



JBS LeakDB Report (KR)

Example.com



Joe Black Security (JBS) 법적 고지 사항

본 명세서에서 제공된 정보는 일반 정보와 교육 목적만을 위한 것입니다. 법적 조언을 구성하기 위해 의도된 것이 아니며 해석되어서는 안됩니다. 여기에 포함된 정보는 모든 상황에 적용되지 않을 수 있으며 가장 현재 상황을 반영하지 않을 수 있습니다. 여기에 포함 된 내용은 제시된 특정 사실과 상황에 근거한 법적 조언 없이 혜택에 의존하거나 행동해서는 안되며, 달리 해석해서는 안됩니다. JBS는 사전 통지 없이 언제든지 이 문서의 내용을 수정할 수 있는 권리를 보유합니다.

JBS와 관련된 단체 또는 개인과 관련된 모든 데이터는 어떤 식으로든 JBS와 관련이 없거나 연결되어 있지 않으며 공공 인터넷에서 발견되었으며, 따라서 공공 도메인으로 간주됩니다. JBS는 모든 조치를 취하여 전체 데이터를 보유한 엄격한 보안 통제를 유지하며 데이터의 원래 소유자의 동의 없이는 민감한 정보를 제3자에게 공개하지 않을 것입니다.

JBS는 정확한 최신 정보를 포함시키기 위해 합리적인 노력을 사용하지만, JBS는 정확성, 통화 또는 완전성에 대해 어떤 종류의 보증이나 표현도 하지 않습니다. 이 문서에 대한 접근과 사용, 그리고 그 내용에 의존하는 것이 당신의 위험에 처해 있다는 것에 동의합니다. JBS는 명시 적이든 묵시적이든 모든 종류의 보증을 부인합니다. JBS나 이 문서를 작성, 제작 또는 전달하는데 관여하는 당사자는 직접, 간접, 특수, 결과, 사업 이익의 손실 또는 특수 손해, 사용에 대한 접근, 사용 또는 사용 불가능, 또는 이 문서의 사용과 관련하여 발생하는 모든 결과, 손실 또는 손상에 대해 책임을 지지 않습니다. 이 정보의 사용은 "있는 그대로" 조건에서 사용하기 위한 수용을 구성합니다.

어떤 자료든 다른 언어로 번역하는 것은 단지 편의상 의도된 것입니다. 번역 정확성은 보장되지 않는다. 번역의 정확성과 관련하여 질문이 발생하면 문서의 원본 언어 공식 버전을 참조하십시오. 번역에서 발생하는 불일치나 차이는 구속력이 없으며 준수나 집행 목적에 대한 법적 효과가 없습니다.

이 문서는 매우 민감하고 기밀로 간주되어야 하는 데이터를 포함하고 있으며, 이에 따라 조직의 대표자가 처리해야 합니다.

Contents

JBS LeakDB.....	4
<i>JBS LeakDB 정보</i>	
<i>LeakDB가 왜 중요한가?</i>	
<i>다음 단계</i>	
비밀번호 분석 요약.....	5
<i>비밀번호 분석론 소개</i>	
<i>비밀번호 분석</i>	
유출된 데이터베이스 요약.....	7
<i>샘플 데이터</i>	
<i>JBS LeakDB 검색 결과</i>	

JBS LeakDB 정보

LeakDB는 고객 네트워크에 쉽게 침입할 수 있는 모의 해킹 공격팀 툴로 개발되었습니다. 데이터가 제공하는 통찰력은 몇 번이고 귀중한 것으로 입증되었으며 직원이 진정으로 가장 약한 연결 고리임을 입증했습니다.

평균 온라인 사용자는 20-25 개의 계정을 가지고 있습니다. 추적해야 할 계정이 너무 많기 때문에 잘못된 암호 습관과 암호 재사용이 심각한 문제가 됩니다. 직원의 회사 자격증이 제 3 자 사이트에서 유출되는 것을 알면 직원에 대한 적시에 불편한 비밀번호 재설정과 조직의 네트워크 무단 위반 간의 차이를 의미 할 수 있습니다.

수많은 사이트가 매일 침해 당하고 데이터베이스가 다크웹으로 유출되거나 심지어 공개 인터넷으로 직접 유출되기 때문에, 기본 기술을 가진 일반 사용자도 이 데이터의 사본을 찾아 다운로드 하는 것이 쉽지 않습니다. 즉, 직원들이 회사 이메일을 통해 어디에서 무엇을 하고 있는지 정확히 아는 것이 그 어느 때보다 중요합니다. 악의적인 공격자가 사용하기 전에 직원의 자격 증명을 공개적으로 포착하면 조직에 많은 시간과 비용을 절약할 수 있습니다.

LeakDB가 왜 당신에게 더 중요한가?

