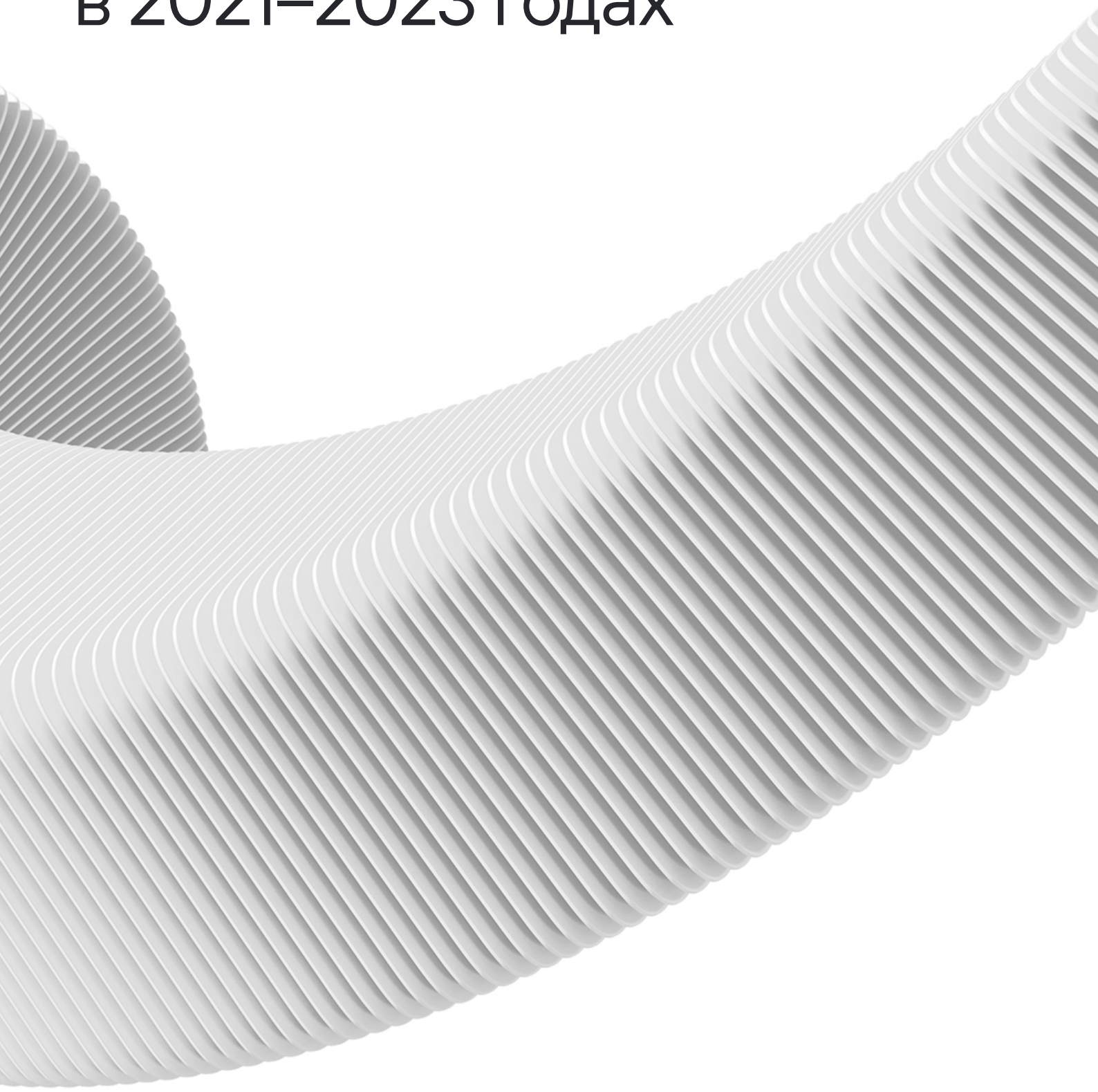
Итоги расследований инцидентов ИБ в 2021–2023 годах



Positive Technologies

ptsecurity.com

Содержание

Краткие итоги ... 4

Основная часть исследования ... 6

Отличие ретроспективного анализа инфраструктуры от проектов по реагированию на инциденты ИБ ... 6

Как действуют злоумышленники ... 9

Последствия атак ... 15

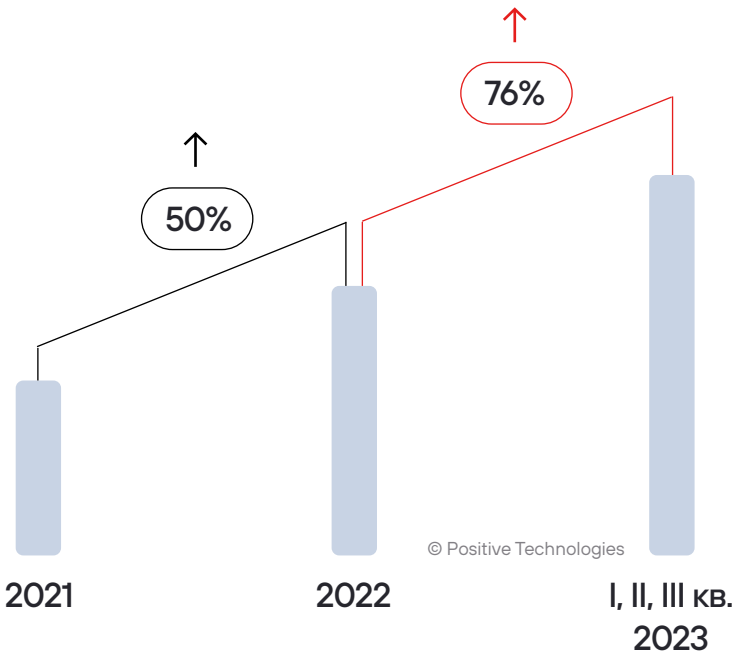
Примеры выявленных атак ... 18

Заключение ... 21

[1] Расследование инцидента — это процесс исследования и анализа событий, направленный на оперативное определение источника угрозы, локализации следов присутствия злоумышленника в скомпрометированной инфраструктуре, помощь в восстановлении нарушенных бизнес-процессов.

В последние два года количество проектов по расследованию инцидентов[1] информационной безопасности, выполняемых ежегодно командой Incident Response (IR) экспертного центра безопасности Positive Technologies (PT Expert Security Center), постоянно увеличивалось. Только в 2022 году прирост составил 50%. За первые девять месяцев 2023 года, в сравнении с показателями за весь 2022 год, количество таких проектов выросло на 76%. Мы предполагаем, что такой скачок может быть спровоцирован увеличением количества инцидентов ИБ вследствие последних геополитических и экономических событий в мире.

