CybelAngel

WHITEPAPER

Internet Connected Storage: The New Cybersecurity Blind Spot

Internet Connected Storage: The New Cybersecurity Blind Spot

I. INTRODUCTION

For a long time, the cybersecurity industry has focused on shoring up their internal networks in order to keep external threat actors out. Those who operate inside the wall - employees, partners, suppliers - have been viewed with relatively minimal suspicion. And yet third party data breaches are starting to account for an increasingly larger share of overall incidents. According to the Ponemon Institute, 52 percent of leaks have their origins in a system glitch or human error[1], and 56 percent of the businesses polled in 2017 said that they had experienced a data breach linked to a vendor at some point[2].

The rise in accidental data leaks is not at all surprising when we consider the shifts that have taken place in the way we do business. For one thing, our supplier ecosystems are becoming more complex. On average companies now have 470 external entities who have access to their sensitive corporate information, which is up from around 380 in 2016[3]. And companies are not adapting their security policies around this. Alarmingly, 36 percent of organizations do not apply the same - or higher - cybersecurity standards to their extended ecosystems of partners as they apply to their own business[4].

We are living in an 'oversharing economy', where shareability is favoured over securability. There is a proliferation of sharing devices and cloud storage services with dubitable security credentials which compounds the risk of third-party data leaks. Stories are abounding in the press of sensitive information being leaked by negligent third-parties: thousands of classified US Air Force documents leaked on an unprotected NAS Drive of a Lieutenant colonel[5]; tens of thousands of sensitive corporate documents leaked via the unprotected Connected Storage device of a supplier servicing hundreds of automotive companies[6]; 340 million individual records leaked by a marketing and data aggregation firm on a publicly accessible server[7]. The trend of third-party data leaks is not only worrisome for the risks it entails, but also because these types of leaks are by nature extremely difficult to control.

In this white paper we will look at the places where third party data leaks are showing up and how they are getting there. We will also look at the type of information that is leaking; and most importantly, what can be done to mitigate the risk of these situations.

[1] Ponemon Institute 2018 Cost of Data Breach study
[2] Ponemon Institute 2018 Cost of Data Breach study
[3] Ponemon Institute 2018 Cost of Data Breach study
[4] Accenture 2018 State of Cyber Resilience
[5] https://www.scmagazineuk.com/massive-data-leak-us-air-force-exposes-details-4000+-officers/article/1475052
[6] https://www.nytimes.com/2018/07/20/business/suppliers-data-leak-automakers.html
[7] https://www.wired.com/story/exactis-database-leak-340-million-records/

II. WHERE DO THIRD PARTY LEAKS HAPPEN?

1%	Paste-Sites	**What is it?** Websites for storing plain text and code snippets	**What are we finding there?** Sensitive code, as well as credentials embedded within the code
6%	Code-Sharing Platforms	**What is it?** Websites designed for coding collaboration	**What are we finding there?** Sensitive code posted accidentally by employees, as well as exposed credentials embedded within the code
89%	Internet-Connected Storage	**What is it?** Storage devices with an internet connection, designed for sharing information (eg. NAS drives, databases or cloud storage)	**What are we finding there?** Sensitive documents uploaded to internet-connected storage devices whose security settings have not been properly configured

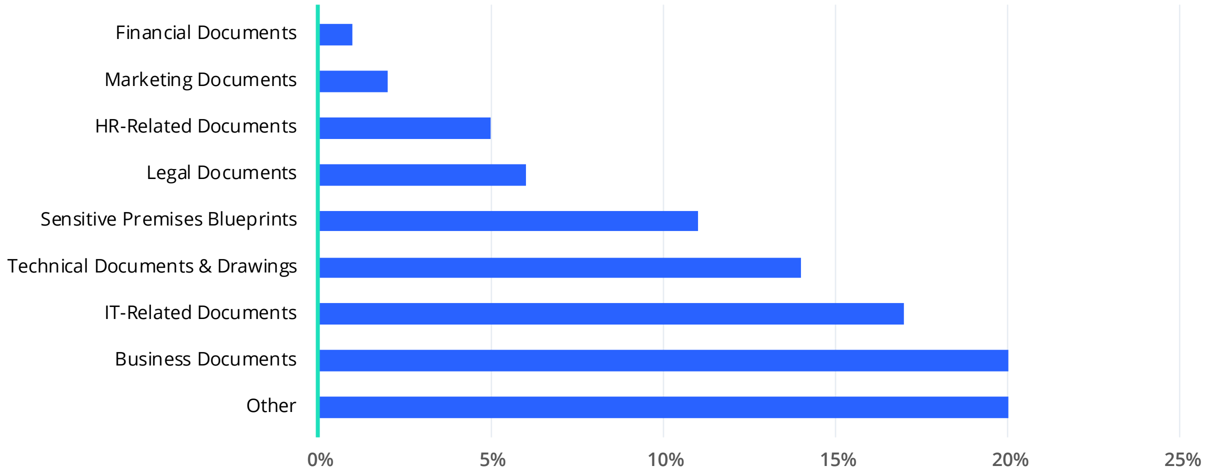
III. INTERNET-CONNECTED STORAGE - THE FAVOURITE HAUNT OF ACCIDENTAL LEAKS

Third-party data leaks are closely bound up in the culture of ‘oversharing’. It is therefore no surprise that we are finding more and more critical data leaks on internet-connected storage, a category which is literally designed to make data shareable. Internet-connected storage includes such devices as NAS drives, cloud storage and databases and the category is rising in popularity. The global consumer market for NAS drives alone is expected to reach USD 8.2 billion by 2025[8]. As for cloud storage, the use of these services is forecast to rise from 1.75 billion in 2017 to 2.3 billion by 2020[9].