왜 이 중 어떤 것이 조직에 중요한가? 타사 사이트에서 유출된 데이터베이스가 귀사의 평균 조직과 무슨 관련이 있습니까? 답은 네 부분으로 나눌 수 있습니다:

무단 인증 액세스 / 암호 재사용

- 인증되지 않은 공격자가 일반적으로 조직의 네트워크에 액세스하려고 시도하는 것을 발견 할 수 있지만 인증 된 사용자와 인증되지 않은 인증되지 않은 인증된 공격자간에 구분하기가 상당히 어려울 수 있습니다. 유효한 자격 증명으로 액세스 권한을 얻었습니다.
- 매일 전 세계의 주요 및 소규모 조직에서 수많은 데이터베이스가 온라인으로 유출되고 있습니다. 일부는 뉴스를 만들기에는 충분하지만 일부는 너무 작지만 많은 사람들이 눈에 띄지 않습니다.
- 부정한 방식으로 사용자 계정에 액세스하기 위해 'Credential Stuffing' 또는 위반 된 사용자 이름 / 암호 쌍을 자동으로 주입하는 방법은 최근 유출 된 데이터가 대량으로 유입되어 비교적 새로운 유형의 공격입니다.
- 공격자들은 인터넷과 다크웹을 뒤져 현금 보석을 찾습니다. 조직과 관련된 모든 이메일이 인터넷에 노출된 로그인 양식에 대해 테스트되고 있음을 확신할 수 있습니다.
- 침입자가 네트워크에 무단으로 인증된 액세스 권한을 얻지 못하게 하는 유일한 방법은 침입자가 자격 증명을 사용하기 전에 유출된 자격 증명을 아는 것입니다.

비밀번호 알림(패턴) 및 습관 예측

- 직원 이메일과 관련된 자격 증명에 온라인으로 유출된 경우가 많으므로 회사 네트워크에 로그인 할 수 없습니다.
- 이로 인해 자격 증명에 없어질 수는 있지만, 전용 공격자는 유출된 자격 증명으로부터 많은 것을 배울 수 있습니다.
- 사용자가 다른 서비스를 위해 단일 숫자를 추가하거나 공통 암호로 숫자를 증가시키는 습관이 있는 경우.
- 이것은 비밀번호 패턴 예측으로 알려져 있으며, 이것이 직원의 습관이고 허가 받지 않은 인증된 액세스로 이어질 수 있는 경우 재앙일 수 있습니다.

사용자 습관과 오용 학습

- 조직에 대한 덜 알려져 있지만 여전히 관련 있는 위협은 직원이 회사 이메일을 사용하는 다른 서비스입니다.
- LinkedIn과 같은 일부 서비스는 일반적으로 허용되지만 이러한 서비스는 자체적인 위험을 수반합니다. 공격자가 제3자 사이트의 계정을 넘겨받아 그것을 이용하여 계정이 가지고 있는 신뢰를 악용하는 것과 같은 것입니다.
- 또한 직원들은 데이트나 음란 사이트와 같은 더 의심스러운 서비스에서도 자신이 좋아하는 모든 서비스에서 회사 이메일을 사용할 수 있다고 느낄 때가 있습니다. 절대로 이러면 안 됩니다.
- 회사 이메일은 회사 이메일이며, 회사 관련 서신에만 사용해야 합니다.

대량 피싱 캠페인

- 크고 작은 모든 조직에 대한 최종 위협은 대량 피싱 캠페인입니다.
- Exploit.IN 및 BreachComp와 같은 수백만 또는 수십억 개의 전자 메일이 포함 된 거대한 편집 목록이 유출되어 유출된 암호가 유효하지 않더라도 공격자는 이제 수많은 회사 전자 메일에 대해 피싱 캠페인을 수행할 풍부한 정보를 보유하게 됩니다.

다음 단계

- JBS는 독점 도구를 사용하여 외부에서 직면한 네트워크 리소스에 대해 유출된 자격 증명을 테스트 할 수 있습니다. 유효한 자격 증명에 발견되면 즉시 경고를 받고 JBS가 치료 계획을 지원합니다.
- 자체 내부 인증 시스템에 대해 테스트하기 위해 유출 된 자격 증명의 전체 목록을 얻습니다.
- JBS의 LeakDB 경고 서비스에 가입하고 조직의 새 자격 증명에 발견된 경고가 표시됩니다.
- 자세한 정보는 info@joe.black 으로 문의하십시오

Password Analytics Summary

비밀번호 분석 소개

도메인 Example.com의 전자 메일 주소는 129개의 데이터베이스 유출에 나타납니다.

텍스트 기반 암호는 전 세계 정보 시스템에서 사용되는 기본 사용자 인증 수단입니다. 이는 이 인증 메커니즘의 단순성과 저렴한 구현 때문입니다. 이러한 인증 방식이 문제가 되는 것은 사용자가 도입될 때입니다. 사용자가 하루에 여러 번 사용할 수 있는 서비스에 대해 복잡한 암호를 기억하고 사용하는 방식은 이러한 사용자가 더 간단한 암호를 선택하고 여러 사이트에서 암호를 재사용하는데 영향을 주는 경향이 있습니다. 이것은 조직의 네트워크와 같은 잠재적으로 중요한 시스템에 약한 암호를 도입하는 효과가 있습니다.

또한, 해커와 사이버 범죄 집단은 비밀번호의 선택에 있어 조직의 직원 습관을 이해하기 위해 유출된 데이터베이스로부터 패스워드를 연구함으로써 큰 이익을 얻습니다. 이것은 그들이 현재 유효한 암호를 찾을 가능성을 크게 증가시킵니다.

또한 이러한 유형의 데이터를 분석하면 조직이 직원의 암호 습관을 이해하고 비밀번호 복잡성 규칙을 선택할 때 이들을 돕고 직원에게 안전한 암호 관행에 대한 교육을 제공할 수 있습니다.

다음은 Example.com 도메인과 관련된 일반 텍스트 암호에 대한 간단한 분석입니다. 다음은 Example.com 도메인과 관련된 일반 텍스트 암호에 대한 간단한 분석입니다.