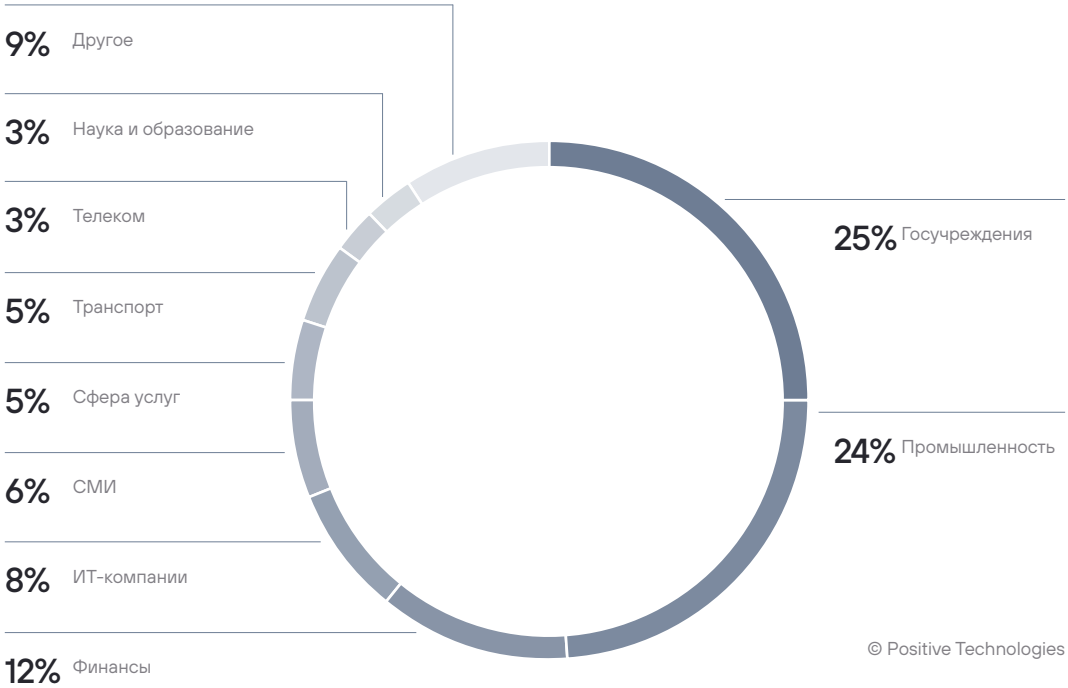
Рисунок 1. Количество проектов по расследованию инцидентов в 2021-м, 2022-м и за I–III квартал 2023 года



[2] Ретроспективный анализ инфраструктуры компании — это детальное исследование доступных наборов данных (образов систем, журналов событий ОС, дампов памяти, сетевого трафика, образцов вредоносного ПО, журналов СЗИ и т. д.) за заданный (в большинстве случаев — максимально доступный, исходя, в частности, из глубины хранения журналов и имеющихся forensic-артефактов) промежуток времени с целью выявить следы возможной компрометации.

В рамках данного исследования мы проанализировали информацию, полученную по результатам более чем 100 проектов по расследованию инцидентов, а также ретроспективному анализу инфраструктуры[2], которые проводились с I квартала 2021 года по III квартал 2023 года в различных компаниях на территории РФ и СНГ. Большинство этих организаций (69%) — госучреждения, а также промышленные, финансовые и ИТ-компании. Значительная часть расследованных нами атак носили целенаправленный характер, то есть злоумышленники ставили своей целью нанести ущерб именно конкретной компании.

Рисунок 2. Распределение организаций-жертв по отраслям



20% организаций входят в рейтинг крупнейших компаний России по объему реализации продукции RAEX-600 за 2022 год и 21% — в рейтинг «Эксперт-400» за 2021 год.

Краткие итоги

В результате анализа проектов по расследованию инцидентов и работ по ретроспективному анализу инфраструктур компаний было установлено, что:

- 40% инцидентов связаны с деятельностью известных однозначно идентифицированных APT-группировок[3];
- оставшиеся 60% инцидентов связаны с деятельностью APT-группировок, которые на момент исследования не удалось однозначно идентифицировать, и других неустановленных злоумышленников, основным мотивом которых послужила финансовая выгода и (или) хактивизм, в том числе политической окраски;

[3] APT-группировка — организованная киберпреступная структура с высоким уровнем технической подготовки, обладающая ресурсами и возможностями для долгосрочного скрытого присутствия в инфраструктурах компаний-жертв.

С начала 2022 года мы отмечаем рост количества инцидентов политической направленности (на момент публикации оно составляет 9% от общего числа за исследуемый период). Ранее такие мотивы в атаках злоумышленников практически не наблюдались.

- в 25% выполненных проектов по ретроспективному анализу инфраструктур компаний были выявлены следы деятельности APT-группировок, зачастую находившихся в сетях компаний-жертв достаточно длительное время (от полугода до года на момент анализа), не выдавая себя;
- чаще всего атакам APT-группировок подвергались государственные учреждения (34%), промышленные предприятия (30%), ИТ-компании (7%), СМИ (5%) и телекоммуникационные компании (5%);
- в среднем злоумышленники находились в инфраструктуре компании-жертвы до момента их обнаружения (time to detect, TTD) 37 дней (медианное значение), а самое долгое пребывание в инфраструктуре составило 3 года;
- среднее время от начала расследования до написания итогового отчета (time to response, TTR) составило 21 день, причем нередко первые результаты расследований удавалось получить всего через несколько часов после обращения;

[4] Кибератака, в ходе которой злоумышленники получают несанкционированный доступ в корпоративную инфраструктуру путем компрометации поставщиков ПО или оборудования пострадавшей компании. Например, злоумышленники могут внедрить вредоносную функциональность в исходный код программного продукта или распространить вредоносные обновления ПО, чтобы заразить инфраструктуру целевой организации.

На основании первых результатов расследований можно оперативно предпринять организационно-технические меры для противодействия злоумышленнику.

Более подробно о том, как быстро получать первые значимые результаты расследований, можно прочитать в основной части исследования в пункте «Что может повлиять на время расследования».

- за первые три квартала 2023 года количество инцидентов, вызванных атаками типа supply chain[4] и trusted relationship[5], выросло в два раза по сравнению с аналогичным показателем, взятым за весь 2022 год.