The number of data leaks that we are finding for our customers on internet-connected storage is also rising: between 2016 and 2018 the number of CybelAngel customer alerts related to internet-connected storage doubled from an average of 31 per month to an average of 69 per month. Typically, we are finding sensitive business documents (24 percent); IT-related documents (17 percent); technical documents and drawings (14 percent) and Legal documents (6 percent). 93% of these breaches are caused by negligent third-parties - suppliers, partners or customers - who have either uploaded the files to internet-connected storage via an unconscious back-up, or else who have saved the files to a device whose security settings have not been properly configured. In many cases, internet-connected storage devices are set to open by default, and the sensitive files that are kept there are therefore open for anyone to access.

[8] Grand View Research Inc., https://www.grandviewresearch.com/press-release/global-consumer-network-attached-storage-nas-market
[9] Statistica, https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/

Internet-connected storage leaks by document type



Case Study

In September 2017, the CybelAngel platform detected sensitive files belonging to a customer, which had been saved on the unprotected NAS drive of one its suppliers, an IT consulting firm. These files included IP addresses, server configurations and credentials of our client, which could have been used to penetrate their internal network. An alert was issued to our client instantly via the CybelAngel SaaS platform, which enabled them to take down the server and change all their passwords. Two weeks later, a member of the customer's IT security team witnessed a hacking attempt using the data which had originally been exposed by the supplier. This disturbing case shows that threat actors are indeed monitoring and exploiting data exposures on internet-connected storage, and underscores the importance of threat intelligence in order to minimize the risk.

And yet, the magnitude of the breaches we are finding on Connected Storage is only part of the picture. Even more alarming is the criticality of the exposed information. Although internet-connected storage accounts for 26% of overall customer alerts, it accounts for 93% of the most critical.

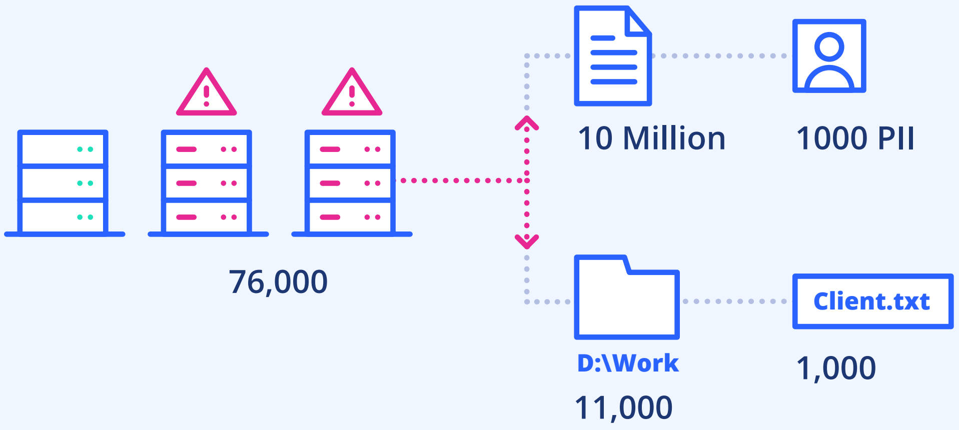
IV. WHAT ARE THE RISKS OF THIRD-PARTY LEAKS?

It is clear that companies' sensitive information is being exposed by third parties, especially on internet-connected storage. But is there actually a risk of it falling into the wrong hands? Many of the third-party data breaches we hear about in the press are uncovered by researchers, rather than threat actors. For example the thousands of open Trello boards containing passwords and login credentials exposed by InfoSec blogger Brian Krebs[10]; or the thousands of sensitive corporate documents being exposed by automotive supplier Level One Robotics, which was uncovered by UpGuard researcher Chris Vickery[11].

[10] https://krebsonsecurity.com/2018/06/further-down-the-trello-rabbit-hole/#more-43780
[11] https://www.nytimes.com/2018/07/20/business/suppliers-data-leak-automakers.html

In order to answer this question, we conducted an experiment to determine how easy it would be for threat actors to access exposed data on internet-connected storage. We scanned 10% of the range of IPv4 on FTP, using open source tools which would be available to mid-level hackers.

Following 10 days of scanning we uncovered a total of 76,000 servers allowing anonymous access, which contained over 11 million documents. This included 1,000 documents containing personally identifiable information (PII), stored on open Connected Storage devices. Moreover, this included 11,000 work-related folders and file paths, and 1,000 with the filename “client”.



Of course, the CybelAngel tool is a much more efficient method of detecting sensitive data exposures. However it is clear that this information is also within easy reach even of mid-strength hackers.

Earlier this year, for example, the group SamSam launched a series of ransomware attacks on hospitals in the US. The group scanned the internet for RDP connections without password protection, before breaking into and freezing networks and asking for a Bitcoin ransom. It is only a matter of time before we start reading about more such examples in the press.

V. WHAT CAN WE DO TO MITIGATE THE RISKS OF CONNECTED STORAGE?

Educating suppliers

Classification of information

Using own tools

Threat intelligence

VI. CONCLUSION

Increasingly complex supplier networks, together with a penchant for sharing information rather than protecting it, are spawning a rise in third party data leaks.

At the same time we are seeing a rise in internet-connected storage devices which, in keeping with the oversharing trend of the modern workplace, are designed to share information rather than secure it. This is where we are seeing the majority of third party data leaks occur, and they are also accounting for the most critical leaks about which we are alerting our clients.

Third party data leaks are quickly becoming the new blindspot of cybersecurity. The industry needs to start taking third party risk as seriously as it regards purely external threats, and a good place to start would be in incorporating it into data risk management strategies.