검색요약	도메인	총 이메일 수	일반 텍스트 암호*	해시 된 암호*	발견된 것
	Example.com	319,640	186,159	177,620	129 databases

* 일반 텍스트 비밀번호 및 해시 비밀번호는 유출된 데이터베이스에서 발견된 데이터 포인트 수를 기반으로 합니다. 어떤 경우에는 단일 데이터베이스에서 명확한 암호와 해시 된 암호를 모두 찾았지만 다른 암호는 찾지 못했습니다.

비밀번호 분석

Password Length Analysis

비밀번호 길이 분석

비밀번호 길이	퍼센트	전체
7	21.09 %	39884
8	19.76 %	37369
6	17.62 %	33314
9	13.97 %	26413
10	11.12 %	21036

암호 길이는 직원들이 일상적인 온라인 활동에 사용하는 보안 수준에 대한 빠른 지표입니다. 이것은 기업 환경에서 사용되는 클리어텍스트 암호의 길이에 대한 직접적인 표시는 아니지만, 많은 사용자들이 많은 온라인 계정에 '쓰레기 암호' 암호를 사용하는 경향이 있기 때문에, 공격자에게 그들이 직면할 수 있는 길이에 대한 일반적인 개요를 제공한다.

이 분석은 다중 유출에서 발견된 일반 텍스트 비밀번호에 대해 수행되었으며 타사 사이트에서 일반적으로 사용되는 상위 5 개의 비밀번호 길이를 보여줍니다.

Frequency Analysis

빈도 분석

조직과 관련된 유출된 계정에 특정 암호가 얼마나 자주 나타나는지 사용자의 습관에 대한 또 다른 지표입니다. 이러한 암호는 제3자 사이트에서 유출되기 때문에 자주 사용되는 단어는 공격자에게 데이터가 특정 조직에 속한다는 증거뿐만 아니라 일반적인 단어를 재사용하여 다른 누출에서 발견된 추가 해시를 해독하는데 도움이 되는 정보를 제공합니다. 이 분석은 조직 이름의 키워드를 사용하여 수행되었습니다.

비밀번호	횟수
91***61	11269
12**56	3161
123***789	2010
12*45	973
9-1***961	933

Advanced (Hashcat) Mask Analysis

고급 (Hashcat) 마스크 분석

고급 마스크	퍼센트	전체
?d?d?d?d?d?d?d	8.98 %	16989
?d?d?d?d?d?d	6.8 %	12854
?l?l?l?l?l?l?l	4.86 %	9185
?l?l?l?l?l?l	4.33 %	8180
?d?d?d?d?d?d?d?d	4.14 %	7831

마스크 분석은 클라스트 텍스트 암호를 사용하여 각 문자의 문자 집합에 대해 설정된 값을 적용합니다. 이 마스크는 더 이상 전체 문자 집합을 강제할 필요가 없고 대신 미리 정해진 문자 마스크에만 집중하기 때문에 해시 균열에 필요한 시간을 크게 단축시킵니다.

Mask values:
l: lower alpha
u: capfirst alpha
d: digit
s: special
a: all

Simple Mask Analysis

단순 마스크 분석

단순 마스크 분석은 고급 마스크와 비슷하지만 사용된 문자에만 초점을 맞춥니다.
암호 유출에 사용되는 문자의 분포를 더 명확하게 정의해 줍니다.

단순 마스크	퍼센트	전체
lower_alpha_num	39.76 %	75200
numeric	27.92 %	52800
lower_alpha	20.34 %	38464
lower_alpha_special	2.71 %	5116
lower_alpha_special_num	2.49 %	4705

Additional Findings:

부가적인 발견

다른 발견	횟수
유출된 암호의 총 수	257064
고유한 이메일 수: 암호 조합	186159
고유한 이메일 수	211272
9자 아래의 암호	41355
조직의 이름이 발견됨	1357 times
60개의 공통 비밀번호가 발견됨	9724 times
키보드 워킹이 발견됨	20 times
비밀번호에서 발견되는 일반적인 날짜	16 times

- 유출된 비밀번호의 총 개수는 공개 유출에서 발견된 모든 일반 텍스트 비밀번호의 개수입니다.

- 고유한 전자 메일의 총 수 : 모든 누출을 통한 암호 조합.

- LeakDB에서 이 도메인에 대해 발견된 고유한 이메일의 총 수

- 9 자 미만의 비밀번호는 최소 10 자 길이를 충족하지 않는 모든 일반 텍스트 비밀번호의 수입니다.

- 일반 텍스트 비밀번호의 어느 부분에서든 조직 이름이 발견된 시간.

- 가장 일반적인 60개의 암호와 몇 번 클리어 텍스트 암호가 일치하는지 카운트.

- 키보드 워킹은 키보드를 가로질러 예측 가능하거나 간단한 패턴으로 빠른 키 누름의 한 형태이다.

- 일반 텍스트 비밀번호에서 발견 된 날짜 수.

Leaked Database Summary

샘플 데이터:

아래는 유출 된 자격 증명 목록에서 수정되고 잘린 행 샘플입니다.


- * 보안상의 이유로 비밀번호가 수정되었습니다.
- * 최종 CSV는 수정되지 않은 추가 정보를 포함합니다.