В результате выявленных инцидентов пострадавшие компании чаще всего сталкивались:

- с нарушениями внутренних бизнес-процессов (32%);
- кибершпионажем — достаточно длительным пребыванием злоумышленников в инфраструктуре жертвы, как правило с целью непрерывной выгрузки конфиденциальной информации (32%);
- непосредственно с выгрузкой конфиденциальной информации (26%).

Мы проанализировали наиболее важные, на наш взгляд, аспекты исследованных инцидентов, в том числе ошибки, допущенные в системах безопасности компаний, и подготовили перечень рекомендаций, которые помогут свести к минимуму[6] количество успешных атак.

[5] Кибератака, в ходе которой злоумышленники получают несанкционированный доступ в корпоративную инфраструктуру путем компрометации доверенной третьей стороны, с которой у пострадавшей компании есть организованные каналы связи. В качестве примера можно привести компрометацию филиала, через которую злоумышленники попадают в корпоративную инфраструктуру головной организации.

[6] Полностью исключить атаки, к сожалению, не представляется возможным, так как, например, злоумышленники могут воспользоваться уязвимостями нулевого дня (уязвимости, о которых еще никому неизвестно).

Основная часть исследования

Отличие ретроспективного анализа инфраструктуры от проектов по реагированию на инциденты ИБ

Как правило, ретроспективный анализ инфраструктуры проводится с целью выявить следы возможной компрометации за максимально доступный промежуток времени. Этот период определяется, в частности, исходя из глубины хранения журналов и имеющихся forensic-артефактов. В ходе ретроспективного анализа эксперты:

- проводят сигнатурное сканирование файловых систем и оперативной памяти на узлах инфраструктуры с целью поиска потенциального вредоносного ПО и его дальнейшего анализа;
- собирают и детально анализируют прочие релевантные сведения (журналы событий ОС, следы пользовательской активности, информацию о пользовательских сессиях, следы запуска ПО на конечных узлах, журналы со всех доступных СЗИ — средств защиты информации и т. д.);
- собирают сетевые артефакты и проводят их анализ по репутационной базе PT ESC.

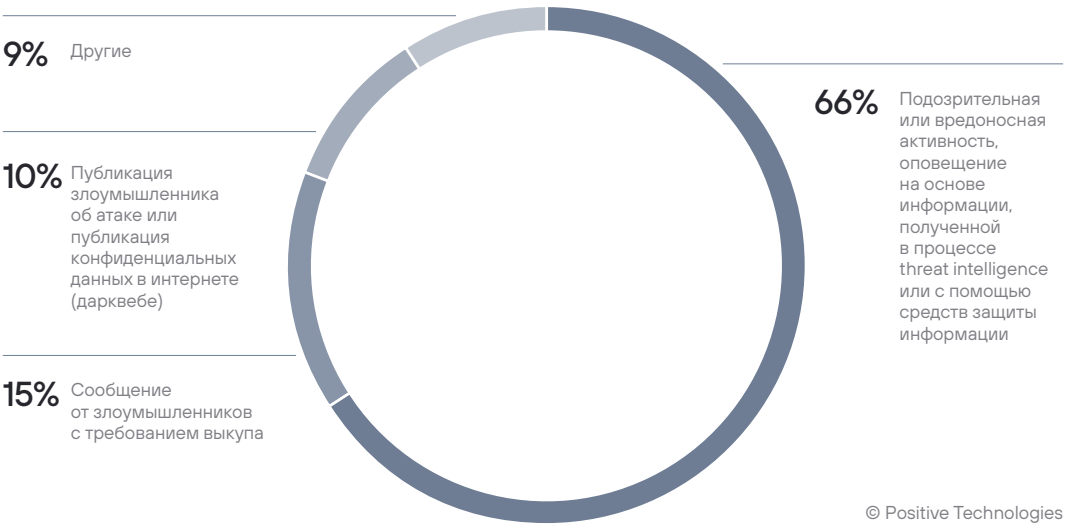
Доля ретроспективных проектов в нашей выборке — 18%.

Среднее время проведения подобного проекта — 30 дней.

Расследование инцидента информационной безопасности, как правило, инициируется по одной из следующих причин:

- обнаружение подозрительной или прямо вредоносной активности в инфраструктуре компании-жертвы (в частности, при помощи имеющихся СЗИ) либо оповещение на основе информации, полученной в процессе threat intelligence (66% случаев);
- получение пострадавшей компанией информации от злоумышленников о шифровании или затирании ими данных в корпоративной инфраструктуре, в большинстве случаев с требованием выкупа (15%);
- обнародование злоумышленниками информации о проникновении во внутреннюю сеть компании или публикация похищенных конфиденциальных сведений в интернете или даркнете (10%).

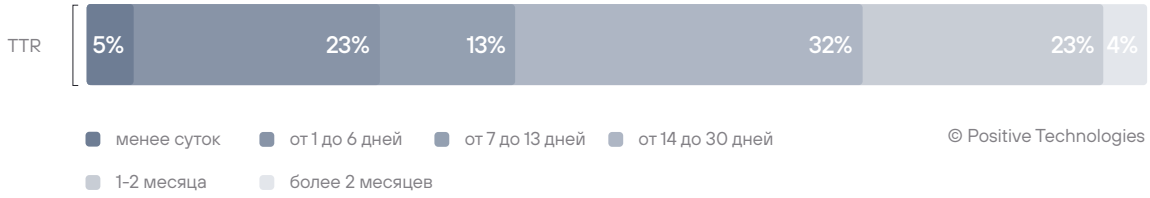
Рисунок 3. Причины обращений пострадавших компаний (доля отчетов о расследовании инцидентов ИБ)



Среднее время от начала расследования до написания итогового отчета составило 21 день. С общим распределением можно ознакомиться на рисунке 4. Если компания при обнаружении инцидента незамедлительно обратилась к IR-экспертам PT Expert Security Center и передала все необходимые для начала расследования сведения — первые значимые результаты[7] могут быть получены уже в течение нескольких часов.

[7] В частности, первичные сведения о хронологии и причинах инцидента и рекомендуемые организационно-технические меры по противодействию злоумышленнику, такие как указания по изоляции пораженных узлов.

Рисунок 4. Время от начала расследования до готового отчета (TTR)



Что может повлиять на время расследования

- Несвоевременный сбор сведений, необходимых для расследования.

Собирая необходимые для расследования данные не сразу после обнаружения инцидента (спустя несколько дней или даже позже), вы повышаете вероятность ротации[8] релевантных для анализа журналов.

- Несвоевременное предоставление собранных данных, отказ от предоставления информации в требуемом объеме.

Чем больше затягивается этот этап, тем дольше злоумышленники присутствуют в инфраструктуре вашей компании и тем больший ущерб они могут нанести бизнесу.

