СЕТЕВАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННОГО СЕКТОРА

ROOT LEVEL RESOURCES

Телекоммуникационный сектор является одним из приоритетных для атак проправительственных группировок на критически важные объекты инфраструктуры государств. Так, скомпрометировав компанию сектора, злоумышленники получают доступ к ее клиентам с целью шпионажа и саботажа. Такие действия приводят к негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической и прочих сферах.

Основные вызовы сетевой безопасности в телекоммуникационном секторе:

Телекоммуникационные услуги сильно зависят от различных взаимосвязанных средств связи (маршрутизаторов, коммутаторов, серверов и т.п.), как результат, проблемы безопасности телекоммуникаций могут возникать в различном оборудовании и быстро распространяться через сеть на другое оборудование.

BGP hijacking

Суть угрозы заключается в перенаправлении сетевого трафика отдельных префиксов автономной системы (пулов IP-адресов) через свое оборудование.

Уязвимые роутеры

Небезопасные настройки и невозможность обновления оборудования приводят к деградации сервиса и росту вредоносного трафика.

2G/3G/4G

Недостатки защиты мобильных сетей позволяют обходить тарификацию, пользоваться услугами связи за счет других абонентов, перехватывать SMS, прослушивать разговоры, менять условия обслуживания, обходить ограничения оператора, переходить в небезопасный режим и лишать абонента связи. Кроме того злоумышленники получают возможность доступа к банковским счетам абонентов.

5G

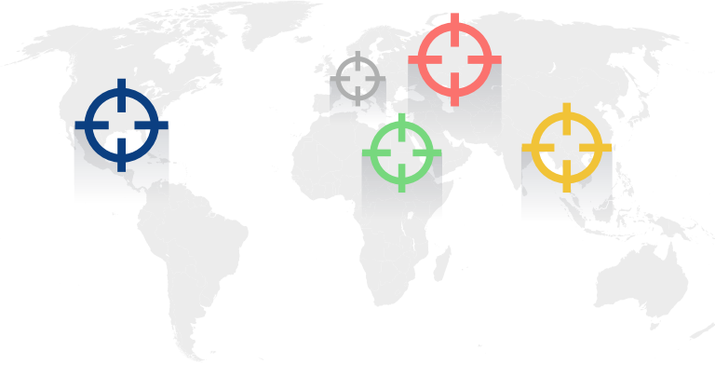
(новый драйвер угроз)

В связи с переходом на технологии 5G (стандартизация ожидается в 2021 году) появится новый рынок, который станет целью для лидерства у злоумышленников. Это может привести к демонстрации новых возможностей по взлому отдельных вендоров и появлению большого количества анонимных исследований об уязвимостях определенных технологических решений.

Все это может увеличить масштаб угроз: жертвами могут стать подключенные автомобили и системы жизнеобеспечения

Проправительственные группы, которые являются угрозой сектору:

За последние годы эксперты по информационной безопасности обнаружили новые группы, спонсируемые государствами. Многие из них уже давно совершают атаки на сектор, но длительный перид оставались незамеченными. Кроме того, многие из них действуют аналогичными методами на одинаковые цели, чем создают конкуренцию и сложность в их обнаружении.



Название группы/ Период активности	География основных атак	Вектор проникновения	Инструменты
APT 10 (Китай) *Январь 2012 – настоящий момент*	Европа; Азиатско-Тихоокеанский регион	Модифицированная версия веб-оболочки.	Poison Ivy RAT
WINNTI (Китай) *Январь 2017- апрель 2019*	Азиатско-Тихоокеанский регион; Ближний восток и Африка; Россия и СНГ	"Living off the land" - использование легитимных локальных приложений во вредоносных целях для установки троянов.	ShadowPad
MUDDY WATER (Иран) *Сентябрь 2017 – настоящий момент*	Европа; Ближний восток и Африка; Россия и СНГ	Атаки через доступ локальной сети оператора мобильной связи.	Powerstats
THRIP (Китай) *Январь – июнь 2018*	Точно не установлено	"Living off the land" - использование легитимных локальных приложений во вредоносных целях для установки троянов.	PsExec, Mimikatz, WinSCP и LogMeIn
APT33 (aka Elfin, Magnallium) (Иран) *Июнь 2016 – декабрь 2018*	США; Европа; Ближний восток и Африка	Перезапись MBR, разделы и файлы в системе случайно сгенерированными данными.	Shamoon
CHAFER (aka APT39) (Иран) *Июль 2014 – настоящий момент*	Ближний восток и Африка; Азиатско-Тихоокеанский регион	Фишинговые письма, использование украденных учетных записей	POWBAT, Antak, Asxpy
LAZARUS (Северная Корея) *Март 2016 – ноябрь 2018*	США; Европа; Азиатско-Тихоокеанский регион; Ближний восток и Африка; Россия и СНГ	Целевой фишинг, социальные сети, атаки типа watering hole.	Ratankba, PowerRatankba, ClientRAT, ClientTraficForwarder (Proxy), AppleJeus, PowerTask, PowershellRAT, Bankswift/BBSwift, RatankbaPOS, Mimikatz, Metasploit, Dtrack, Rising Sun
LYCEUM (так же известный как HEXANE) *Апрель 2018 – настоящий момент*	Ближний восток и Африка; Россия и СНГ	Атаки через поставщиков (Supply Chain), целевой фишинг, подбор паролей, брутфорс	DanBot, Posh C2, PowerShell Empire

Проблемы безопасности в телекоммуникационном секторе, помимо саботажа и шпионажа, являются основной причиной потери персональных данных и финансовой информации о клиентах. Это приводит к тому, что компании телекоммуникационного сектора, подвергшиеся атакам, кроме прочего, привлекаются к материальной ответственности (в крупных размерах) за невозможность реализовать необходимые технические и организационные меры для защиты персональных данных своих клиентов, в соответствии с положениями GDPR (General Data Protection Regulation).

Стоит обратить внимание, что большинство проправительственных групп враждуют между собой и выкладывают в открытый доступ инструменты и материалы о своих соперниках. С одной стороны, это помогает в уголовном преследовании разоблаченных лиц, с другой — позволяет более эффективно маскироваться.

Действия группировок, которые финансируются государством, как правило, планируются единым государственным центром на стратегическом, тактическом и операционном уровнях и проводятся под особым контролем. Все это приводит к тому, что идентифицировать атаки и их виновников становится крайне сложной задачей, так же как и вопрос привлечение их к ответственности.

Поэтому основные надежды возлагаются на технологии и провайдеров сетевой безопасности, которые смогут закрыть старые бреши и избежать новых, таким образом, повысив безопасность маршрутизаторов и снизить риски манипуляции в телекоммуникационном секторе.

Используемые источники:

ROOT LEVEL RESOURCES

1 Отчеты Компании Secureworks // URL: https://www.secureworks.com/

2 Отчеты Компании Dragos // URL: https://dragos.com/

3 Отчеты Компании Group-IB // URL: https://www.group-ib.ru/

4 Отчеты Компании Positive Technologies // URL: https://www.ptsecurity.com/ru-ru/