CybelAngel

WHITEPAPER

Internet-Connected Storage: The New Cybersecurity Blind Spot

WWW.CYBELANGEL.COM

Internet-Connected Storage: The New Cybersecurity Blind Spot

I. THE MODERN IT ECOSYSTEM: MORE THIRD PARTIES, MORE SHARING, MORE CONNECTED DEVICES

Historically, many enterprise IT departments have been preoccupied with shoring up their internal networks in an effort to thwart external threats and malicious activity. Individuals operating inside those internal networks with trusted relationships and access - such as third-party vendors, suppliers, or partners - have often been the subject of relatively minimal attention. Yet third-party data breaches are now accounting for an increasingly larger share of enterprise cybersecurity incidents. Analysts estimate that over 60% of data breaches are linked to third parties,[1] while at CybelAngel, 90% of the data breaches we identify for enterprise customers can be attributed to a third party.

The current volume of third-party data leaks should come as no surprise to those heeding the evolution of the modern enterprise IT ecosystem. For starters, the third-party networks utilized by enterprises are becoming larger and more complex. What's more, to keep pace with the speed of the digital transformation, enterprises are compelled to enable the sharing of their most sensitive information with those third parties. Studies suggest that the average enterprise now shares sensitive and confidential information with about 470 third parties, and this figure has been increasing.[2] Nevertheless, many enterprises fail to adapt their cybersecurity posture to account for these growing third-party ecosystems. An estimated 36% of enterprises apply lower cybersecurity standards to third parties than that which they apply to their own business.[3]

Greater numbers of enterprise IT departments find themselves operating in this 'oversharing economy,' where shareability is favored over securability. And perhaps the most notable (and hazardous) effect of this shareability phenomenon is the proliferation of the use of internet-connected storage devices. The droves of third parties servicing enterprises are invariably accessing and sharing sensitive information via countless connected storage devices - both within and beyond the network perimeter. This aspect of the modern IT ecosystem, an extensive interconnectedness achieved through the strategic adoption of diverse internet-connected devices, is popularly referred to as the 'Internet of Things' or IoT.

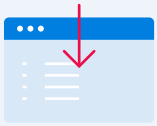
[1] KPMG, Enduring the IoT storm to unlock new paths to value (2018).
[2] Ponemon Institute, Data Risk in the Third-Party Ecosystem (2017).
[3] Accenture, 2018 State of Cyber Resilience (2018).

Unfortunately, many of these internet-connected devices are often insecure by design, and their default security configurations often leave the information they store especially vulnerable. Stories of sensitive information being leaked from connected storage devices abound in the press: thousands of classified US Air Force documents leaked from the misconfigured NAS drive of a lieutenant colonel,[4] tens of thousands of sensitive corporate documents leaked from the unprotected connected device of a third-party supplier to hundreds of automotive companies,[5] and 340 million records of personal information leaked from a marketing firm's exposed connected server.[6] Connected storage data leaks like these, often perpetrated by third-party vendors or suppliers, present arguably the most critical cybersecurity challenges of the modern IT ecosystem. And yet there is reason to fear these challenges are being dangerously overlooked by cybersecurity professionals across modern enterprises. By 2020, more than 25% of all enterprise security attacks are expected to involve IoT devices, but analysts predict that less than 10% of enterprise IT security budgets will actually account for those IoT devices.[7]

In this whitepaper, we explore some findings from CybelAngel's continuous connected storage scanning, and demonstrate the ease with which threat actors can obtain information exposed on connected storage. Our intention is to alert enterprise IT professionals to the risks of the expanding use of connected storage by third parties, and to help avert the potential damage of this new cybersecurity blind spot.

II. BURGEONING CONNECTED STORAGE DATA LEAKS

Where do third-party leaks happen?



1%

Paste Sites

WHAT ARE THEY?

Websites for storing plain text and code snippets (Ex: Pastebin)

WHAT IS CYBELANGEL FINDING THERE?

Sensitive code, as well as exposed credentials embedded within the code

6%

Code-Sharing Platforms

WHAT ARE THEY?

Websites designed for coding collaboration (Ex: GitHub)

WHAT IS CYBELANGEL FINDING THERE?

Sensitive code, often posted accidentally by employees, as well as exposed credentials embedded within the code

89%

Internet-Connected Storage

WHAT ARE THEY?

Storage devices with an internet connection, designed for sharing information (Ex: NAS drives, cloud storage, connected databases)

WHAT IS CYBELANGEL FINDING THERE?