- Некорректные действия специалистов по защите информации и информационным технологиям в компании-жертве.

В результате некорректных (хотя и интуитивно понятных) действий специалистов по ИТ и ИБ на месте происшествия могут быть безвозвратно удалены образцы вредоносного ПО (нужные для дальнейшего исследования с целью, например, получения индикаторов компрометации), уничтожено содержимое оперативной памяти (вследствие перезагрузки компьютера), а также утеряны другие ключевые сведения, необходимые для проведения качественного расследования.

[8] Процесс затирания журналов по истечении установленного времени для оптимизации дискового пространства, предоставляемого под их хранение.

После того как остановлено развитие атаки или митигирована острая фаза (как правило, до 2–3 дней), IR-эксперты PT Expert Security Center приступают к активной фазе расследования. В среднем она занимает 5–7 рабочих дней. За это время, как правило, в большинстве случаев удается установить масштаб инцидента, TTP[9] злоумышленников, основной используемый инструментарий и управляющую сетевую инфраструктуру. Эти сведения позволяют оперативно разработать и принять эффективные организационно-технические меры по локализации инцидента и ликвидации присутствия злоумышленников в инфраструктуре, иными словами, составить и реализовать план по реагированию на инцидент.

[9] Tactics, techniques, and procedures (TTP) — описание действий злоумышленника во время атаки. Знание TTP позволяет более эффективно составить верхнеуровневое описание кибератаки, и более детально ее декомпозировать.

Интересный факт

С начала пандемии COVID-19 и по сегодняшний день большая часть (95%) инцидентов, с которыми обращаются к IR-экспертам PT Expert Security Center, расследуется в формате удаленного взаимодействия. Такой формат позволяет получить первые результаты быстрее, не тратя время на дорогу до места расположения пострадавшей компании. Однако если регламент компании категорически не предусматривает никаких вариантов удаленного взаимодействия, эксперты всегда готовы пойти навстречу и провести все работы непосредственно на территории.

IR-эксперты PT Expert Security Center разработали инструментарий для реагирования на инциденты и их расследования, охватывающий большое число популярных ОС, включая Windows, Linux и macOS.

Более подробно познакомиться с форматом удаленного взаимодействия, а также используемым нашими экспертами инструментарием можно в статье «Incident response на удаленке: как вызовы COVID-19 превратились в новые практики».

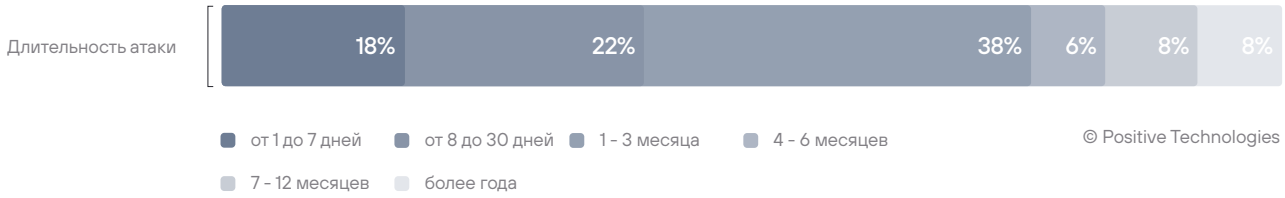
В ходе расследования инцидента IR-эксперты PT Expert Security Center при непосредственном содействии технических специалистов обратившейся компании:

- проводят анализ доступных журналов средств защиты информации, образцов вредоносного программного обеспечения, сетевых индикаторов, дампов оперативной памяти, образцов сетевого трафика и других наборов данных с ключевых узлов инфраструктуры, как затронутых, так и не затронутых в ходе инцидента;
- определяют перечень скомпрометированных узлов и учетных записей;
- определяют исходный вектор атаки и восстанавливают хронологию инцидента;
- составляют перечень обнаруженного ВПО, узловых и сетевых индикаторов компрометации;
- производят сканирование всей доступной инфраструктуры на наличие выявленных индикаторов компрометации;
- ликвидируют присутствие злоумышленников, включая их каналы связи, в инфраструктуре.

Как действуют злоумышленники

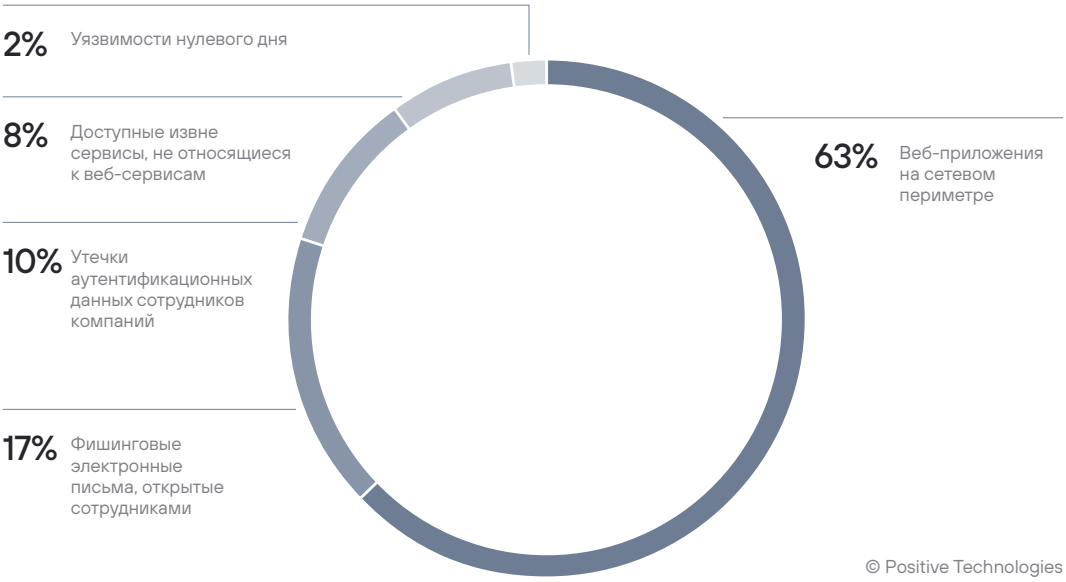
Среднее время с момента компрометации инфраструктуры преступниками и до их остановки (или локализации) составило 45 дней (медианное значение); самая долгая атака длилась 5 лет. С соответствующим распределением можно ознакомиться на рисунке 5.

