Adobe Data Breach of 2019

Student: Nedim Bandžović
Professor: Adnan Miljković
Course: Secure Software System Development

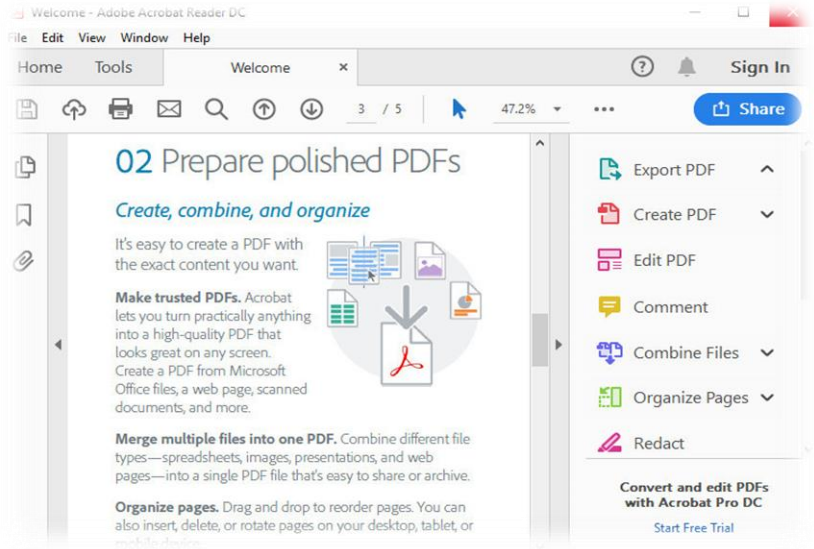
Adobe Creative Cloud

- provides apps, web services and resources for photography, graphic design, video editing, UX design, social media etc;

- in 2019, it was assumed that the Adobe Creative Cloud had approximately 15 million subscribers;

- initially released on July 17th, 2013.

- most famous apps of the Adobe Creative Cloud are Acrobat, After Effects, Photoshop, Illustrator, Premiere Pro etc.



The breach

- on October 19th, 2019, security researcher Bob Diachenko discovered an unsecured Elasticsearch database which belonged to Adobe Creative Cloud.

- Bob Diachenko, together with security firm Comparitech, search for unsecured databases via the Internet and later reports the issue to the databases's owner.

- the Adobe Creative Cloud database could be accessed by anyone easily because it did not require any kind of authentication or password.

Bob Diachenko

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	.kibana_task_manager	ZCxr	1	1	2	0	59.7kb	29.8kb
green	open	[redacted]	NTq4	1	2	7465549	1664215	85.9gb	17.5gb
green	open	.monitoring-es-7-2019.10.16	Jesc	1	1	138327	172740	201.6mb	101.8mb
green	open	.monitoring-es-7-2019.10.17	n5W5	1	1	155642	208496	240.2mb	119.9mb
green	open	.monitoring-es-7-2019.10.15	UbN_	1	1	91728	98162	105.6mb	52.9mb
green	open	.kibana_1	Etva	1	1	8	0	171.5kb	85.7kb
green	open	.monitoring-es-7-2019.10.18	bRas	1	1	172761	242227	261mb	129.7mb
green	open	.monitoring-es-7-2019.10.19	F4jI	1	1	62633	93786	162.7mb	72.7mb
green	open	.monitoring-kibana-7-2019.10.15	Rocn	1	1	7062	0	4mb	1.9mb
green	open	.security-7	gb3e	1	1	44	10	188.2kb	94.1kb
green	open	.monitoring-logstash-7-2019.10.16	Dgn9	1	1	188972	0	21mb	10.5mb
green	open	.monitoring-logstash-7-2019.10.15	R0-k	1	1	177951	0	20.4mb	10.2mb
green	open	.monitoring-kibana-7-2019.10.19	ZmWE	1	1	196	0	1.9mb	1010.8kb
green	open	.monitoring-kibana-7-2019.10.18	iNg5	1	1	8639	0	4.9mb	2.5mb
green	open	.monitoring-kibana-7-2019.10.17	OTBT	1	1	8639	0	5mb	2.5mb
green	open	.monitoring-kibana-7-2019.10.16	iF-6	1	1	8666	0	5.3mb	2.6mb

