kaspersky

Реагирование на компьютерные инциденты

Аналитический отчет

2018

www.kaspersky.ru

kaspersky

Если вы хотите обратиться за услугами цифровой криминалистики, реагирования на инцидент или анализа вредоносного ПО, свяжитесь с нами по адресу gert@kaspersky.com.

Общая информация

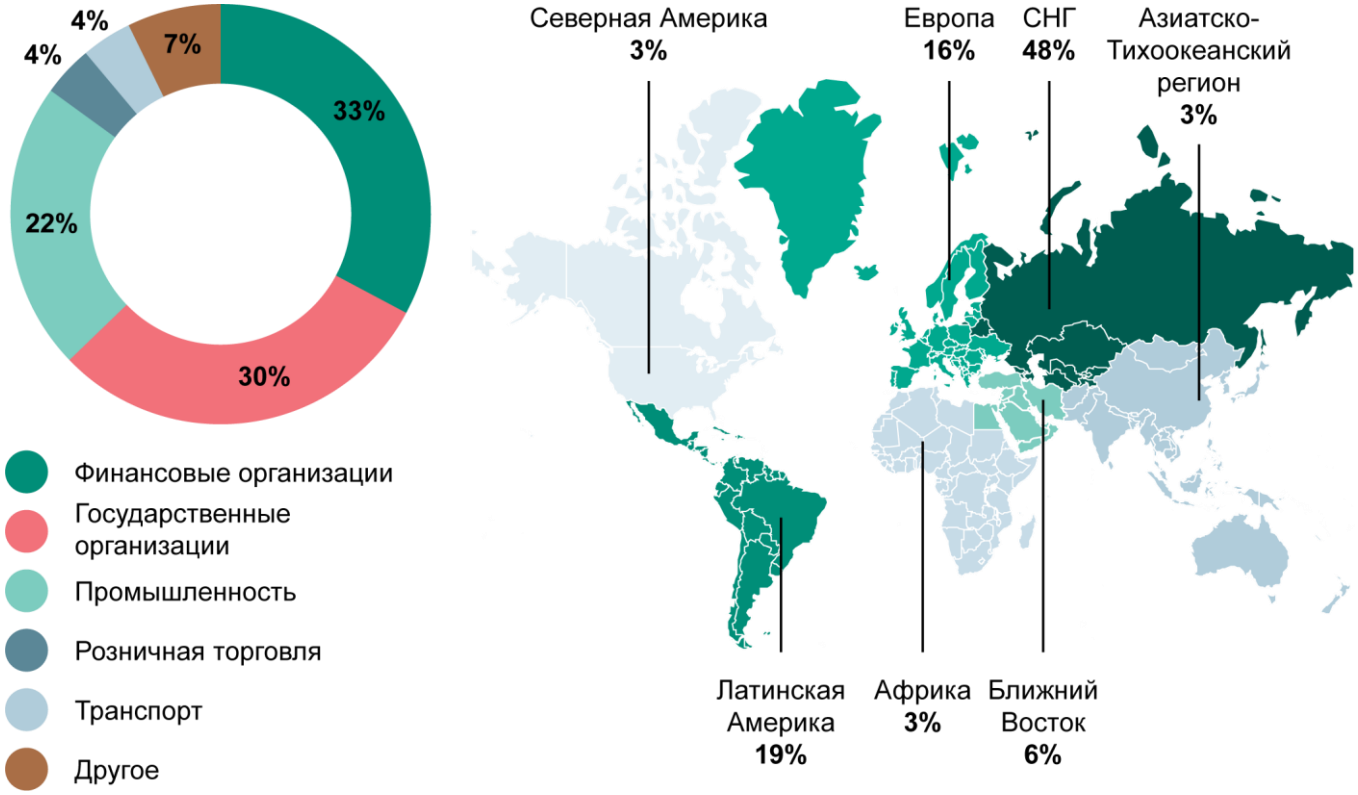
В данном отчете описаны результаты работ по реагированию на инциденты, проведенных нашей командой за год. Мы тщательно проанализировали все запросы на услуги, общение с клиентами и результаты расследований, чтобы подготовить для вас этот обзор “в цифрах”. Данный отчет содержит информацию о том, как компании обнаруживают факты компрометации своих систем, какие векторы атак обычно используют киберпреступники, как долго злоумышленники находятся в сети организации и многое другое. Также мы подготовили ряд рекомендаций, позволяющих повысить уровень безопасности и уменьшить возможный ущерб от компрометации.