Leak	연도	이메일	일반 텍스트 암호	해시 된 암호
Comp	2019	el*****in@example.com	sa****no	--
Comp	2019	j.*****er@example.com	93**67	--
Comp	2019	a**e@example.com	pr***e3	--
Mate1.com	2016	fs*****32@example.com	fsd*****...	--
Fling.com	2011	pf*****ib@example.com	fra****646	22d64c90c5e5b88435e2ad46be4b0...
MySpace	2008	lt*****er@example.com	ar****e1	19D07468CA8C0D626B2F4E4D1538E...
MySpace	2008	sa**em@example.com	emr****753	F98FF81D93E500AD7EB12D83293F9...
MySpace	2008	pl*****am@example.com	pe***77	A9F2901495418C76A4410D1531569...
iMesh.com	2013	ss*gs@example.com	aaa***aaa	a08b0c06465c3c2bac8f34f1473c7...
iMesh.com	2013	du*****99@example.com	51***32	--

JBS LeakDB 검색 결과:

JBS LeakDB에는 Example.com 도메인의 이메일이있는 129 개의 데이터베이스가 있습니다.
다음 목록은 각 데이터베이스 누출에 대한 세부 사항을 제공합니다:

- Legend:
- 유출된 연도: 웹 사이트가 해킹되었거나 데이터가 인터넷에 유출된 경우
 - 이메일 수: 각 누출에 포함 된 위의 도메인과 관련된 이메일 수
 - 검증?: 데이터가 유출 된 회사 또는 타사 연구원이 데이터를 검증 한 경우
 - 민감도?: 데이터가 데이트 또는 포르노 웹 사이트와 같은 민감한 출처에서 온 경우
 - 세부 정보: 위반 및 유출 된 데이터에 대한 특정 세부 정보입니다
 - 노출 된 데이터: 유출 된 데이터베이스에 필드 데이터가 포함되었음을 나타냅니다
 - -: 유출 된 데이터베이스에 해당 필드에 대한 데이터가 포함되지 않았음을 나타냅니다

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://armorgames.com/		2019		24		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	데이터 유출	--	--	--	데이터 유출	

In January 2019, the game portal website website Armor Games suffered a data breach. A total of 10.6 million email addresses were impacted by the breach which also exposed usernames, IP addresses, birthdays of administrator accounts and passwords stored as salted SHA-1 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.classickorea.co.kr/		2019		1		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.



This is a compilation of numerous untitled email:password leaks including giant lists like Colletion #1-#5, Breach Comp, Exploit.In, Anti Public, etc... Note: This list does not include data from many of the most popular free email services. If your org uses a free email service, contact us for a more detailed search.

Flash Revolution

In February 2016, the music-based rhythm game known as Flash Flash Revolution was hacked and 1.8M accounts were exposed. Along with email and IP addresses, the vBulletin forum also exposed salted MD5 password hashes.



In April 2019, the PDF management service Lumin PDF suffered a data breach. The breach wasn't publicly disclosed until September when 15.5M records of user data appeared for download on a popular hacking forum. The data had been left publicly exposed in a MongoDB instance after which Lumin PDF was allegedly been "contacted multiple times, but ignored all the queries". The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token.


stockX

In July 2019, the fashion and sneaker trading platform StockX suffered a data breach which was subsequently sold via a dark web marketplace. The exposed data included 6.8 million unique email addresses, names, physical addresses, purchases and passwords stored as salted MD5 hashes.


In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes.

Town of Salem


In December 2018, the Town of Salem website produced by BlankMediaGames suffered a data breach. The data contained 7.6M unique user email addresses alongside usernames, IP addresses, purchase histories and passwords stored as phpass hashes.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.cashcrate.com/			2018	277	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	데이터 유출	--	데이터 유출	--	--	--	데이터 유출


In June 2017, news broke that CashCrate had suffered a data breach exposing 6.8 million records. The breach of the cash-for-surveys site dated back to November 2016 and exposed names, physical addresses, email addresses and passwords stored in plain text for older accounts along with weak MD5 hashes for newer ones.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.chegg.com/			2018	373	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	데이터 유출	--	--	--	--	--	--


In April 2018, the textbook rental service Chegg suffered a data breach that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	http://www.desura.com/			2018	306	NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--


In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as Desura. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and cleartext passwords

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://dubsmash.com/			2018	5,325	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	데이터 유출	--	데이터 유출	--	--	--	--


In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.hautelook.com/			2018	209	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--

In mid-2018, the fashion shopping site HauteLook was among a raft of sites that were breached and their data then sold in early-2019. The data included over 28 million unique email addresses alongside names, genders, dates of birth and passwords stored as bcrypt hashes.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.morele.net/			2018	4	NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	데이터 유출	--	--	데이터 유출	--	--	--


In October 2018, the Polish e-commerce website Morele.net suffered a data breach. The incident exposed almost 2.5 million unique email addresses alongside phone numbers, names and passwords stored as md5crypt hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.myfitnesspal.com/		2018		765		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	


In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.shein.com		2018		421		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In June 2018, online fashion retailer SHEIN suffered a data breach. The company discovered the breach 2 months later in August then disclosed the incident another month after that. A total of 39 million unique email addresses were found in the breach alongside MD5 password hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://news.zing.vn/		2018		236		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	데이터 유출	데이터 유출	--	--	데이터 유출	


In April 2018, news broke of a massive data breach impacting the Vietnamese company known as VNG after data was discovered being traded on a popular hacking forum where it was extensively redistributed. The breach dated back to an incident in May of 2015 and included of over 163 million customers. The data in the breach contained a wide range of personal attributes including usernames, birth dates, genders and home addresses along with unsalted MD5 hashes and 25 million unique email addresses.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.51cto.com/		2017		7		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In 2013, 51cto, a Chinese social media site was hacked and over 2 million accounts were leaked to the internet.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://8tracks.com/		2017		100		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In June 2017, the online playlists service known as 8Tracks suffered a data breach which impacted 18 million accounts. In their disclosure, 8Tracks advised that "the vector for the attack was an employee's GitHub account, which was not secured using two-factor authentication". Salted SHA-1 password hashes for users who didn't sign up with either Google or Facebook authentication were also included.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.binweevils.com/		2017		4		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	--	--	--	--	데이터 유출	

In September 2014, the online game Bin Weevils suffered a data breach. net indicated that a more extensive set of personal attributes were impacted (comments there also suggest the data may have come from a later breach). Data matching that pattern was later provided to Have I been pwned by @akshayindia6 and included almost 1.3m unique email addresses, genders, ages and plain text passwords.



