Приклади повідомлень про спроби підібрати паролі до сайтів

На діаграмі показана залежність кількості локаутів від IP-адрес, з яких здійснювали неправильне введення логіну чи пароля до сайту Система+. Взято останні 400 локаути з фільтром на три локаути і більше.

Нижче у списку подано 400 останніх локаутів, які виникали з причин введення користувачами неправильних логінів чи паролів до сайту “Система+” більше ніж 3 рази (деякі користвачі видалені, а логіни змінені):

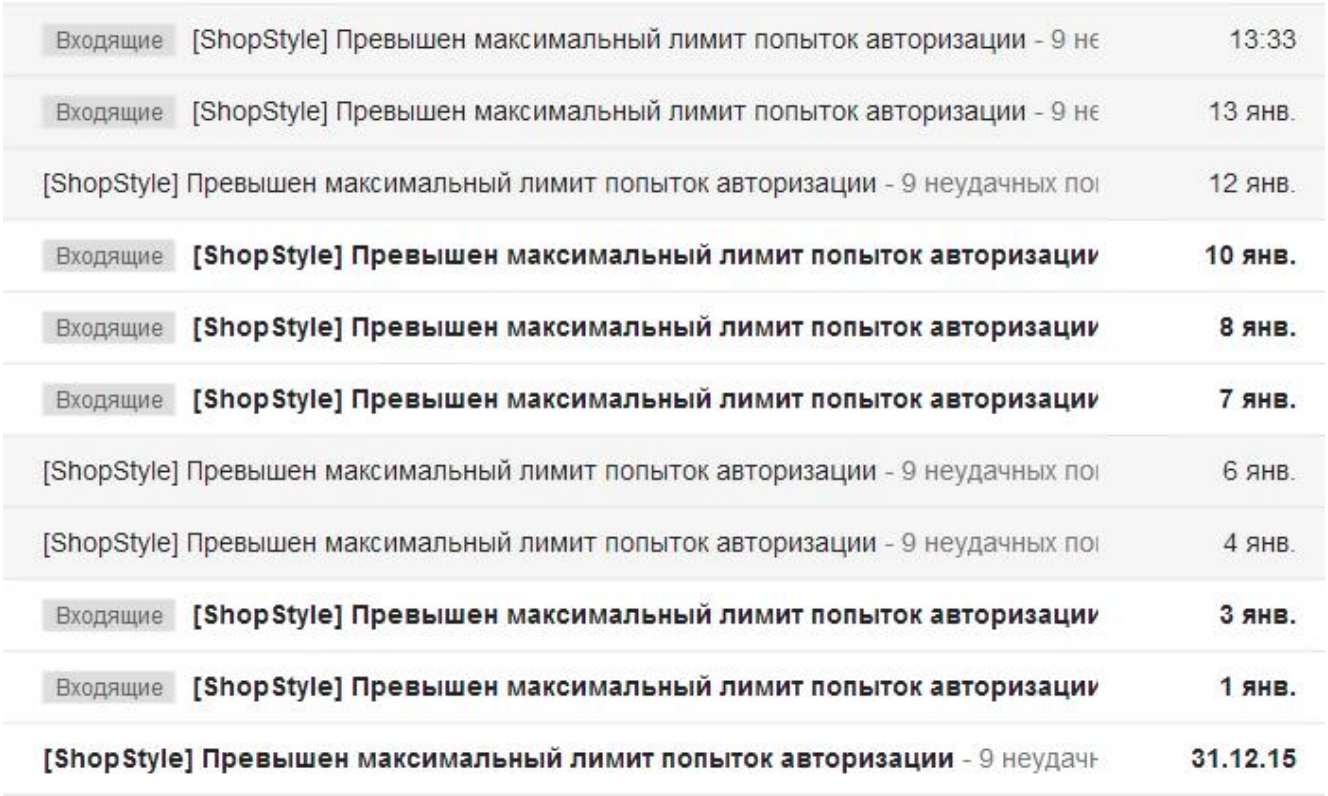
IP:212.111.197.130 system (1 lockout), …1 (1 lockout), Cepro (1 lockout), pro.artur9tko (2 lockouts)
IP:178.92.250.223
IP:211.110.140.155 volunteer (8 lockouts)

IP:74.220.207.143 dss-bi (4 lockouts)
IP:178.216.20.99 student (1 lockout)
IP:27.255.84.219 … (4 lockouts)
IP:37.115.141.53 120oX (2 lockouts)
IP:212.199.184.80 … (4 lockouts)
IP:195.211.155.156 … (13 lockouts)
IP:120.42.5.101 … (3 lockouts), admin (1 lockout)
IP:174.129.228.67 (13 lockouts)
IP:125.77.237.63 … (2 lockouts), admin (2 lockouts)
IP:125.77.232.217 … (2 lockouts), admin (2 lockouts)
IP:121.204.195.81 …1 (4 lockouts)
IP:37.115.83.78 120oX (1 lockout), …1 (1 lockout)
IP:110.89.41.6 …1 (4 lockouts)
IP:185.19.93.180 …1 (8 lockouts)
IP:72.43.201.2 …1 (12 lockouts)
IP:117.26.79.195 …1 (4 lockouts)
IP:117.26.118.220 … 1 (8 lockouts)
IP:176.215.128.60 …1 (20 lockouts)
IP:176.215.131.207 …1 (4 lockouts)
IP:176.215.165.229 …1 (12 lockouts)
IP:59.58.157.120 …1 (4 lockouts)
IP:110.89.41.161 …1 (4 lockouts)
IP:117.26.196.209 …1 (3 lockouts), admin (1 lockout)
IP:27.150.247.178 …1 (3 lockouts), admin (1 lockout)

