Контакты для прессы:
Екатерина Быстрова
eb@2l-pr.ru +7 (926) 318-30-26

Евгения Мамичева
e.mamicheva@2l-pr.ru +34 (635) 092 591

Trend Micro: в 2021 году количество выявленных киберугроз выросло на 42% и превысило 94 млрд. В странах Центральной Азии более 122 млн угроз содержались в сообщениях электронной почты

Ежегодный обзорный доклад Trend Micro поможет компаниям стран Центральной Азии в разработке стратегий кибербезопасности на 2022 год

Нур-Султан, 18 марта 2022 г. — Trend Micro Incorporated (TYO: 4704; TSE: 4704), мировой лидер в области кибербезопасности, предупреждает о растущем риске для цифровой инфраструктуры и удаленных работников, поскольку киберпреступные группировки увеличивают скорость атак на организации и частных лиц. Об этом эксперты компании рассказали в ежегодном обзорном докладе *Navigating New Frontiers. Trend Micro 2021 Annual Cybersecurity Report*.

В нём, помимо прочего, приводятся следующие данные о киберугрозах в странах Центральной Азии:

- лидером по количеству обнаруженных и заблокированных вредоносных писем стал Узбекистан: по данным доклада, количество обнаружений в 2021 году превысило показатель 60 млн;
- на первом месте по количеству обнаруженных экземпляров вредоносного ПО в 2021 году оказался Кыргызстан — на компьютерных системах страны заблокировано более 125 тыс. угроз;
- в Казахстане зафиксировано более 1 млн переходов пользователя на вредоносные сайты, ещё больше подобных действий в 2021 году совершили пользователи Узбекистана, нажавшие на опасные ссылки более 1,86 млн раз.

«Злоумышленники стремятся увеличить прибыль любыми способами, в том числе за счёт количества и эффективности атак, — комментирует Джон Клей (Jon Clay), вице-президент Trend Micro по анализу угроз. — Широкий спектр собранных нашими сенсорами данных о глобальных угрозах позволяет нам выявлять изменения в том, как злоумышленники атакуют своих жертв по всему миру. Наше последнее исследование показывает, что, хотя количество обнаруженных Trend Micro угроз в 2021 году выросло на 42% по сравнению с предыдущим годом и превысило 94 млрд, в некоторых регионах оно сократилось, поскольку атаки стали более точными».

По данным доклада, злоумышленники, использующие вымогательское ПО, фокусируются на критически важных отраслях и предприятиях, которые с большей вероятностью заплатят выкуп, а тактика двойного, тройного и даже четверного вымогательства обеспечивает несколько способов получения прибыли. Разработанные профессионалами вымогательские сервисы (Ransomware-as-a-Service — «вымогатель как услуга») открыли новый рынок для злоумышленников с ограниченными техническими знаниями и стали стимулом для формирования преступного конвейера. В ходе этого процесса выделяются всё более узкие

криминальные специализации, например, возникли брокеры начального доступа, которые стали важной частью «цепочки поставок» киберпреступности.

Эксперты Trend Micro поясняют, что хакеры всё активнее используют человеческий фактор для компрометации облачной инфраструктуры и удаленных сотрудников. Trend Micro Cloud App Security (CAS) обнаружила и предотвратила 25,7 млн угроз электронной почты в 2021 году по сравнению с 16,7 млн в 2020 году, причем количество блокированных попыток фишинга за этот период увеличилось почти вдвое. Наше исследование показало, что домашние работники часто склонны идти на больший риск, чем те, кто работает в офисе, что делает фишинг в отношении удалённых и гибридных работников особенно опасным.

Неправильно настроенные облачные системы продолжают формировать ландшафт рисков организаций. AWS Key Management Service (AWS KMS) и Amazon Elastic Container Service (Amazon ECS) имеют одни из самых высоких показателей неправильной конфигурации среди сервисов AWS. Trend Micro также обнаружила, что жертвами неправильной конфигурации часто бывают API-интерфейсы Docker REST, что делает их уязвимыми для атак хакерских группировок, специализирующихся на нелегальном майнинге криптовалют (TeamTNT, Outlaw, Kinsing и другие).

Хотя 2021 год стал рекордным по количеству новых уязвимостей, исследование Trend Micro показывает, что 22% эксплойтов, проданных на киберпреступных торговых площадках в прошлом году, были старше трёх лет.