In May 2017, the education platform Edmodo was hacked resulting in the exposure of 77 million records comprised of over 43 million unique customer email addresses. The data was consequently published to a popular hacking forum and made freely available. The records in the breach included usernames, email addresses and bcrypt hashes of passwords.



This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

futoboom

In early 2018, a large dataset consisting of over 1400 individual databases was found online. This leak contained a file named `www.fotoboom.com.txt` consisting of email addresses and a combination of hashed and plaintext passwords. While the validity of this breach cannot be confirmed, many of the accounts had not been seen in previous data breaches.

futureshop
connecting you with #1 excellence.co.uk


This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

교차로

In early 2018, a large dataset consisting of over 1400 individual databases was found online. This leak contained a file named `lifetip.icross.co.kr.txt` consisting of email addresses and a combination of hashed and plaintext passwords. While the validity of this breach cannot be confirmed, many of the accounts had not been seen in previous data breaches.




This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.jobstreet.com/		2017		10		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	데이터 유출	데이터 유출	--	데이터 유출	데이터 유출	

In October 2017, the Malaysian website lowyat.net ran a story on a massive set of breached data affecting millions of Malaysians after someone posted it for sale on their forums. The data spanned multiple separate breaches including the JobStreet jobs website which contained almost 4 million unique email addresses. The dates in the breach indicate the incident occurred in March 2012. The data later appeared freely downloadable on a Tor hidden service and contained extensive information on job seekers includ

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.magazinedee.com/		2017		6		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	RiverCity		2017		69		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
--	데이터 유출	--	데이터 유출	--	--	--	데이터 유출	


In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.taringa.net		2017		14		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In September 2017, news broke that Taringa had suffered a data breach exposing 28 million records. Known as "The Latin American Reddit", Taringa's breach disclosure notice indicated the incident dated back to August that year. The exposed data included usernames, email addresses and weak MD5 hashes of passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.zomato.com/		2017		260		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In May 2017, the restaurant guide website Zomato was hacked resulting in the exposure of almost 17 million accounts. The data was consequently redistributed online and contains email addresses, usernames and salted MD5 hashes of passwords (the password hash was not present on all accounts).

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://17.media		2016		34		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	


In April 2016, customer data obtained from the streaming app known as "17" appeared listed for sale on a Tor hidden service marketplace. The data contained over 4 million unique email addresses along with IP addresses, usernames and passwords stored as unsalted MD5 hashes.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://en.cdprojektred.com/			2016	19	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--


In March 2016, Polish game developer CD Projekt RED suffered a data breach. The hack of their forum led to the exposure of almost 1.9 million accounts along with usernames, email addresses and salted SHA1 passwords.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://cfire.mail.ru/			2016	214	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--


In August 2016, the Russian gaming forum known as Cross Fire (or cfire.mail.ru) was hacked along with a number of other forums on the Russian mail provider, mail.ru. The vBulletin forum contained 12.8 million accounts including usernames, email addresses and passwords stored as salted MD5 hashes.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.clixsense.com/			2016	1	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	데이터 유출	데이터 유출	데이터 유출	--	--	--	데이터 유출


In September 2016, the paid-to-click site ClixSense suffered a data breach which exposed 2.4 million subscriber identities. The breached data was then posted online by the attackers who claimed it was a subset of a larger data breach totalling 6.6 million records. The leaked data was extensive and included names, physical, email and IP addresses, genders and birth dates, account balances and passwords stored as plain text.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.dailymotion.com/			2016	85,367	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--


In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	http://ddo.com/			2016	4	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	데이터 유출	--	--	--	--	데이터 유출


In April 2013, the interactive video game Dungeons & Dragons Online suffered a data breach that exposed almost 1.6M players' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and password hashes.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.dfb.de/			2016	27	NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--

This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.dlh.net/			2016	11	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	데이터 유출	데이터 유출	--	--	--	--	--


In July 2016, the gaming news site DLH.net suffered a data breach which exposed 3.3M subscriber identities. Along with the keys used to redeem and activate games on the Steam platform, the breach also resulted in the exposure of email addresses, birth dates and salted MD5 password hashes. The data was donated to Have I been pwned by data breach monitoring service Vigilante.pw.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.dropbox.com/			2016	1,833	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--


In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://elobuddy.net/			2016	2	NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	데이터 유출


This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://www.evony.com/			2016	2,632	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	데이터 유출


In June 2016, the online multiplayer game Evony was hacked and over 29 million unique accounts were exposed. The attack led to the exposure of usernames, email and IP addresses and MD5 hashes of passwords (without salt).