Источником данных для анализа выступал широкий спектр сервисов по расследованию инцидентов, предоставляемых «Лабораторией Касперского». Основным подразделением, занимающимся цифровой криминалистикой и реагированием на инциденты является команда Global Emergency Response Team (GERT[1]), в которую входят эксперты из Европы, Латинской Америки, Северной Америки, России и Ближнего Востока. Однако, сфера деятельности компании гораздо шире, и включает ряд других сервисов, связанных с реагированием на инциденты и исследованием вредоносного ПО. В частности, обратите внимание на расследования целевых атак от команды Global Research and Analysis Team (GReAT[2]).

В данном отчете рассматриваются следующие вопросы:

- В каких случаях наши клиенты обращаются за расследованием?
- Как часто организации сталкиваются с инцидентами и что это за инциденты?
- Какие векторы атаки были наиболее распространены?
- Как долго злоумышленники находились внутри сети?
- Какие тактики и техники использовали атакующие?

География и отрасли наших работ в 2018 году



[1] https://www.kaspersky.ru/enterprise-security/incident-response
[2] https://great.kaspersky.com/

kaspersky

Причины для обращения за расследованием

Причины обращений за реагированием на инцидент

Более половины случаев обращений за расследованием связаны с обнаружением очевидных последствий атаки (несанкционированный перевод денежных средств, зашифрованные рабочие станции, недоступность сервисов и т.д.). Данный показатель говорит о необходимости совершенствования методов обнаружения атак и оптимизации процессов реагирования на инциденты, что позволило бы избежать денежных потерь и минимизировать ущерб от атак на инфраструктуру компании.

Отдельно следует отметить, что в **двух случаях из трех** расследования инцидентов, связанных с **обнаружением подозрительных файлов или сетевой активности**, действительно приводили к обнаружению **атаки на инфраструктуру заказчика**. В остальных случаях причиной подозрительной активности выступали нехарактерные действия пользователей или поведение программного обеспечения, связанное с ошибками конфигурации.

Наиболее частой причиной обращения стала атака шифровальщиков. Данная категория атак характеризуется высокой скоростью развития, сложно детектируется на ранних стадиях, а ее последствия, напротив, очевидны.

Топ 7 шифровальщиков по доле заражений

Название	Доля заражений
WannaCry	40.64%
Cryakl	7.37%
GandCrab	5.15%
(generic verdict)	3.63%
Purgen/ GlobeImposter	2.74%
Crysis/Dharma	2.67%
Shade	2.41%

Специалистами отдела антивирусных исследований Лаборатории Касперского был составлен рейтинг наиболее распространенных образцов шифровальщиков, атакующих организации, за 2018 год[3].

В случае обнаружения активности шифровальщика необходимо:

- Изолировать компьютер и сегмент сети, в котором произошел инцидент, для исключения дальнейшего развития атаки.
- Сделать снимки оперативной памяти и снять образы жестких дисков для дальнейшего детального расследования.
- Проанализировать зашифрованные файлы с целью выявления типа вредоносной программы, что позволит оперативно принять комплекс мер по первоначальному реагированию.
- Провести расследование инцидента для установления начальных векторов компрометации, а также выявления возможных точек закрепления злоумышленников в инфраструктуре, что позволит избежать повторного заражения.

[3] https://securelist.ru/kaspersky-security-bulletin-2018-statistics/92906/

kaspersky

В реальности инцидентов намного больше

Только 22% компаний, у которых были обнаружены признаки вредоносной активности, обратились за услугой по реагированию на инцидент.

