InfoArmor

InfoArmor reports identification numbers of **120 million Brazilians** exposed online

infoarmor.com

Earlier this year, the InfoArmor research team discovered an unsecured server hosting the taxpayer registry identification numbers for 120 million Brazilian nationals, representing another stunning example of relaxed cybersecurity practices putting hundreds of millions of people at risk.

In March of 2018, the InfoArmor Advanced Threat Intelligence team discovered an open http server during regular internet scanning for compromised machines, building of IP reputations, and threat actor activity. The misconfigured, publicly accessible server contained 120 million unique Cadastro de Pessoas Físicas (CPFs). CPFs are an identification number issued by the Brazilian Federal Reserve to Brazilian citizens and tax-paying resident aliens, and each exposed CFP linked to an individual's banks, loans, repayments, credit and debit history, voting history, full name, emails, residential addresses, phone numbers, date of birth, family contacts, employment, voting registration numbers, contract numbers, and contract amounts.

Unfortunately, it is not uncommon for InfoArmor's research team to regularly encounter leaked data in unsecured S3 buckets and misconfigured servers, publicly revealing information intended to be private. "With the mad rush to share tenant cloud services, we are seeing a tremendous amount of leaked data that is potentially 10 times greater than actual threat actor activity," says Christian Lees, chief intelligence officer at InfoArmor.

It is important to note that this discovery is not a hack or breach — the information was freely accessible to anyone who happened to be looking. That being said, this was an extensive list of readily-available, highly personal, and valuable information for about 57 percent of Brazil's population, and it is very likely sophisticated adversaries harvested this information. It took over a year for data stolen from Yahoo to appear for sale on the dark web, and data as unique as what was available in Brazil's CPF server is likely to be traded among the most closed off and exotic data troves of the dark web. For this reason, InfoArmor's team is closely monitoring for any emergence of this data and is hoping to make people aware that their information could be at risk.

Process of Discovery and Notification

Upon closer examination of the server that was discovered by InfoArmor's researchers, it was found that someone had renamed the "index.html" to "index.html_bkp," revealing the directory's contents to the world. Anyone who knew the filename or navigated to it would have unfettered access to all the folders and files within. The links pictured in the "Index" screenshot show the database files open and available for download. A screenshot of the table for just the "aero_20180322.tar.gz" file shows how much information was available in the open directory.

Index of /

[ICO]	Name	Last modified	Size
[ ]	aero_20180322.tar.gz	2018-03-22 13:45	27M
[ ]	correcoes_20180322.tar.gz	2018-03-22 20:36	6.2G
[ ]	index.html_bkp	2018-03-05 22:40	11K
[ ]	infophp.php	2018-03-05 22:42	20
[ ]	inss_20180322.tar.gz	2018-03-22 19:17	17G
[ ]	mex_20180322.tar.gz	2018-03-22 13:49	50M
[ ]	siape_20180322.tar.gz	2018-03-22 14:08	643M
[ ]	telefonia.tar.gz	2018-03-14 16:53	78G

Apache/2.4.27 (Ubuntu) Server at 5.189.131.159 Port 80

ame	Engine	Version	Row Format	Rows	Avg Row Length	Data Length
cpf_temp	InnoDB	10	Compact	2984514	33	94.7 MiB
dados_emprestimo	MyISAM	10	Dynamic	146540	38	5.4 MiB
dados_endereco	MyISAM	10	Dynamic	57015	88	4.8 MiB
dados_militares	MyISAM	10	Dynamic	80409	30	2.4 MiB
dados_pessoais	MyISAM	10	Dynamic	80409	63	4.9 MiB
dados_pessoais2	MyISAM	10	Dynamic	0	0	0.0 bytes
dados_telefone	MyISAM	10	Dynamic	110744	36	3.9 MiB
total	MyISAM	10	Dynamic	160626	154	23.6 MiB

Two simple security measures could have prevented this: not renaming the main index.html file or prohibiting access through .htaccess configuration. Neither of these basic cybersecurity measures were in place.

In the days following the initial discovery, InfoArmor's research team attempted to determine who owned the server so they could be notified. During this time, InfoArmor observed that one of the files, an 82 GB file, had been replaced by a raw .sql file 25 GB in size, though its filename remained the same. This swap suggests a human intervened. It is possible that a server administrator had discovered the leak, however the server remained unsecured for weeks after this swap.

Further research revealed this new file host had a different IP address than the previous one, which created confusion as to the server's owner and who our team should notify of the leak.

In April 2018, InfoArmor researchers attempted to contact one of the email addresses registered to one of the hosts of the SQL. However, the email bounced and returned to us with "user unknown." After two more attempts to contact database hosts, we received a reply that they had notified their customers about the legal issues of leaving such data exposed, yet the data remained exposed online for several weeks thereafter.

For weeks, InfoArmor attempted to notify the owners. The team watched the open directory, and saw the files grow larger and smaller, as if users were just working with them in the open.

Later that month, the server had been fixed to secure the data. What was originally misconfigured to be accessible by IP address was reconfigured as a functional website with an authenticated alibabaconsultas.com domain that redirected to its login panel. Although InfoArmor cannot be sure that alibabaconsultas.com was responsible for the leak, it appears they were somehow involved, likely in a hosting-as-a-service function.

The Future of This Data

This exposure has revealed data sets as large as the 2017 Equifax breach. Brazil's population is roughly 211 million people, and millions of Brazilians live abroad — 426,000 of them in the U.S. An estimated 70,000 Americans live in Brazil. Because a CPF is available to anyone, there is presumably a wide swath of Brazilian nationals and foreign nationals who could have their information exposed in this database.

It is safe to assume that any intelligence organization or cybercrime group with reasonable collection capabilities and expertise will have captured this data. This data could very likely be used against the population of Brazil, the nation of Brazil, or any nations hosting people who have a CFP.

In a globalized world where countries do considerable amounts of business, travel, and trade with each other, this oversight could be a vehicle for serious misrepresentation. For example, an advanced cyber ring or malicious nation state with the ability to make it appear as if Brazil were attacking, say, the U.S. when the attack was in fact driven by another country.

There are also implications for every individual in this database. With voting records, debts, bank accounts, and the like exposed to the world's savviest cyber communities, the identities of these individuals are at greater risk to be sold and traded in the underground economy. Although as of the writing of this article there are no signs of this data on the dark web or elsewhere, there have been several cases in which threat actors have stockpiled data and eventually leaked or sold the massive collections much later.

This is an alarming problem that organizations all over the world face at all levels — a problem which is likely to continue to grow in scope, instance, and complexity. Such sensitive data being repeatedly and carelessly exposed on such a large scale is a threat to citizens in every country and a substantial boon to threat actors, hackers, and cybercriminals.

When major breaches happen, it is easy to point the finger of blame at a large organization that should "know better." But it must be acknowledged that in most cases, we are our own worst enemy. Whether we mean to or not, disregarding basic cybersecurity practices makes the work of hackers substantially easier and, in the end, we are all affected.