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	http://www.fashionfantasygame.com/			2016	133	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--


In late 2016, the fashion gaming website Fashion Fantasy Game suffered a data breach. The incident exposed 2.3 million unique user accounts and corresponding MD5 password hashes with no salt. The data was contributed to Have I been pwned courtesy of rip@creep.im.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://game-tuts.com/			2016	45	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	데이터 유출

Likely in early 2015, the video game website GameTuts suffered a data breach and over 2 million user accounts were exposed. The site later shut down in July 2016 but was identified as having been hosted on a vBulletin forum. The exposed data included usernames, email and IP addresses and salted MD5 hashes.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	http://forum.gamevn.com/			2016	3	NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	데이터 유출


This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스			유출된 연도	이메일 숫자	검증?	민감도?
	https://en.gamigo.com/			2016	67	YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address
데이터 유출	--	--	--	--	--	--	--


In March 2012, the German online game publisher Gamigo was hacked and more than 8 million accounts publicly leaked. The breach included email addresses and passwords stored as weak MD5 hashes with no salt.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.gfan.com/		2016		111		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	


In October 2016, data surfaced that was allegedly obtained from the Chinese website known as GFAN and contained 22.5M accounts.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.i-dressup.com/		2016		326		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In June 2016, the teen social site known as i-Dressup was hacked and over 2 million user accounts were exposed. At the time the hack was reported, the i-Dressup operators were not contactable and the underlying SQL injection flaw remained open, allegedly exposing a total of 5.5 million accounts. The breach included email addresses and passwords stored in plain text.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://forums.lbsg.net/		2016		1,319		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In January 2016, the Minecraft community known as Lifeboat was hacked and more than 7 million accounts leaked. Lifeboat knew of the incident for three months before the breach was made public but elected not to advise customers. The leaked data included usernames, email addresses and passwords stored as straight MD5 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://leet.cc/		2016		571		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	


In August 2016, the service for creating and running Pocket Minecraft edition servers known as Leet was reported as having suffered a data breach that impacted 6 million subscribers. The incident reported by Softpedia had allegedly taken place earlier in the year contained only 2 million subscribers. The data included usernames, email and IP addresses and SHA512 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.mangafox.me/		2016		16		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	--	--	--	--	데이터 유출	

In approximately July 2016, the manga website known as mangafox.me suffered a data breach. The vBulletin based forum exposed 1.3 million accounts including usernames, email and IP addresses, dates of birth and salted MD5 password hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.mate1.com/		2016		2,915		YES	YES
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	--	--	--	--	--	


In February 2016, the dating site mate1.com suffered a huge data breach resulting in the disclosure of over 27 million subscribers' information. The data included deeply personal information about their private lives including drug and alcohol habits, incomes levels and sexual fetishes as well as passwords stored in plain text.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://modbsolutions.com		2016		133		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
--	데이터 유출	데이터 유출	데이터 유출	--	--	--	데이터 유출	


In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.muzhiwan.com/		2016		227		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.nulled.to/		2016		10		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	--	--	--	--	데이터 유출	


In May 2016, the cracking community forum known as Nulled was hacked and 599k user accounts were leaked publicly. The compromised data included email and IP addresses, weak salted MD5 password hashes and hundreds of thousands of private messages between members.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.shadi.com/		2016		70		YES	YES
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	데이터 유출	데이터 유출	--	--	--	


In 2016 Shadi.com's Database was breached containing 2 million of their users information containing private information about their sexual lives or fantasies along with their addresses, names and email/passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://subagames.com/		2016		127		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In September 2016, SubaGames.com was hacked and 3,494,889 Users' account data was breached. The passwords in this database are in salted(hex) vB hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.youku.com/		2016		728		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In late 2016, the online Chinese video service Youku suffered a data breach. The incident exposed 92 million unique user accounts and corresponding MD5 password hashes. The data was contributed to Have I been pwned courtesy of rip@creep.im.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.000webhost.com/		2015		209		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	--	--	--	--	--	데이터 유출	


In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.ashleymadison.com/		2015		1,428		YES	YES
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	데이터 유출	데이터 유출	--	--	--	


In July 2015, the infidelity website Ashley Madison suffered a serious data breach. The attackers threatened Ashley Madison with the full disclosure of the breach unless the service was shut down. One month later, the database was dumped including more than 30M unique email addresses. This breach has been classed as "sensitive" and is not publicly searchable, although individuals may discover if they've been impacted by registering for notifications. Read about this approach in detail.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://bitcointalk.org/		2015		9		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	--	--	--	--	데이터 유출	


In May 2015, the Bitcoin forum Bitcoin Talk was hacked and over 500k unique email addresses were exposed. The attack led to the exposure of a raft of personal data including usernames, email and IP addresses, genders, birth dates, security questions and MD5 hashes of their answers plus hashes of the passwords themselves.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://butterflylabs.com		2015		2		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.daniweb.com/		2015		27		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	

In late 2015, the technology and social site DaniWeb suffered a data breach. The attack resulted in the disclosure of 1.1 million accounts including email and IP addresses which were also accompanied by salted MD5 hashes of passwords. However, DaniWeb have advised that "the breached password hashes and salts are incorrect" and that they have since switched to new infrastructure and software.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.gaadi.com/		2015		96		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	--	--	데이터 유출	--	--	데이터 유출	

In May 2015, the Indian motoring website known as Gaadi had 4.3 million records exposed in a data breach. The data contained usernames, email and IP addresses, genders, the city of users as well as passwords stored in both plain text and as MD5 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.gamerzplanet.net		2015		6		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	

In approximately October 2015, the online gaming forum known as Gamerzplanet was hacked and more than 1.2M accounts were exposed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

In late 2015, the online penpal site InterPals had their website hacked and 3.4 million accounts exposed. The compromised data included email addresses, geographical locations, birthdates and salted hashes of passwords.


In October 2015, the multiplayer game hacking website MPGH was hacked and 3.1 million user accounts disclosed. The vBulletin forum breach contained usernames, email addresses, IP addresses and salted hashes of passwords.

