9p1 Ubuntu Nginx Grafana Prometheus Node Exporter Mongodb 6.0.3	OpenSSH Nginx Blazor Microsoft ASP.NET Grafana Dashboard
	Домены	●●	●●●	-	●	●●● ●
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-
2	Порты: nmap: 8: 22 80 443 5223 8070 8893 8894 10050	3: 22 80 443	3: 22 80 443	3: 22 80 443 Ист. инф. (8070 10050)	7: 22 80 443 5223 8070 8893 8894	7: 22 80 443 5223 8070 8893 8894 (результаты за последний год)
	Продукты/метки	OpenSSH 7.4 Nginx 1C-BITRIX PHP	Openssh (7.4) Nginx 1c_bitrix php	OpenSSH 7.4 Nginx 1C-Bitrix PHP	OpenBSD OpenSSH 7.4 Nginx PHP linux	OpenSSH jQuery Nginx
	Домены	●●●	●●●●●●	●●	●●	●●●●● ●
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-
3	Порты: nmap: 3: 80 502 9443	3: 80 502 9443	1: 80	- ист. инф (80)	3: 80 502 9443	3: 80 502 9443
	Продукты/метки	jQuery	sierra_wireless	httpd	Scada	jQuery Sierra ACEmanager Router
	Домены	●	●	●	●●	●
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-
4	Порты: nmap: 5: 22 23 123 161 1723	4: 22 23 123 161	4: 22 23 123 161	3: 22 23 1723	4: 22 23 123 1723	6: 22 23 123 161 1701 1723
	Продукты/метки	Cisco SSH 1.25 ciscoSystems	Cisco cisco_ssh (1.25)	Cisco sshd Cisco Systems Inc.	Cisco SSH 1.25 Cisco IOS	NTP Cisco SSH Cisco IOS telnetd Cisco SNMP service
	Домены	●	●	●	-	-
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-
5	Порты: nmap: 9: 22 80 161 443 623 1900 2198 2199 8208	5: 80 161 443 623 1900	2: 22 161	4: 22 80 443 1900	6: 22 80 443 2198 2199 8208	5: 80 161 443 2199 8208
	Продукты/метки	net-snmp	openssh	OpenSSH	-	net-snmp
	Домены	-	-	●	-	-
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-
6	Порты: nmap: 4: 22 80 123 443	3: 22 80 443	3: 22 123 443	3: 22 80 443	4: 22 80 123 443	5: 22 80 123 443 50000
	Продукты/метки	OpenSSH 7.9 Nginx 1.20.1 1C-Bitrix Fancybox Jquery Jquery UI Modernizr OWL Carousel PHP	openSSH 7.9 font_awesome nginx 1.20.1 php 7.4.26 phpbb	OpenSSH 9.1 nginx 1.20.1	FreeBSD OpenBSD OpenSSH 9.1 nginx 1.20.1 PHP 7.4.26	Nginx jQuery PHP Font Awesome NTP
	Домены	●●	●●●●●●●●●●●●●●	●●	●	●●●●●●●●●●●●●
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-
7	Порты: nmap: 4: 21 80 443 8080	2: 80 443	4: 21 80 443 8080	- ист. инф. (21 80 443 8080)	4: 21 80 443 8080	4: 21 80 443 8080
	Продукты/метки	nginx	nginx	Nginx Pure-FTPd	PureFTPd Pure-FTPd nginx	Nginx Pure-FTPd
	Домены	●	●●●●●●●●●● ●●●●●●●●●●●	● ●	●	●● ●●●●●●●●●●●●●●●
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-
8	Порты: nmap: 14: 21 25 53 80 110 123 143 443 465 587 993 995 3306 7819	12: 21 25 53 80 110 143 443 465 587 993 995 3306	12: 21 25 53 80 110 123 143 443 465 993 995 3306	7: 21 25 53 80 110 443 587	12: 21 25 53 80 110 123 143 443 465 587 993 3306	14: 21 25 53 80 110 123 143 443 465 587 993 995 3306 7819
	Продукты/метки	ProFTPD 1.3.4a Exim smtpd 4.80 Apache httpd 2.2.22 MySQL 5.6.40-84.0	Debian Exim 4.80 Apache 2.2.22 Dovecot	ProFTPD 1.3.4a Exim smtpd 4.80 Apache 2.2.22 pop3d ssl	ProFTPD Project ProFTPD 1.3.4a exim 4.80 Debian linux ISC BIND 9.8.4-rpz2+rl005.12-P1 Apache HTTPD 2.2.22 Dovecot Oracle MySQL 5.6.40-84.0	NTP OpenSSH Apache Debian jQuery PHP ProFTPD Exim smtpd ISC BIND Dovecot pop3d Dovecot imapd MySQL
	Домены	●●	●●●●●●●●●●●	●●	●	●●●●●●●●●●●●●
	JARM/JA3S/JA3	-	-	-	JARM, JA3S	-

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Методика оценивания точности определения открытых портов: для каждого узла находится доля открытых портов по сравнению с результатами сканирования средствами nmap. После этого вычисляется сумма долей и нормируется по 5-бальной шкале. Данная методика применяется поскольку доподлинно известно какие открытые порты находятся на узле.