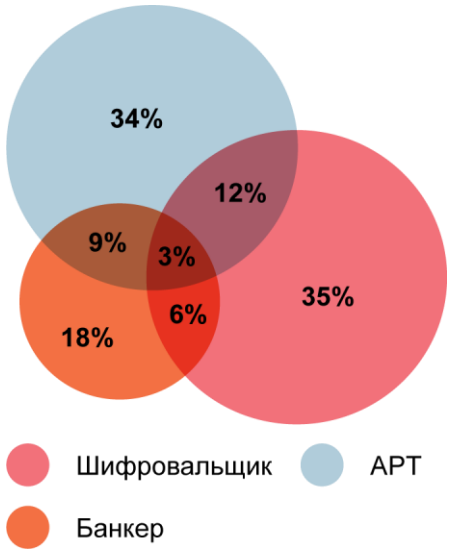
Часто клиенты Лаборатории Касперского обращаются за экспертным анализом данных, собранных с использованием автоматических средств мониторинга. В результате исследования предоставленных данных были получены следующие результаты:

81% организаций, предоставивших данные для анализа, имели признаки вредоносной активности во внутренней сети.

У каждой третьей компании обнаружена активность, свидетельствующая о возможной таргетированной атаке[4].

Для трех ключевых категорий организаций были выявлены основные тенденции, связанные с угрозами безопасности:

Доля клиентов, у которых обнаружена вредоносная активность



Финансовые организации

В финансовых организациях **в полтора раза чаще (54%),** чем среди всех организаций, была обнаружена активность, являющаяся признаком **таргетированной атаки.**

У малой доли финансовых организаций обнаружены признаки **заражения шифровальщиком (12%)** или **банкером (8%)**.

Государственные организации

У **95%** государственных организаций обнаружены признаки **вредоносной активности**, что **на 14% больше,** чем среди всех организаций в общем.

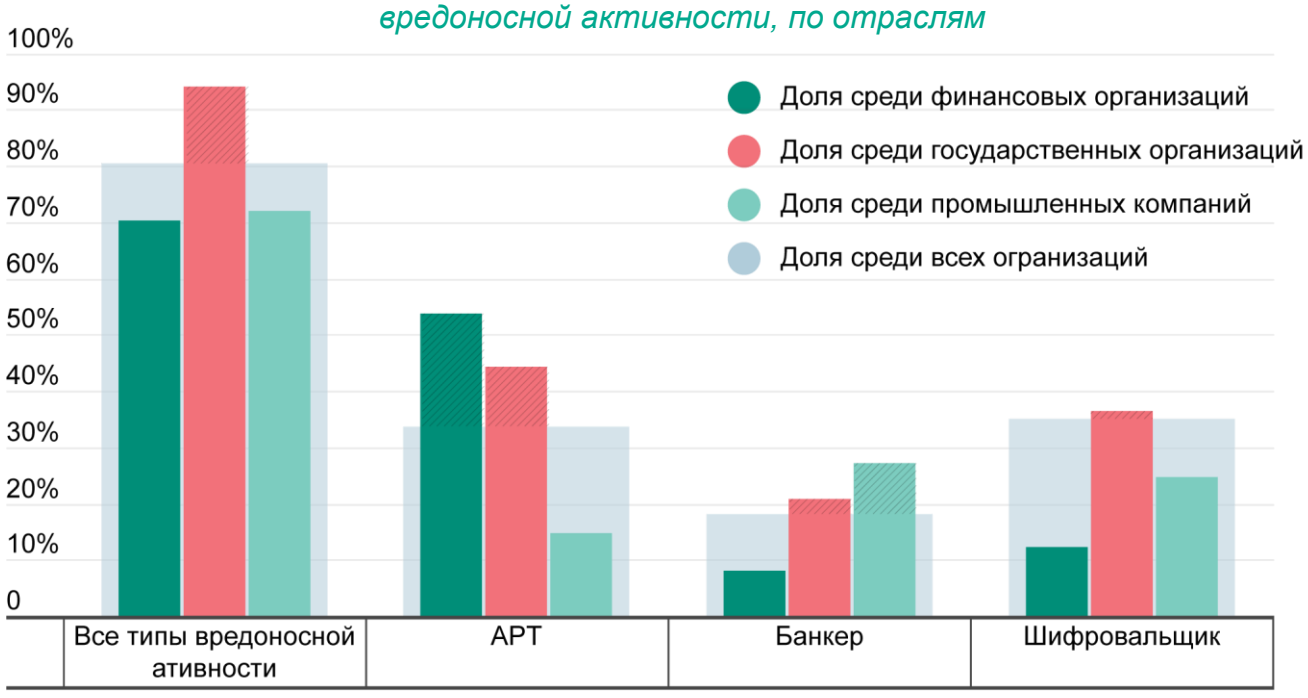
У **45%** государственных организаций зафиксированы обращения к ресурсам, связанным с **таргетированными атаками**.

