Massive trading of stolen data

Threat Memo - Date: 12/05/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime	Data exposure	World	Digital services Personal data	A1

Key Points

- At least 11 digital services companies affected by several breaches in the previous period, now see their databases sold on the darknet.
- A single cybercriminal actor is claiming to be in possession of all the data.
- Microsoft GitHub account was highly likely also breached by the same threat actor.

Summary

A previously unknown cybercrime threat actor has been releasing data stolen from numerous organisations, trading it in underground marketplaces. According to open sources[1] since May 3, there has been a number of high profile data breach and exposure cases all over the world. As discovered by news media a specific threat actor going by the name Shiny Hunters is claiming to be in possession of all the data allegedly stolen in the incidents and is offering it for sale at darknet locations.

Exposure of data due to accidental misconfigurations or threat actor activity is quite prevalent. Characteristically, on May 11, personal data of 3.6 million users of the Android dating app MobiFriends was being sold on the darknet, on May 9 the US Marshal service accidentally exposed information on prisoners, and on May 8 the operators of the Revil ransomware threatened to expose celebrity legal documents as part of their extortion tactic (see also TM 20-005).

In the case discussed however, the stolen databases come from different companies, all over the world, offering digital services across several sectors, including e-commerce, photo print services, wellbeing, education, etc. In total 11 companies have been affected (for a full list, please see the Annex) and the data stolen appears to be user record information that includes names and emails, as well as other private information. The number of records in each database range between 1 million and 91 million while the average price asked for each database is around €2500.

Most prominently, there was a report on May 6 that the Github account of Microsoft had been breached, and the contents of the repositories had been acquired (more than 500GB). Although the publicised parts appear to be from non-critical projects they could nevertheless expose significant code segments and most importantly compromise the credentials developers are using to access the repositories. The threat actor has contacted news media himself with repository samples and is pledging to give away the database free. Microsoft sources have later confirmed the breach, which probably occurred on March 28, 2020, as legitimate.

Comments

As in all such cases except the immediate effects of personal data publication there is a possibility of cascading dangers from user password reuse across services. There is also the possibility of abuse of personal information available to cyber actors to create highly personalised phishing emails.

Personnel of EU institutions, bodies and agencies (EU-I) are advised to check the list of the affected companies and change their passwords in case they had in the past registered in any of them. As a rule, use of professional emails for registration to commercial digital services should be avoided. As part of its regular services, CERT-EU is using third party services to scrutinize some well-known web locations used in publication of stolen documents, for possible email/password leaks for emails belonging the EU-I's subdomains (e.g. europa.eu). Affected EU-I are duly informed in case of compromise.

[1] https://www.bleepingcomputer.com/news/security/hacker-group-floods-dark-web-with-data-stolen-from-11-companies/

Annex: Affected companies

Company name	Sector	Country	Number of records stolen	Asking price
Tokopedia	e-commerce	Indonesia	91 million	approx. €4.600
Homechef	food services	US	8 million	approx. €2.300
Bhinneka	e-Commerce, internet services	Indonesia	1,2 million	approx. €1.100
Minted	online marketplace for art and design	US	5 million	approx. €2.300
Styleshare	mobile platform for fashion	South Korea	6 million	approx. €2.500
Ggumim	mobile platform for furniture	South Korea	2 million	approx. €1.200
Mindful	wellbeing NGO	US	2 million	approx. €1.200
StarTribune	newspaper	US	1 million	approx. €1.000
ChatBooks	photo printing service	US	15 million	approx. €3.200
The Chronicle Of Higher Education	newspaper	US	3 million	approx. €1.400
Unacademy	education	India	22 milion	approx. €1.800