Рисунок 5. Длительность атаки



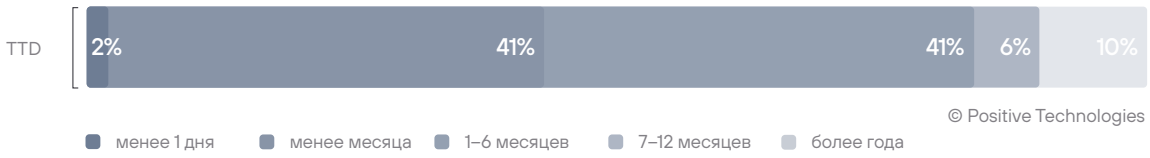
В качестве исходного вектора проникновения злоумышленники чаще всего (63%) эксплуатировали уязвимости в используемых жертвой публично доступных в интернете веб-приложениях. В частности, среди таких веб-приложений наиболее часто, по нашему опыту, подвергались атакам почтовый сервер Microsoft Exchange (50% всех атак, где в качестве исходного вектора проникновения были уязвимые веб-приложения), веб-сервер «Битрикс» (13%) и продукты компании Atlassian (7%), например Confluence и Jira. На втором месте по частоте успешного использования — фишинговые письма, направляемые на электронную почту.

Рисунок 6. Исходные векторы проникновения в сети компаний



На момент начала расследования злоумышленник в большинстве случаев (96%) еще находится в скомпрометированной инфраструктуре или как минимум имеет доступный установленный заранее канал связи. Медианное время с момента компрометации и до обнаружения злоумышленников (TTD) составило 37 дней, самое долгое — 3 года. С соответствующим распределением можно ознакомиться на рисунке 7.

Рисунок 7. Время с момента компрометации до обнаружения злоумышленников (TTD)



Одними из наиболее часто встречающихся в последнее время (21% среди общего числа инцидентов, расследованных в исследуемый период) можно с уверенностью назвать инциденты, связанные с полным шифрованием или затиранием информации на узлах инфраструктуры заказчика. Полный перечень соответствующего ВПО[10], выявленного при расследовании инцидентов ИБ, представлен в таблице 1.

[10] Важно отметить, что в таблице встречается ПО, которое может использоваться и в легитимных целях (BitLocker, DiskCryptor).

Таблица 1. Перечень ВПО для шифрования и (или) затирания информации, выявленного в рамках проектов по расследованию инцидентов ИБ

Omerta	TinyCrypt	Babuk и его модификации, например BadWeather	Filecoder.MY
BitLocker	Phobos	CrossLock	Locker
Zeppelin	DiskCryptor	BlackCocaine	CaddyWiper и его модифицированные версии
VoidCrypt	LockBit	RCRU64	

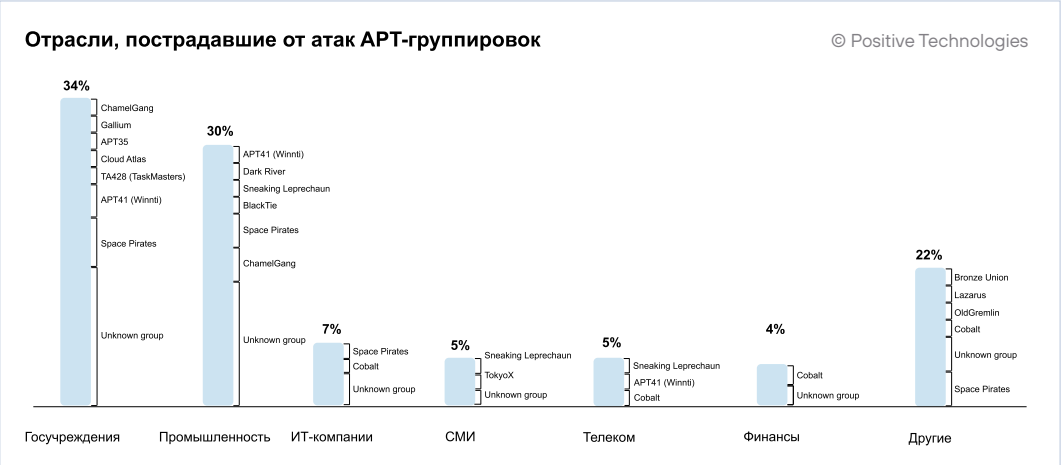
Атрибуция злоумышленников, ответственных за кибератаку, — это сложный процесс, который не всегда завершается успешно. За последние три года IR-эксперты PT Expert Security Center выявили инциденты с участием 15 известных APT-группировок, идентифицируемых на основании используемого инструментария, сетевой инфраструктуры и TTP. Полный перечень представлен в таблице 2.

Таблица 2. Перечень идентифицированных APT-группировок

APT35 (Magic Hound)	Cloud Atlas	OldGremlin
APT41 (Winnti)	Cobalt	Sneaking Leprechaun
BlackTie (Twisted Panda)	Dark River	Space Pirates
Bronze Union	Gallium	TA428 (TaskMasters)
ChamelGang	Lazarus	TokyoHotel

Доля инцидентов, которые удалось однозначно связать с деятельностью конкретных публично известных APT-группировок, за исследуемый период составила 40%. Распределение жертв подобных атак (а также атак с участием неустановленных APT-группировок) по отраслям представлено ниже на рисунке 8.

Рисунок 8. Категории жертв, пострадавших от атак APT-группировок



Как правило, APT-группировки используют уникальное ВПО, которое отвечает за доступ злоумышленников в инфраструктуру компании после первичной компрометации. С примерами можно ознакомиться в таблице 3.

Таблица 3. Вредоносное ПО, использованное в атаках APT-группировками

App_global	Daxin	Facefish	Msdaprst Backdoor	ShadowPad
Backdoor Leiosaurid	Decoy Dog	Fasol RAT	MsmRAT	Sidewalk
BeaconLoader	Deed RAT	Gh0st RAT	Owowa	SPINNER
Bisonal	DiskTool	IP He1per (PingPull)	PlugX	TaskMasters Backdoor
CobInt	DNSep	Kitsune	ProjC	TaskMasters Backdoor PowerShell
Cotx RAT	DonutHole	MataDoor	PwShell	TgRAT
DarkPulsar (2017)	DoorMe	Microcin	RemShell	ThreatNeedle
TinyFluff	TinyNode	TokyoHotel	Voidoor	XDSpy

© Positive Technologies

Тем не менее как APT-группами, так и менее квалифицированными злоумышленниками используется вспомогательное ПО, в подавляющем большинстве случаев публично доступное в интернете. Мы проанализировали это ПО и разметили его на тепловой карте MITRE ATT&CK® в зависимости от выполняемой задачи и частоты выявления в проектах.