Одновременно системы киберзащиты компании T&T Security, технологического партнёра Trend Micro в Казахстане, проанализировали более 1.5 миллиона файлов в различных организациях страны и зафиксировали бурный рост шпионского ПО в течение последнего года. Специалисты вирусной лаборатории T&T Security VirLab отмечают, что в атаках на территории РК с 2020 года особенно популярна платформа ВПО AveMaria/WarZone, которая используется злоумышленниками для удалённого доступа к компьютеру пользователя и получения ценных данных. В начале 2021 года T&T Security обнаружила в государственном секторе Казахстана разновидности популярного «стилера» Agent Tesla — вируса, который крадёт персональные данные сотрудников.

Помимо массовой рассылки спама с вредоносным ПО, в середине 2021 года компания отметила использование злоумышленниками атаки типа Spear Phishing (целенаправленный фишинг) на банковский сектор РК. Например, таким способом рассылался документ, который при открытии загружал вредоносный файл, устанавливающий Lokibot. Кроме того, T&T Security зафиксировала и исследовала артефакты трояна Razy, случайно размещённые на легитимных государственных ресурсах.

«Использование платформ для создания вредоносов приводит к резкому скачку угроз нулевого дня разного характера от шпионского ПО до шифровальщиков. - **сообщает эксперт Арнур Тохтабаев, Доктор PhD и основатель T&T Security.**

Наблюдается тенденция использования модели Ransomware-as-a-Service (вредонос по подписке) и техники Double Extortion, где злоумышленники требуют выкуп как за расшифровку данных, так и угрожают публикацией ценных данных организации. В последнее время также наблюдается переход конкретных техник, которые были присущи целевым угрозам в массовые атаки, например распространение шифровальщиков через цепочку поставок (supply chain), как это было сделано в случае с Kaseya REvil. Кроме того, проявляется

тенденция использования уязвимостей и в системах мировых вендоров кибербезопасности для распространения вредоносов (пример LockBit 2.0)”

Подобные тенденции требуют использование более современных подходов к защите, такие как принцип Zero Trust (нулевое доверие), в том числе на уровне поведенческого анализа в песочнице. Наш продукт tLab работает по принципу нулевого доверия опираясь на глубокий поведенческий анализ, а высокая пропускная способность позволяет анализировать десятки тысяч файлов в день без фильтров и белых списков, что эффективно блокирует подобные угрозы» — добавил эксперт.

Узнать больше подробностей из отчёта *Navigating New Frontiers. Trend Micro 2021 Annual Cybersecurity Report* можно на сайте Trend Micro.

О компании Trend Micro
Компания Trend Micro, мировой лидер в области кибербезопасности, помогает защитить обмен цифровой информацией во всём мире. Наша платформа кибербезопасности, разработанная с опорой на многолетний опыт работы в этой области, глобальные исследования угроз и постоянное внедрение инноваций, защищает сотни тысяч организаций и миллионы людей, а также облака, сети, устройства и конечные точки. Будучи лидером в области облачной и корпоративной кибербезопасности, мы предлагаем платформу с мощным набором передовых методов защиты, оптимизированных для таких сред, как AWS, Microsoft и Google, а также инструменты централизованной визуализации, позволяющие более быстро и эффективно обнаруживать угрозы и реагировать на них. Trend Micro — это 7000 сотрудников в 65 странах. Наши специалисты помогают организациям упростить и обезопасить их онлайн-среду. www.trendmicro.com.

О компании T&T Security
T&T Security — новая динамичная компания, занимающаяся кибербезопасностью. Более 8 лет мы успешно боремся с атаками класса APT, нулевого дня и целевым вредоносным ПО. Наши технологии эффективны там, где бессильны типичные средства защиты. Мы сотрудничаем с компаниями и государственными учреждениями, помогая им выявлять и предотвращать угрозы нового типа. Это позволяет оперативно выявлять и реагировать на атаки любого типа. Важным элементом нашей компании является вирусная лаборатория T&T Security VirLab. Мы первые в СНГ провели детальный анализ вредоносной программы WannaCry, суммарный ущерб от которой превысил 1 млрд долларов. VirLab преимущественно фокусируется на региональных угрозах (Республика Казахстан и Центральная Азия). www.tntsecure.kz