Промышленные компании

Промышленные компании **чаще становятся жертвами банкеров**. Активность, соответствующая данному ВПО, обнаружена у **27%** компаний.

Промышленные компании в **меньшей** степени подвержены **таргетированным атакам (15%)** или **атакам шифровальщиков (25%)**.

Доли организаций, у которых обнаружены признаки определенной вредоносной активности, по отраслям

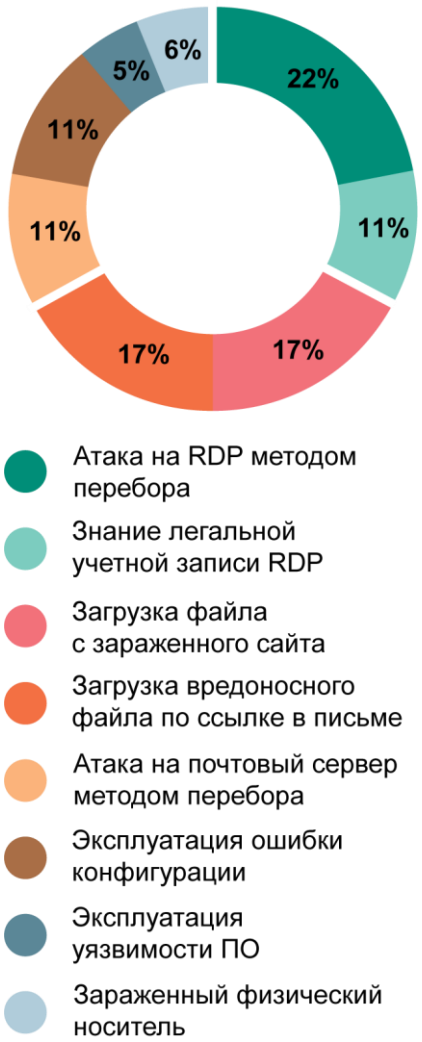


[4] Таргетированная атака или Advanced Persistent Threat (APT) - кибератака, направленная на конкретную организацию, и полностью или частично контролируемая злоумышленником в режиме реального времени.

kaspersky

Векторы первичной компрометации

Распространённые векторы атак[5]



В трети инцидентов для начальной компрометации системы использовалась служба удаленного управления RDP. В большинстве случаев злоумышленникам удавалось подобрать учетные данные пользователя, причем на перебор данных у атакующих уходило порядка нескольких часов. Настолько высокая скорость объясняется использованием сотрудниками ненадежных или словарных паролей. Кроме того, в большинстве случаев для аутентификации в различных системах использовались одинаковые учетные данные, в результате чего злоумышленники смогли повторно использовать полученные имена пользователей и пароли для доступа к другим узлам.

Следует также отметить, что в **трети случаев** атак через службу удаленного управления учетные данные были известны атакующим заранее (попыток подбора пароля обнаружено не было). Вероятно, эти данные были получены с использованием методов социальной инженерии или обнаружены в открытом доступе (например, если сотрудник использовал такой же пароль для регистрации на сторонних ресурсах).

Рекомендуется:

- Ограничить доступ к службам удаленного управления со всех внешних IP адресов. Удаленный доступ к корпоративным ресурсам и рабочим станциям должен быть организован с помощью VPN.
- Придерживаться строгой парольной политики.
- Придерживаться политики минимальных привилегий.
- Придерживаться политики минимальных привилегий.