IP:117.26.196.243 …1 (3 lockouts), admin (1 lockout)
IP:91.234.211.248 KinG (1 lockout)
IP:91.200.12.9 YdVBQouxxD (1 lockout)
IP:216.157.34.103 admin (1 lockout)
IP:104.171.2.78 …1 (1 lockout)
IP:216.70.80.22 …1 (1 lockout)
IP:46.235.14.93 …1 (2 lockouts)
IP:146.120.89.132 …1 (1 lockout)
IP:162.253.145.122 …1 (2 lockouts)
IP:46.4.68.239 …1 (1 lockout)
IP:23.253.56.96 …1 (1 lockout)
IP:37.57.231.111 …1 (2 lockouts)
IP:91.200.12.116 (2 lockouts)
IP:203.6.149.134 admin (3 lockouts)
IP:103.53.225.47 …1 (1 lockout)
IP:178.32.216.214 …1 (8 lockouts)
IP:91.200.12.49 nikita545 (4 lockouts)
IP:216.131.91.227 …1 (2 lockouts)
IP:37.73.221.242 sos123 (2 lockouts)
IP:91.200.12.86 nikita545 (6 lockouts), system1 (1 lockout)
IP:37.115.137.247 …1 (1 lockout)
IP:94.23.13.174 …1 (1 lockout)
IP:91.200.12.19 (2 lockouts)
IP:91.200.12.130 (3 lockouts)
IP:91.200.12.63 (2 lockouts)
IP:91.200.12.71 (2 lockouts)
IP:5.248.131.254 angelachek93@gmail.com (1 lockout)
IP:91.200.12.106 (29 lockouts)
IP:91.200.12.141 (28 lockouts)
IP:91.200.12.137 (35 lockouts), epovoqo (1 lockout)
IP:91.200.12.143 (33 lockouts)
IP:91.200.12.136 (18 lockouts)
IP:91.200.12.7 (19 lockouts)
IP:37.115.88.73 angelachek93@gmail.com (1 lockout)
IP:86.109.6.1 …1 (4 lockouts)
IP:185.22.185.223 …1 (2 lockouts)
IP:199.217.112.120 …1 (1 lockout)

IP:89.200.142.245 …1 (3 lockouts)
IP:71.6.151.130 …1 (4 lockouts)
IP:62.210.211.161 …1 (4 lockouts)
IP:188.165.229.190 …1 (2 lockouts)

Дане нижче зображення є фрагментом копії екрану електронної пошти адміністратора сайту і відображає узагальнені відомості про спроби підібрати пароль до навчального сайту ShopStyle.



Повідомлення на електронній пошті про спроби підібрати пароль до SiteLabe SLS ShopStyle

У деталізованій формі подані повідомлення відображають певну кількість параметрів порушників.

Деяких порушників легко ідентифікувати. Деякі порушники внесені до відповідних Web-баз даних спамерів понад 1000 раз.

Показана вище інформація про порушення у більш деталізованій формі автоматично відправляється на електронну адресу за межами хостингу та звідти автоматично відправляється ще на одну поштову скриньку – для резервування . Таким чином, вся інформація про порушення накопичується для подальшого науково-практичного аналізу за допомогою комплексу аналітичних засобів із взаємно дублючими і доповнюючими функціями.

У загальному випадку можна встановити більше 10-ти параметрів порушника, у т.ч. ключові параметри комп`ютера, основні програмні засоби, його географічні параметри за різними даними, з різною точністю, ін.

Сучасний Web, пошукові системи і їх доповнення, хостинги та сайти побудовані так, що, як правило, дозволяють за певний час встановити порушників за допомогою комплексу організаційних заходів і програмно-технічних засобів – при наявності бажання і необхідних грошових коштів. Це нічим не загрожує безпеці добросовісних відвідувачів і навіть допитливих користувачів, проте дозволяє встановити явно зловмині спроби підбору паролей, особливо з використанням спеціальних програм.

Всі сайти, як правило, резервуються в одному-двох місцях під потужних захистом. Тому, знищений чи пошкоджений сайт, як правило, може бути відновлений із втратою публікацій за одну-дві доби. Для прикладу, дві доби назад сайт “Система+” був знищений з вини адміністратора, проте був швидко відновлений за допомогою спеціалістів UAhosting.

Не варто руйнувати чужі web-системи, а краще спробувати побудувати свою конструктивну систему. Як правило, після таких спроб і апробації всіх реальних складнощів створення конструктивної вебсистеми, бажання руйнувати чиюсь систему пропадає. Це тим більш важливо, що хакери

працюють в інтернеті, часто мають свої інтернет-ресурси, які теж можуть бути атаковані і знищені чи пошкоджені – у відповідь на зловмисні дії їх власників. Є відоме російське прислів`я: “Ломать – не строить”.