OUCH! Апрель 2023

SANS SECURITY AWARENESS

OUCH!

Ежемесячный информационный бюллетень по безопасности

Страшное ПО: история

Предупреждение! Ваш компьютер заражен программой-вымогателем Black Basta. Немедленно позвоните по этому номеру телефона, чтобы починить компьютер! - *Если бы вы увидели всплывающее окно с предупреждением на своем компьютере, вы бы позвонили по номеру телефона?*

Атака

После тридцати лет напряженной работы Дебора скопила достаточно денег, чтобы выйти на пенсию вместе с мужем. Желая проверить свои пенсионные счета, она ввела в браузер название своего банка. Чего она не осознавала, так это того, что она опечаталась в названии банка, что привело ее на другой веб-сайт, на котором сразу же появился предупреждающий баннер, в котором утверждалось, что ее компьютер заражен, и ей предлагалось немедленно позвонить в службу технической поддержки. Всплывающее предупреждение было очень профессиональным. В нем подробно описывалось, какое вредоносное ПО заразило ее компьютер, имелся официальный логотип компании и был указан номер службы экстренной помощи, по которому она могла позвонить.

Дебора немедленно позвонила по указанному номеру, на который ответил, казалось бы, профессиональный агент службы поддержки. Агент объяснил, что ее компьютер действительно был заражен и что им нужен доступ к ее компьютеру, чтобы исправить это. Ей нужно было посетить определенный веб-сайт, загрузить их защитное программное обеспечение, а затем установить его. Она выполнила просьбу, и агент службы поддержки сообщил ей, что у них есть доступ, после чего они начали исследовать ее компьютер.

Вскоре они подтвердили ее худшие опасения: не только компьютер был заражен, но и банковский счет был взломан. К счастью, у компании технической поддержки была прямая связь с ее банком, и они быстро перевели ее к агенту по мошенничеству. Агент по мошенничеству подтвердил, что ее учетная запись действительно была скомпрометирована и использовалась для перевода средств мошенническим путем. Они сказали ей немедленно перевести все свои деньги на другой банковский счет, чтобы защитить их. Дебора сделала, как было велено. Затем они сообщили ей, что ее пенсионный счет также был скомпрометирован. К счастью, у них также были партнерские отношения с государственным налоговым органом. Затем ее связали с правительственным агентом, который объяснил, что для обеспечения безопасности пенсионного счета ей нужно обналичить свои сбережения и перевести их на другой счет, прежде чем преступники смогут получить доступ ко всему этому. Она сделала это. Это была долгая и ужасно эмоциональная ночь, но Дебора была рада, что не только починила свой компьютер, но и сохранила все свои деньги, переведя их на новые безопасные счета. Она легла спать в изнеможении.

На следующее утро она вошла в свой новый банковский счет, чтобы получить доступ к своим недавно перемещенным сберегательным и пенсионным счетам, но все деньги исчезли. В панике она позвонила в техподдержку по вчерашнему номеру. Ответа не было. Вскоре она поняла, что все ее сбережения пропали. Она все это потеряла.

Как избежать того, чтобы это не случилось с вами?

Киберпреступники узнали, что самый простой способ заразить ваш компьютер или украсть ваши деньги — это просто спросить. Обычно они делают это с помощью пугающих программ, заставляя вас думать, что ваш компьютер заражен, хотя на самом деле это не так. Затем они подталкивают вас к поспешным действиям, чтобы воспользоваться вами. Эта история основана на реальных событиях, которые произошли с реальными людьми. Компьютер Деборы никогда не был заражен, вместо этого она случайно зашла не на тот сайт. Компания технической поддержки была не настоящей компанией, а командой киберпреступников, объехавших полмира. Даже банковское мошенничество и правительственные агенты были просто разными членами одной и той же команды киберпреступников. Как только киберпреступники позвонят вам по телефону, они сделают все возможное, чтобы забрать ваши деньги. Как защитить себя?

- Подозрение — лучшая защита. Каждый раз, когда кто-то пытается подтолкнуть вас к действию, это может быть нападением. Чем сильнее чувство срочности и чем больше на вас давят, тем больше вероятность, что это мошенничество.
- Ни одна законная компания никогда не попросит вас ввести пароль. Ни один банк не будет просить вас перевести деньги.
- Никогда не используйте контактную информацию, указанную в предупреждении или всплывающем окне. Если вы хотите проверить законность оповещения, всегда используйте уже известные вам способы связи, такие как номера телефонов в выписках по банковским счетам или кредитным картам, или используйте ссылки, добавленные в закладки в вашем браузере.

Если вы считаете, что вы или ваш близкий человек стали жертвой финансового мошенничества, немедленно сообщите об этом в правоохранительные органы и в свой банк. Чем раньше вы сообщите об этом, тем больше шансов, что вы сможете вернуть свои деньги.

Ресурсы

Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Браузеры: https://www.sans.org/newsletters/ouch/browsers/
Эмоциональные триггеры: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Фишинговые атаки становятся все более изощренными:
https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Роман Полаков