33% атак произошли вследствие небезопасных действий со стороны работников компании. Сотрудник загружал из недоверенных источников вредоносный файл и запускал его, в результате чего злоумышленники получали контроль над рабочей станцией. Следует отметить, что невозможно полностью исключить влияние человеческого фактора, однако регулярное обучение персонала основам компьютерной безопасности позволяет значительно уменьшить вероятность успешной атаки с использованием методов социальной инженерии.

Рекомендуется:

- Использовать антивирусное решение на всех узлах сети и обеспечить регулярность его обновления.
- Использовать «песочницу» для проверки загружаемых из внешней сети файлов.
- Проводить регулярные тренинги для сотрудников, посвященные информационной безопасности.

Также, для повышения общего уровня безопасности рекомендуется:

- Обеспечить централизованное обновление программного обеспечения, в том числе на компьютерах, не являющихся частью доменной инфраструктуры.
- Внедрить процессы мониторинга подозрительной сетевой активности.
- Автоматически осуществлять резервное копирование данных на носитель, недоступный для записи (кроме процесса копирования).
- Регулярно проводить тестирование на проникновение.

[5] В 20% случаев данные, необходимые для установления изначального вектора атаки, не были предоставлены.

kaspersky

Продолжительность атак

Для ряда инцидентов специалистам «Лаборатории Касперского» удалось установить промежуток времени, между началом активных действий со стороны атакующих и завершением атаки. В результате последующего анализа, все инциденты были разделены на три категории по длительности.

Быстрые атаки (Несколько часов)

К данной категории отнесены атаки длительностью менее суток. В основном, это инциденты, связанные с заражением шифровальщиками. Ввиду большой скорости развития, эффективное противодействие данным атакам возможно только превентивными методами.

В некоторых случаях была замечена задержка между первичной компрометацией и началом активных действий со стороны атакующего, вплоть до недели.

Основной класс угроз:

Заражение шифровальщиком

Основной вектор атаки:

Атака на RDP методом перебора

Длительность атаки (медиана):

6 часов

Методы противодействия:

- Строгая парольная политика.
- Двухфакторная аутентификация.
- Ограниченный доступ к службам удаленного управления.
- Применение антивирусных средств защиты на всех узлах корпоративной сети.

Атаки средней длительности (Несколько дней)

В данную группу выделены атаки, развивающиеся несколько дней. В подавляющем большинстве случаев данная активность была направлена на непосредственное хищение денежных средств. Как правило, злоумышленники добивались поставленной цели в течении недели.

Основной класс угроз:

Хищение денежных средств

Основные векторы атаки:

- Загрузка вредоносного файла по ссылке из письма
- Загрузка файла с зараженного сайта

Длительность атаки (медиана):

8 суток

Методы противодействия:

- Обучение персонала основам кибербезопасности.
- Применение антивирусных средств защиты на всех узлах корпоративной сети.

Длительные атаки (от трех недель)

В это группу были включены инциденты, продолжавшиеся более нескольких недель. Данная активность почти всегда направлена на похищение конфиденциальных данных.

Для таких атак характерно чередование активных и пассивных фаз. Интересно, что суммарная продолжительность активных фаз в среднем близка к длительности атак из предыдущей группы.

Основной класс угроз:

Кибершпионаж и кража конфиденциальных данных

Основной вектор атаки:

Загрузка вредоносного файла по ссылке из письма

Длительность атаки (медиана):

3 месяца

Суммарная длительность активных фаз (медиана):

7 суток

Методы противодействия:

- Полноценное и своевременное расследование всех инцидентов информационной безопасности.
- Использование решений для защиты инфраструктуры на сетевом уровне и на уровне рабочих станций.
- Применение средств мониторинга сетевой активности.
- Сегментирование внутренней сети.