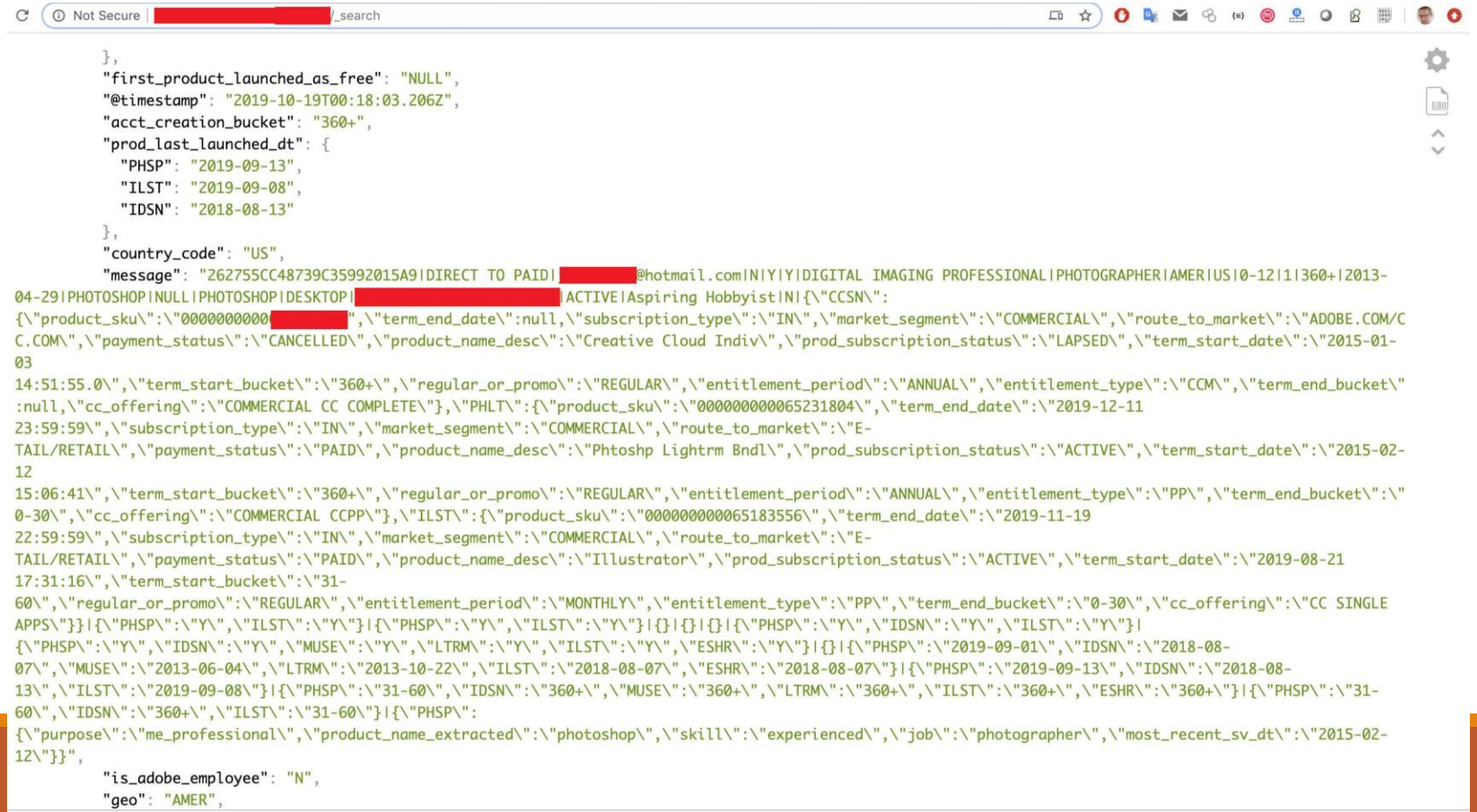
Exposed data

- nearly 7.5 million user records were exposed publicly;

- data which was exposed included email addresses of the user, creation date of the account, Adobe products which the user subscribed to, subscription status, member IDs, user's country, last login time and payment status;

- the data also contained information whether the account belongs to an ordinary user or to an Adobe employee;

- the database did not contain user's real names and surnames, passwords and payment information.



For how long the breach was active?

- Diachenko notified Adobe on the same day when the database was discovered (October 19th, 2019);

- shortly after Diachenko's warning, Adobe secured the database on the same day;

- when it comes to the start of the breach, the precise date is not known. Diachenko however believes that the database was available to the public for about a week.

At Adobe, we believe transparency with our customers is important. As such, we wanted to share a security update.
Late last week, Adobe became aware of a vulnerability related to work on one of our prototype environments.
We promptly shut down the misconfigured environment, addressing the vulnerability.
The environment contained Creative Cloud customer information, including e-mail addresses, but did not include any passwords or financial information.
This issue was not connected to, nor did it affect, the operation of any Adobe core products or services.
We are reviewing our development processes to help prevent a similar issue occurring in the future.

Official statement made by Adobe shortly after the database was secured, October 25th, 2019.

Consequences

- Adobe was praised by Diachenko and many users for their immediate reaction;

- the breach was not severe because it did not expose crucial user information (passwords, payment information);

- even though banking information was not exposed, many companies warned users to check for unusual activity on their bank accounts and to report them;

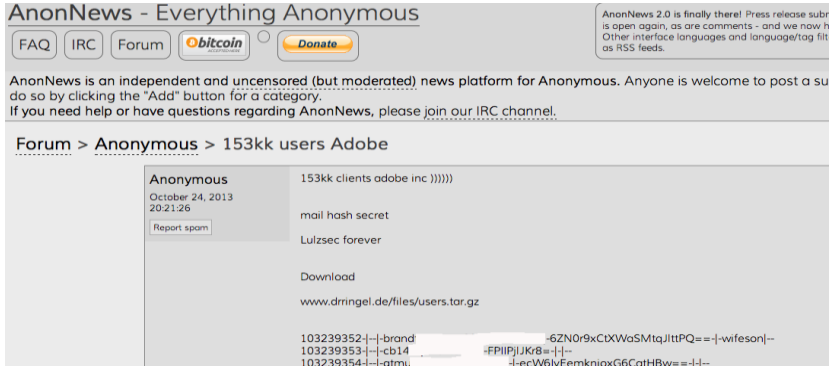
- it is not known if the database had been accessed by someone else besides Diachenko. For this purpose, users were warned that there is a high risk of receiving phishing mails due to the fact that user e-mails were exposed during the breach.

Prevention

- Adobe admitted that one of their prototype environments had an vulnerability which later brought the 2019 breach;

- the company acknowledged the vulnerability and later changed the development processes and increased monitoring of their prototype environments so these breaches do not occur again;

- Adobe has experience with data breaches because in 2013, the company suffered a major data breach which exposed credit card and login information for an unknown number of users and had affected 38 million Adobe users. The company was also fined for 1 million dollars.



Published encrypted passwords of Adobe users on an Anonymous forum in 2013.

THANKS FOR ATTENTION!