Рисунок 9. Инструменты, использованные злоумышленниками в атаках

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Impacket	Неустановленный веб-шелл	invoke-uac-me	UPX	Mimikatz	Advanced IP Scanner	Impacket	7-Zip	Cobalt Strike	rclone	LemonDuck
RemCom	China Chopper	LinEnum	CFFlooderObfuscator	Impacket	nmap	PsExec	WinRAR	ngrok	MEGAsync	Adminer
PowerSploit	Gel4y	Sysinternals	PowerSharpPack	dploot	SoftPerfect Network Scanner	RemCom		Stowaway		Blat
PPLKiller	WSO		Safengine	HackBrowserData	Sysinternals	CrackMapExec		FRP		db1000n
NirSoft			ScareCrow	Lazagne	Bloodhound	Rubeus		Sliver		Wannamine
NSSM			Shikata Ga Nai Encoder	linpeas	NBTscan	NirSoft		Metasploit		
Sysinternals			StdVectorPacker	NirSoft	ADRecon	PsTools		Chisel		
Неустановленный веб-шелл			Themida	ProcDump	AD Explorer	Sysinternals		dnscat2		
			VMProtect	Sysinternals	masscan			gsocket		
			ProcHider	ChangePw	ncat			Neo-reGeorg		
				QuarksPWDump	NirSoft			Poison Ivy RAT		
					noPac			ReGeorg		
					PortQry			Venom Proxy		
					3snake			DarkCrystal RAT		
					Advanced Port Scanner			Diamorphine		
					evil-mhyprot-cli			Dogtunnel		
					fscan			donut		
					Hydra			EarthWorm		
					kingron/s			go-gost		
					KPortScan			go-socks		
					Linux Smart Enumeration			Putty		
					NetSpy			revsh		
					Straciatella			socat		
					Seatbelt			SocksOverRDP		
					SharpHound			Tiny SHell		
					Smbtouch-Scanner			ZxShell		
					WinPwn					

Тепловая карта инструментов, использованных злоумышленниками

Доля проектов, в которых использовались инструменты

<5 5–14 15–20 >20

Время от времени в инструментарий злоумышленников попадают общедоступные легитимные утилиты для удаленного управления узлами (7% от числа всего выявленного ПО в проектах), принесенные в инфраструктуру пострадавшей компании извне самими преступниками или уже используемые ее сотрудниками, например системными администраторами, на момент атаки. С полным перечнем подобных утилит, выявленных при расследовании инцидентов за наблюдаемый период, можно ознакомиться в таблице 4.

Таблица 4. Перечень утилит для удаленного управления узлами

RemoteUtilities (RMS)	TeamViewer	Mesh Agent
Dameware	AnyDesk	AmmyyAdmin
Radmin	WireGuard	Atera
Remote Utilities	Pulseway	Splashtop
OpenVPN		

Злоумышленники не обходят стороной и такой метод атаки, как Living off the Land. Он заключается в том, что для выполнения нелегитимных действий используется легитимное ПО и компоненты операционных систем. С полным перечнем подобных утилит можно ознакомиться на странице проекта LOLBAS. Метод Living off the Land предоставляет преступникам возможность замаскировать вредоносную активность и таким образом остаться незамеченными для СЗИ и специалистов по ИБ пострадавшей компании.

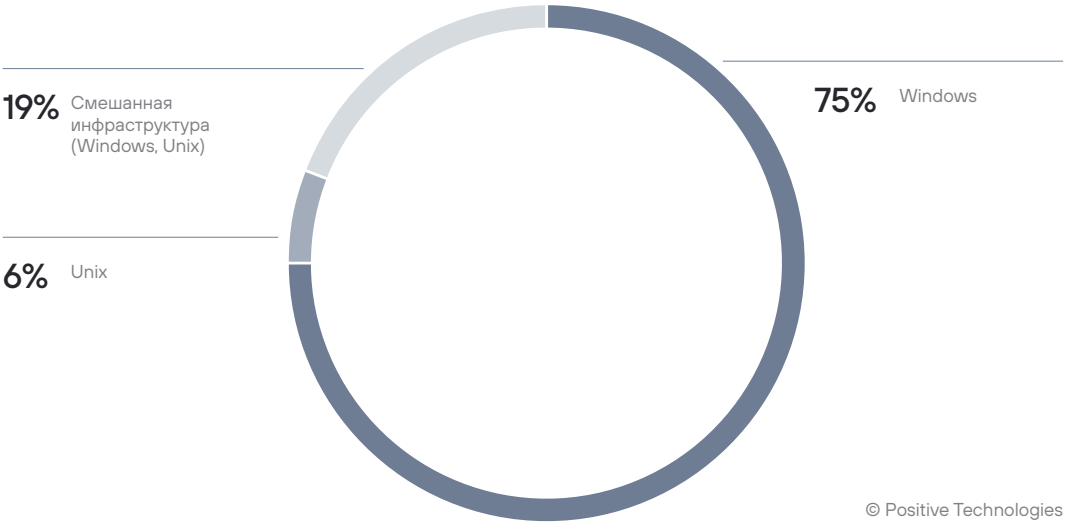
Во всех наших проектах по расследованию инцидентов ИБ злоумышленники использовали встроенные интерпретаторы команд, например cmd, PowerShell и bash.

Примечательно, что в некоторых случаях преступники нестандартно применяли утилиты certutil и msbuild: с помощью certutil они загружали вредоносное ПО из интернета, а msbuild использовалась для запуска полезной нагрузки Cobalt Strike Beacon.

В результате анализа всех проектов предсказуемо выяснилось, что чаще всего при атаке злоумышленники компрометировали узлы под управлением Windows. Однако мы бы хотели обратить внимание на то, что обнаружили немало скомпрометированных узлов и под управлением Linux. Это лишний раз подтверждает ошибочность подхода, декларирующего полную неуязвимость данной ОС или ее ничтожно малую подверженность атакам.

Если в вашей инфраструктуре есть узлы под управлением Linux, уделите особое внимание их защите.

Рисунок 10. Доля ОС на скомпрометированных узлах, выявленных в процессе расследований



Последствия атак

При проведении расследования IR-эксперты PT Expert Security Center оценивают влияние инцидента на инфраструктуру и бизнес-процессы компании. В большинстве случаев последствия могут быть следующими:

- разведывательная деятельность, шпионаж;

Характеризуется достаточно длительным присутствием (медианное значение — 35 дней) злоумышленников в инфраструктуре жертвы. В течение этого времени злоумышленник непрерывно получает оперативный доступ к конфиденциальным сведениям.