kaspersky

Распространенные тактики и техники

Для ряда инцидентов был составлен список используемых техник атак по методологии MITRE[6]. Ниже приведена таблица ATT&CK с указанием частоты, с которой техники встречались в инцидентах. К сожалению, на сегодняшний день лишь немногие компании пользуются преимуществами, которые дает применение методологии ATT&CK или структурированных описаний угроз, таких как STIX. Если вы работаете с таким типом информации, обратите внимание на то, покрываются ли приведенные ниже техники выбранными вами средствами защиты.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Spearphishing Attachment	CMSTP	Component Object Model Hijacking	DLL Search Order Hijacking	CMSTP	Brute Force	Account Discovery	Pass the Hash	Data from Local System	Data Compressed	Commonly Used Port
Spearphishing Link	Command-Line Interface	Create Account	Hooking	Component Object Model Hijacking	Credential Dumping	File and Directory Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Encrypted	Connection Proxy
Valid Accounts	Execution through API	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Credentials in Files	Network Service Scanning	Remote File Copy	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Encoding
	Graphical User Interface	Hidden Files and Directories	Process Injection	Disabling Security Tools	Exploitation for Credential Access	Network Share Discovery	Remote Services	Input Capture		Remote Access Tools
	LSASS Driver	Hooking	Scheduled Task	DLL Search Order Hijacking	Hooking	Network Sniffing	Windows Admin Shares	Screen Capture		Remote File Copy
	PowerShell	LSASS Driver	Valid Accounts	File Deletion	Input Capture	Peripheral Device Discovery				Standard Application Layer Protocol
	Regsvr32	New Service	Web Shell	Hidden Files and Directories	Network Sniffing	Permission Groups Discovery				
	Rundll32	Registry Run Keys / Startup Folder		Masquerading		Process Discovery				
	Scheduled Task	Scheduled Task		Modify Registry		Query Registry				
	Scripting	Shortcut Modification		Obfuscated Files or Information		Remote System Discovery				
	Service Execution	Valid Accounts		Process Injection		Security Software Discovery				
	Signed Binary Proxy Execution	Web Shell		Regsvr32		System Information Discovery				
	User Execution			Rundll32		System Network Configuration Discovery				
	Windows Management Instrumentation			Scripting		System Network Connections Discovery				
				Signed Binary Proxy Execution		System Owner/User Discovery				
				Software Packing		System Service Discovery				
				Valid Accounts						

> 10% случаев
> 20% случаев
> 50% случаев

[6] https:/attack.mitre.org/

kaspersky

Заключение

Полученные данные позволяют сделать вывод, что кибератакам подвержены все компании, вне зависимости от отрасли или региона. Разработка процедур защиты и реагирования на такого рода атаки больше не является необходимой лишь для ограниченного числа организаций, а обязательна для всех компаний, независимо от вида их деятельности.

Поддержка и совершенствование существующих процессов реагирования на инциденты позволяет оперативно устранять угрозы за счет точной локализации, анализа и изоляции зараженных элементов сети. Также, благодаря использованию опыта, полученного в результате расследования каждого инцидента, значительно снижается риск повторного заражения и совершенствуется защита от целевых кибератак.

Наряду со строгими политиками мониторинга и хранением журналов событий на протяжении, по меньшей мере, полугода, разработка процедур для надлежащей работы с цифровыми доказательствами, несомненно, повышает скорость расследования инцидентов и обеспечивает полноту его результатов. Это, в свою очередь, приводит к более быстрой локализации инцидента и, как следствие, снижает возможные финансовые потери, урон репутации компании и объем полученных злоумышленниками данных.

Регулярное проведение работ по анализу защищенности доказало свою эффективность в раннем выявлении слабых мест в инфраструктуре. Это позволяет устранить их до того, как злоумышленники обнаружат выявленные уязвимости и воспользуются ими в ходе реальной атаки.

Кроме того, как видно из статистики, люди все еще являются самым слабым звеном в безопасности. Даже при использовании строгих политик безопасности и внедрении надежных защитных решений, всего лишь один обманутый злоумышленниками сотрудник может стать причиной компрометации значительной части инфраструктуры. Потому так важно уделять особое внимание повышению осведомленности персонала в области информационной безопасности.