In October 2015, the Chinese site known as NetEase (located at 163.com) was reported as having suffered a data breach that impacted hundreds of millions of subscribers. The data in the breach contains email addresses and plain text passwords.


In late 2015, the anime community known as Nihonomaru had their vBulletin forum hacked and 1.7 million accounts exposed. The compromised data included email and IP addresses, usernames and salted hashes of passwords.

In late 2015, the gaming website R2Games was hacked and more than 2.1M personal records disclosed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked. A further 11M accounts were added to "Have I been pwned" in March 2016 and another 9M in July 2016 bringing the total to over 22M.


In November 2015, the online chatroom known as "xat" was hacked and 6 million user accounts were exposed. Used as a chat engine on websites, the leaked data included usernames, email and IP addresses along with hashed passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://bitly.com/		2014		85		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://boards.cannabis.com/		2014		18		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	--	--	--	--	데이터 유출	

In February 2014, the vBulletin forum for the Marijuana site cannabis.com was breached and leaked publicly.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.couponmom.com/		2014		258		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In 2014, a file allegedly containing data hacked from Coupon Mom was created and included 11 million email addresses and plain text passwords. On further investigation, the file was also found to contain data indicating it had been sourced from Armor Games.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.diet.com/		2014		36		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	--	--	--	--	데이터 유출	


In August 2014, the diet and nutrition website diet.com suffered a data breach resulting in the exposure of 1.4 million unique user records dating back as far as 2004. The data contained email and IP addresses, usernames, plain text passwords and dietary information about the site members including eating habits, BMI and birth date. The site was previously reported as compromised on the Vigilante.pw breached database directory.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.forbes.com/		2014		1		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In February 2014, the Forbes website succumbed to an attack that leaked over 1 million user accounts. The attack was attributed to the Syrian Electronic Army, allegedly as retribution for a perceived "Hate of Syria". The attack not only leaked user credentials, but also resulted in the posting of fake news stories to forbes.com.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://habbo.st/		2014		9		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.hiapk.com/		2014		114		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In approximately 2014, it's alleged that the Chinese Android store known as HIAPK suffered a data breach that impacted 13.8 million unique subscribers. The data in the breach contains usernames, email addresses and salted MD5 password hashes

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.kickstarter.com/		2014		1		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.klerk.ru/		2014		2		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.tgbus.com/		2014		227		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In approximately 2017, it's alleged that the Chinese gaming site known as TGBUS suffered a data breach that impacted over 10 million unique subscribers.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.adobe.com/		2013		4,306		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.ahashare.com		2013		1		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	--	--	--	--	데이터 유출	


In May 2013, the torrent site AhaShare.com suffered a breach which resulted in more than 180k user accounts being published publicly. The breach included a raft of personal information on registered users plus despite assertions of not distributing personally identifiable information, the site also leaked the IP addresses used by the registered identities.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://badoo.com/		2013		13,944		NO	YES
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	--	--	--	--	--	


In June 2016, a data breach allegedly originating from the social website Badoo was found to be circulating amongst traders. Likely obtained several years earlier, the data contained 112 million unique email addresses with personal data including names, birthdates and passwords stored as MD5 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://imesh.com		2013		13,383		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	

In September 2013, the media and file sharing client known as iMesh was hacked and approximately 50M accounts were exposed. The data was later put up for sale on a dark market website in mid-2016 and included email and IP addresses, usernames and salted MD5 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.neopets.com/		2013		2,032		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	데이터 유출	--	--	--	--	데이터 유출	


In May 2016, a set of breached data originating from the virtual pet website "Neopets" was found being traded online. Allegedly hacked "several years earlier", the data contains sensitive personal information including birthdates, genders and names as well as almost 27 million unique email addresses. Passwords were stored in plain text and IP addresses were also present in the breach.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.nexusmods.com/		2013		14		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	


In December 2015, the game modding site Nexus Mods released a statement notifying users that they had been hacked. They subsequently dated the hack as having occurred in July 2013 although there is evidence to suggest the data was being traded months in advance of that. The breach contained usernames, email addresses and passwords stored as a salted hashes.

tumblr.	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.tumblr.com/		2013		787		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://vk.com/		2013		3,701		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	--	--	데이터 유출	--	--	--	


In approximately 2012, the Russian social media site known as VK was hacked and almost 100 million accounts were exposed. The data emerged in June 2016 where it was being sold via a dark market website and included names, phone numbers email addresses and plain text passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://weheartit.com/		2013		215		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In November 2013, the image-based social network We Heart It suffered a data breach. The data contained user names, email addresses and password hashes, 80% of which were salted SHA-256 with the remainder being MD5 with no salt.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.212300.com/		2012		7		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	데이터 유출	

This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://disqus.com/		2012		12,882		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In October 2017, the blog commenting service Disqus announced they'd suffered a data breach. The breach dated back to July 2012 but wasn't identified until years later when the data finally surfaced. The breach contained over 17.5 million unique email addresses and usernames. Users who created logins on Disqus had salted SHA1 hashes of passwords whilst users who logged in via social providers only had references to those accounts.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.last.fm/		2012		455		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.linkedin.com/		2012		806		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://renren.com/		2012		81		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In December 2011 a database breach affecting renren.com leaked 4.7 million user records including email addresses and plaintext passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.taobao.com/		2012		211		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In approximately 2012, it's alleged that the Chinese shopping site known as Taobao suffered a data breach that impacted over 21 million subscribers. The data in the breach contains email addresses and plain text passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.17173.com/		2011		320		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In late 2011, a series of data breaches in China affected up to 100 million users, including 7.5 million from the gaming site known as 17173.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.52pk.com/		2011		211		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as 52pk. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains usernames, email addresses and cleartext passwords