- выгрузка конфиденциальной информации;

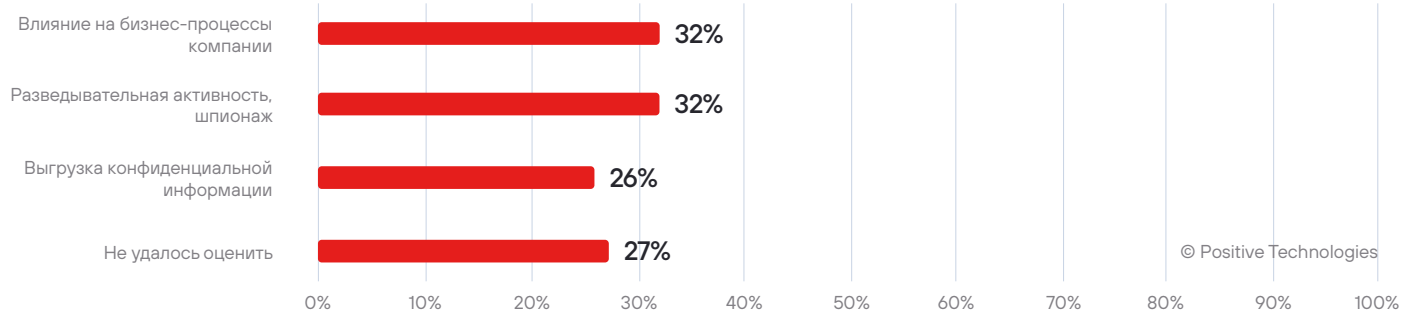
Одним из маркеров выгрузки злоумышленниками конфиденциальной информации зачастую служит состав использованного инструментария, в частности общедоступное ПО для архивации данных WinRar и 7z. За последние годы также участились случаи выгрузки похищенной информации на общедоступные файловые обменники или облачные ресурсы при помощи таких утилит, как Rclone и MEGASync.

С 2022 года мы наблюдаем увеличение количества инцидентов, в которых злоумышленники выгружали определенные пользовательские данные с целью получения доступа к аккаунтам мессенджера Telegram Desktop сотрудников пострадавших компаний. Нередко аккаунты пользователей в этом мессенджере содержат актуальные аутентификационные данные для доступа к корпоративным информационным системам, а также другую конфиденциальную информацию. Доля таких инцидентов среди прочих, в результате которых были выгружены конфиденциальные данные, составила в 2022 году 9%, а за первые три квартала 2023 года — уже 63%.

- воздействие на бизнес-процессы.

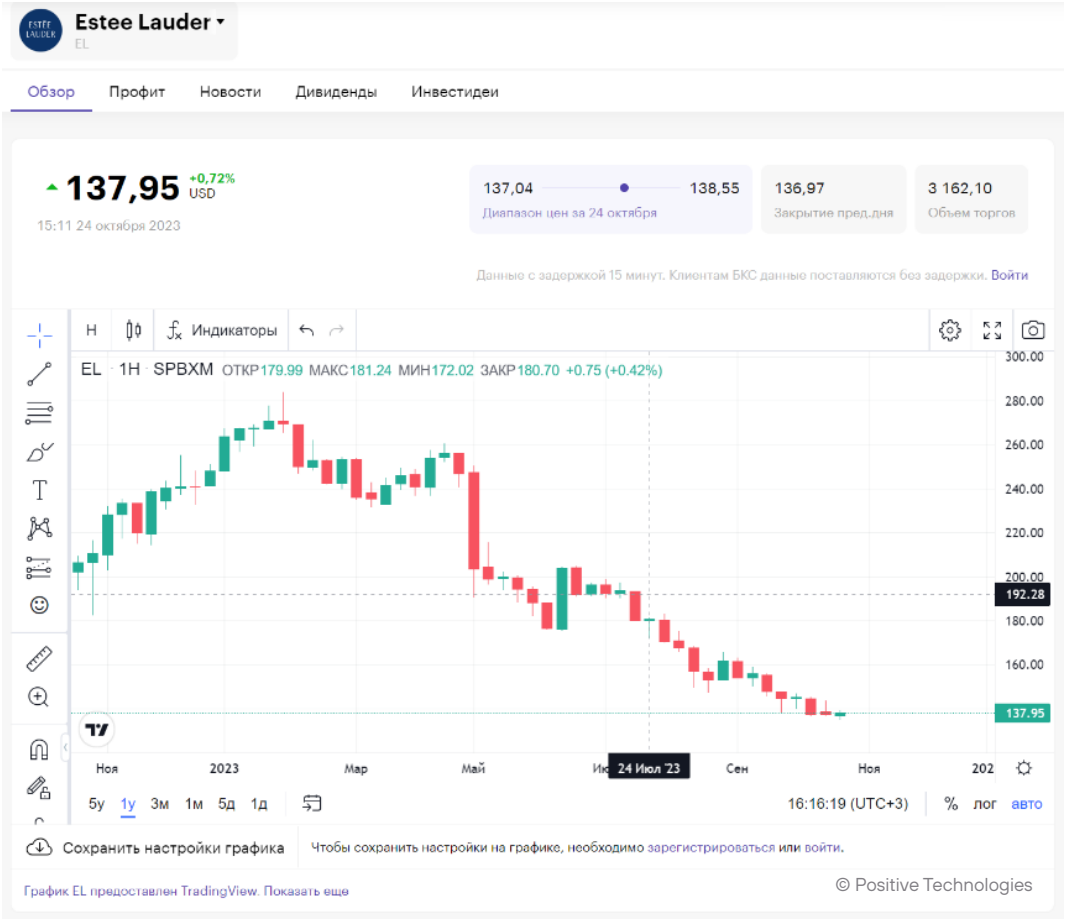
Характеризуется нарушением работы ключевых узлов инфраструктуры компании-жертвы. Чаще всего с таким последствием сталкиваются после запуска злоумышленниками ВПО для шифрования или затирания данных.

Рисунок 11. Последствия атак злоумышленников (доля проектов)



Оценка финансового ущерба от атак не проводилась в связи с тем, что для этого требуется отслеживать финансовые показатели компаний на протяжении нескольких лет. Именно такой способ оценки позволяет наиболее точно определить степень влияния кибератаки на бизнес-показатели. Например, после кибератаки в конце июля 2023 года акции компании Estee Lauder на момент проведения исследования до сих пор не восстановились в цене.

Рисунок 12. Падение акций компании Estee Lauder после 20.07.2023



По данным экспертов компании IBM, в 2023 году средний ущерб от атаки, в результате которой происходила утечка конфиденциальных данных, составил 4,45 млн долл. США. А средний ущерб от успешной атаки с использованием программы-вымогателя, по данным специалистов Embroker, составляет 1,85 млн долл. США.