Методика оценивания точности доменов, связанных с узлом: каждому ASM-у присваивается 16 баллов (по 2 за каждый узел); за каждый узел, для которого система нашла хотя бы один неверный домен с верным доменом второго уровня вычитается 0,5 балла; за каждый узел с хотя бы одним неверно определённым доменом второго уровня вычитается 1 балл; за каждый узел с количеством неверно определённых доменов более половины от общего числа определённых доменов у ASM-а вычитается 2 балла; для каждого узла, для которого система не определила ни одного домена, из оценки вычитается 2 балла. Итоговый балл нормируется по 5-бальной шкале. Данная методика применяется поскольку достоверно не известно точное число доменов, связанных с рассматриваемым ip-адресом, а большое количество (более половины) неверных результатов может мешать пользователю сервиса.

Пример 1. Система определила узлу домены test.abc.ru, test2.abc.ru, test3.abc.ru, при этом только первый не соответствовал ответу на прямой DNS-запрос. Тогда, поскольку остальные домены проверку прошли и abc.ru — верный домен второго уровня, для этого узла вычитается 0,5 балла.

Пример 2. Система определила узлу домены test.def.ru, test2.abc.ru, test3.abc.ru, при этом только первый не соответствовал ответу на прямой DNS-запрос. Тогда, поскольку остальные домены проверку прошли, и abc.ru — верный домен второго уровня, для этого узла вычитается 1 балл.

В Таблице 15 представлены результаты оценки качества данных для рассматриваемых сервисов.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Таблица 15. Сравнение сервисов по качеству данных

Параметр сравнения \ ASM	**Shodan**	**Netlas**	**CriminalIP**	**Censys**	**Hunter.how**
Полнота информации по протоколам	Баннер, сертификат	В responses полный ответ	Баннер, ответ, сертификат	Баннер, ответ, сертификат	Баннер, ответ, сертификат
Точность определения открытых портов	3,4/5	3,1/5	2,1/5 (2,9/5)	4,4/5	4,6/5
Точность смапленных доменов	3,1/5	3,1/5	2,5/5	2,9/5	2,7/5
Качество маппинга продуктов (субъективно)	3,5-4/5	3/5 меньше других, не всегда отдаёт версии	3,5/5	3,5-4/5	3,5/5
JARM/JA3S/JA3	Есть JARM, JA3S во вкладке отчёта (search -> view report), в информации по хосту — нет	JARM есть в raw-ответе	JARM есть, но не для всех	JARM, JA3S	Есть поиск по JARM, но нет собранных отпечатков

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Заключение

Подводя итоги, можно сказать, что ни один из рассмотренных сервисов не превосходит остальных по всем категориям. Однако выбор ASM-а стоит основывать исходя из поставленной задачи. Одни лучше справляются с определением открытых портов и используемых на исследуемом узле продуктах. У других — более удобный API или интерфейс в веб-приложении. Кроме того, некоторые рассмотренные сервисы предлагают больше возможностей, но в рамках данной статьи проводилось сравнение одинаковой по смыслу функциональности.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Список использованных источников

[i] https://www.infosecurity-magazine.com/news/global-cyber-attacks-rise-7-q1-2023/#:~:text=Weekly%20cyber%2Dattacks%20have%20increased,of%201248%20attacks%20per%20week

[ii] https://www.kommersant.ru/doc/5999865

[iii] https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022

[iv] https://rt-solar.ru/analytics/reports/2880/

[v] https://thedfirreport.com/2023/03/06/2022-year-in-review/

[vi] https://services.google.com/fh/files/blogs/gcat_threathorizons_full_july2022.pdf

[vii] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id2

[viii] https://www.cyberok.ru/docs/CyberOK-bitrix_web_14.pdf

[ix] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/cortex_xpanse-attack-surface-threat-report

[x] https://csrc.nist.gov/glossary/term/attack_surface

[xi] https://censys.com/cve-2022-2185-gitlab-server/

[xii] https://help.shodan.io/the-basics/on-demand-scanning#:~:text=at%20le-ast%20once%20a%20week

[xiii] https://github.com/Hunter-How/Support

[xiv] https://support.censys.io/hc/en-us/articles/360059603231-Censys-Internet-Scanning-Intro

[xv] https://support.censys.io/hc/en-us/articles/360059603231-Censys-Internet-Scanning-Intro

[xvi] https://netlas.io/#:~:text=based%20on%20product-,versions,-according%20to%20the

[xvii] https://netlas.io/#:~:text=based%20on%20product-,versions,-according%20to%20the