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.7k7k.com/		2011		89		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In approximately 2011, it's alleged that the Chinese gaming site known as 7k7k suffered a data breach that impacted 9.1 million subscribers. The data in the breach contains usernames, email addresses and plain text passwords.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.aipai.com/		2011		47		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In September 2016, data allegedly obtained from the Chinese gaming website known as Aipai.com and containing 6.5M accounts was leaked online. The data in the breach contains email addresses and MD5 password hashes.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://androidforums.com/		2011		2		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	--	--	--	--	데이터 유출	


In October 2011, the Android Forums website was hacked and 745k user accounts were subsequently leaked publicly. The compromised data included email addresses, user birth dates and passwords stored as a salted MD5 hash.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.csdn.net/		2011		10		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

One of the biggest programming communities in China, leaked 6M user data. A text file with 6M CSDN user info: user name, password, emails, all in clear text, was found on the internet.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://dodoneu.com/		2011		591		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
--	--	--	--	--	--	--	--	


In late 2011, data was allegedly obtained from the Chinese website known as Dodoneu.com and contained 8.7M accounts. The data in the breach contains email addresses and user names.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.fling.com/		2011		3,058		YES	YES
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	--	데이터 유출	--	--	데이터 유출	

In 2011, the self-proclaimed "World's Best Adult Social Network" website known as Fling was hacked and more than 40 million accounts obtained by the attacker. The breached data included highly sensitive personal attributes such as sexual orientation and sexual interests as well as email addresses and passwords stored in plain text.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://houdao.com/		2011		97		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

This database leak was found being spread on a cleartext 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.mop.com/		2011		62		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as Mop. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and cleartext passwords

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.pconline.com.cn/		2011		102		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

This database leak was found being spread on a cleartnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.stratfor.com/		2011		40		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	데이터 유출	--	데이터 유출	데이터 유출	데이터 유출	--	--	

In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.tianya.cn/		2011		426		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
--	데이터 유출	--	--	--	--	--	--	


In December 2011, China's largest online forum known as Tianya was hacked and tens of millions of accounts were obtained by the attacker. The leaked data included names, usernames and email addresses.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.uuu9.com/		2011		515		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In September 2016, data was allegedly obtained from the Chinese website known as uuu9.com and contained 7.5M accounts. The data in the breach contains email addresses and user names.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.weibo.com/		2011		75		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as Weibo. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and cleartext passwords

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.zoosk.com/		2011		2,716		NO	YES
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In approximately 2011, an alleged breach of the dating website Zoosk began circulating. Comprised of almost 53 million records, the data contained email addresses and plain text passwords. However, during extensive verification in May 2016 no evidence could be found that the data was indeed sourced from the dating service. This breach has consequently been flagged as fabricated; it's highly unlikely the data was sourced from Zoosk.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.hacker.co.kr/		2010		2		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	


In early 2010, the popular computer hardware market Hacker.co.kr was breached. Its not known who was the responsible party that leaked the stolen database. Due to its age and the fact that the site no longer exists, its not possible to verify the data.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://moneybookers.com		2009		35		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
--	데이터 유출	데이터 유출	데이터 유출	데이터 유출	--	--	데이터 유출	


Sometime in 2009, the e-wallet service known as Money Bookers suffered a data breach which exposed almost 4.5M customers. Now called Skrill, the breach was not discovered until October 2015 and included names, email addresses, home addresses and IP addresses.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://myspace.com/		2008		26,198		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://www.gpotato.com/		2007		79		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	데이터 유출	데이터 유출	--	--	--	데이터 유출	

In July 2007, the multiplayer game portal known as gPotato (link to archive of the site at that time) suffered a data breach and over 2 million user accounts were exposed. The site later merged into the Webzen portal where the original accounts still exist today. The exposed data included usernames, email and IP addresses, MD5 hashes and personal attributes such as gender, birth date, physical address and security questions and answers stored in plain text.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	https://www.2games.com/		unkn		191		NO	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

In 2017, a leak from Bizbilla.com surfaced on the clear net. Originally with passwords in MD5 format, they were quickly cracked, and a plaintext version began circling.


This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.


In early 2018, a large dataset consisting of over 1400 individual databases was found online. This leak contained a file named `lavoraconnoi.eurionics.it.txt` consisting of email addresses and a combination of hashed and plaintext passwords. While the validity of this breach cannot be confirmed, many of the accounts had not been seen in previous data breaches.


This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.


This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?		민감도?	
	https://mmgp.ru/		unkn		1		NO		NO	
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address			
데이터 유출	--	--	--	--	--	--	--			
This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.										

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?	민감도?
	http://pubpit.com/		unkn		5		YES	NO
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address	
데이터 유출	--	--	--	--	--	--	--	
This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.								

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?		민감도?	
	https://www.readnovel.com/		unkn		981		NO		NO	
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address			
데이터 유출	--	--	--	--	--	--	--			
This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.										

	유출된 웹사이트 / 서비스		유출된 연도		이메일 숫자		검증?		민감도?	
	https://twitter.com/		unkn		171		NO		NO	
비밀번호	이름 / 성	생년월일	주소	전화번호	신용카드	SSN	IP Address			
데이터 유출	--	--	--	--	--	--	--			
This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.										

자세한 정보는 info@joe.black 으로 문의하십시오