Примеры выявленных атак

Рисунок 13. Пример типового сценария развития атаки с наиболее часто встречающимися практическими целями (шпионаж и шифрование или затирание данных)

Сценарии атак, наблюдаемых при расследовании инцидентов, зачастую начинаются примерно одинаково вне зависимости от целей и мотивов злоумышленников. В качестве подготовительного этапа атакующие всегда проводят рекогносцировку (Reconnaissance), то есть собирают и изучают общедоступные сведения о компании, ее сотрудниках, сервисах и доступных ресурсах.

Затем злоумышленники пытаются получить первоначальный доступ (Initial Access) в инфраструктуру — например, обнаружив и проэксплуатировав уязвимый сервис на сетевом периметре компании или проведя успешную фишинговую кампанию в отношении ее сотрудников.

Еще один способ попасть во внутреннюю сеть компании — применить методы социальной инженерии к ее сотрудникам. К примеру, злоумышленники могут направить им фишинговое сообщение, содержащее вредоносное вложение или ссылку на мошеннический сайт.

С этим и другими способами проникновения во внутреннюю сеть компании подробнее можно ознакомиться в соответствующем разделе матрицы MITRE ATT&CK®.

После получения первоначального доступа злоумышленники стараются разместить в инфраструктуре вредоносное ПО для удаленного подключения к их управляющим серверам (Command and Control) и обеспечения постоянного доступа (Persistence). В качестве примеров можно выделить фреймворки Sliver и Cobalt Strike. Как правило, уже на этом этапе атаки встает вопрос ухода от детектирования средствами защиты с целью сокрытия вредоносной активности. Для подобных целей используется разнообразное ПО, в основном направленное на противодействие статическому анализу (Defense Evasion).

Познакомиться с полным перечнем инструментов, использованных злоумышленниками на разных этапах атаки, можно на рисунке 9.

В подавляющем большинстве случаев после проникновения в инфраструктуру злоумышленники проводят хостовую и сетевую или доменную разведку (Discovery) — как правило, на протяжении всего своего пребывания в инфраструктуре жертвы. В результате они могут, например, получать списки процессов, пользователей и их привилегий, перехватывать запросы, получать доступ к базам данных, содержащим конфиденциальную информацию, информацию о структуре объектов Active Directory и другие данные.

Освоившись в инфраструктуре, киберпреступники стараются повысить привилегии (Privilege Escalation), к примеру получив доступ к учетной записи администратора домена. Сделать это можно различными способами, например с помощью извлечения из памяти процесса lsass.exe хэшей паролей. Они могут быть использованы в атаке типа Pass the Hash, что в дальнейшем позволит получить доступ к доменному контроллеру. Привилегированный доступ позволяет злоумышленникам беспрепятственно перемещаться по инфраструктуре компании (Lateral Movement) и распространять вредоносное ПО, соответствующее их целям.

После повышения привилегий, преступники могут действовать по-разному в зависимости от целей:

- Злоумышленники, распространяющие вредоносное ПО для шифрования и (или) затирания данных (в частности, в ряде расследований нами было обнаружено, что для этого использовались ранее скомпрометированные установленные в компании СЗИ), на этом этапе могут загрузить и запустить свое вредоносное ПО (Impact) или, к примеру, для начала выполнить эксфильтрацию (Exfiltration) конфиденциальных сведений, добытых в результате хостовой и сетевой или доменной разведки.

Тренд с выгрузкой конфиденциальных сведений компании-жертвы перед запуском ВПО мы наблюдаем с 2020 года. Такой шаг позволяет злоумышленникам запрашивать выкуп как за восстановление доступа к инфраструктуре, так и за неразглашение украденной информации.

- Злоумышленники, проводящие шпионскую кампанию, в большинстве случаев будут менее шумными. Они заинтересованы в том, чтобы как можно дольше находиться в инфраструктуре компании и оперативно собирать конфиденциальные сведения (корпоративные документы, таблицы, презентации, базы данных — нередко в подобных материалах содержатся в том числе аутентификационные данные в открытом виде).

Чтобы вовремя заметить злоумышленников, нацеленных на кибершпионаж, в инфраструктуре следует выстроить процессы мониторинга. Для некоторых техник, которые встречались в инцидентах, мы уже предлагали набор мер по обнаружению. С ними можно ознакомиться в статье «Как обнаружить 10 популярных техник пентестеров».

Резюмируя эту часть исследования, мы хотим еще раз подчеркнуть, что вне зависимости от мотива, который преследуют злоумышленники, на начальных этапах атаки они часто совершают примерно одни и те же действия. Обратив пристальное внимание на обнаружение TTP и инструментария, характерных для этих этапов, вы сможете вовремя пресечь атаку и не допустить реализации недопустимого события.

Заключение

Наша практика показывает, что многих инцидентов удалось бы избежать или, по крайней мере, уменьшить причиненный ими ущерб. Для этого мы рекомендуем:

- Использовать последние версии ПО и ОС, выстроить процессы, связанные с управлением уязвимостями и их устранением. Отслеживать трендовые уязвимости на активах и установить SLA по их устранению — 24 часа.
- Соблюдать best practices, в частности при определении парольной политики компании.
- Включить требование двухфакторной аутентификации для всех общедоступных сервисов на периметре и критически важных элементов во внутренней сети компании.
- Использовать принцип наименьших привилегий.
- Настроить сегментацию сетевой инфраструктуры и ограничить доступ между сегментами в соответствии с вашими бизнес-процессами, а также устранить неконтролируемую сетевую связность на всех уровнях инфраструктуры.
- Настроить процесс регулярного создания резервных копий для всех узлов домена и организовать хранение этих копий на изолированном от основной сети узле.
- Постоянно проводить проверку периметра инфраструктуры как на наличие уязвимостей и общедоступных сервисов.
- Настроить мониторинг событий ИБ для своевременного выявления инцидентов и реагирования на них.

Также мы настоятельно советуем использовать средства и технологии защиты информации, которые доказали свою эффективность в борьбе с киберпреступниками, например:

- системы контроля привилегированных учетных записей;
- системы управления уязвимостями (VM);
- системы управления событиями информационной безопасности (SIEM);
- системы поведенческого анализа сетевого трафика (NTA);
- современные межсетевые экраны нового поколения (NGFW) для защиты каналов, сегментации сети и харденинга сетевых маршрутов;
- межсетевые экраны уровня приложений (WAF);
- системы статического и динамического анализа для выявления вредоносных объектов (sandbox);
- антивирусное ПО и решения для обнаружения событий, связанных с вредоносной активностью на конечных узлах, и реагирования на них (EDR), а также более продвинутые классы решений XDR.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 200 тысяч акционеров.

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.