Sensitive documents exposed by misconfigured security settings

[4] Rene Millman, Massive data leak in US Air Force exposes details of 4,000+ officers, SC Media UK (2017), https://www.scmagazineuk.com/massive-data-leak-us-air-force-exposes-details-4000+-officers/article/1475052
[5] Stacy Cowley, 'Big Red Flag': Automakers' Trade Secrets Exposed in Data Leak, The New York Times (2018), https://www.nytimes.com/2018/07/20/business/suppliers-data-leak-automakers.html
[6] Andy Greenberg, Marketing Firm Exactis Leaked a Personal Info Database With 340 Million Records, Wired (2018), https://www.wired.com/story/exactis-database-leak-340-million-records/
[7] Gartner, Leading the IoT: Gartner Insights on How to Lead in a Connected World (2017).

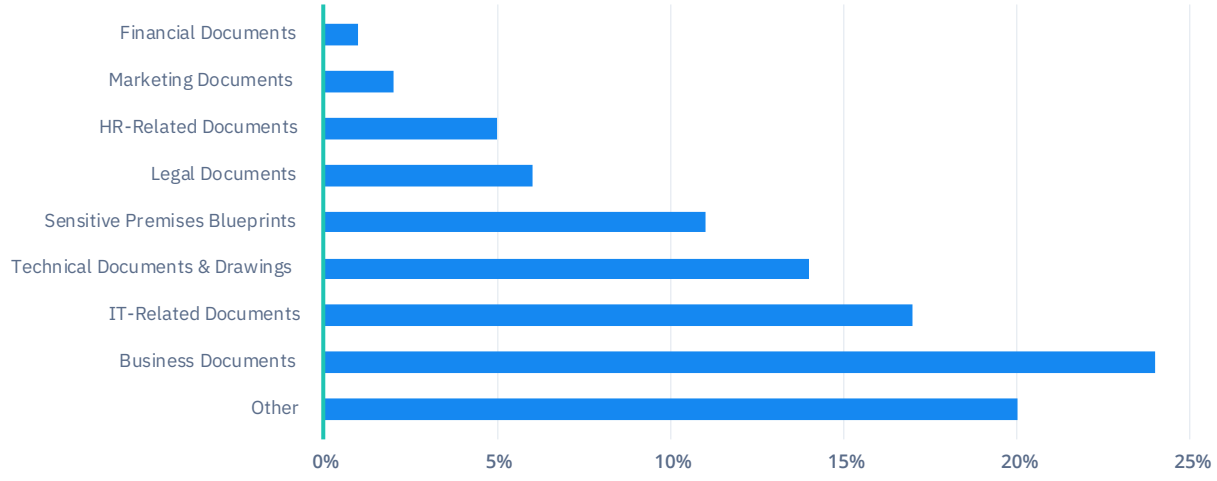
As illustrated above, the vast majority of leaks detected by CybelAngel that are attributable to third parties are leaking from internet-connected storage. Connected storage includes devices like NAS drives, cloud storage, and connected databases, all of which we should expect increasing use of by enterprises' third-party ecosystems. Analysts forecast that more than 65% of enterprises will have adopted the use of IoT devices by 2020 (more than double the adoption ratio in 2017 of 30%), and that by that time, more than 20 billion connected devices will be in use.[8]

Not only are most third-party leaks exposed through connected storage, but most connected storage leaks are caused by third parties. Over 90% of connected storage leaks that CybelAngel detects for enterprises are caused by third parties that either unknowingly backed up information to unsecured connected storage, or negligently saved information to connected storage lacking properly configured security settings. It's worth emphasizing again that many connected storage devices are either completely unsecured or inadequately configured by default.

Indeed, CybelAngel has observed that data leaks from internet-connected storage generally are on the rise. Between 2016 and 2018, the average number of CybelAngel customer data leak alerts related to internet-connected storage more than doubled, from an average of 31 per month to an average of 69 per month. Of course, the volume of connected storage data leaks is not the only cause for concern. The criticality of the data found on connected storage is most concerning. Data leak alerts related to connected storage are currently accounting for 93% of the most critical category of CybelAngel customer alerts.

Details concerning the types of documents we find exposed on connected storage are provided in the chart below. CybelAngel most frequently detects sensitive business documents (24%), IT-related documents (17%), technical drawings (14%), and premises blueprints (11%).

Internet-connected storage leaks by document type



[8] Gartner, Leading the IoT: Gartner Insights on How to Lead in a Connected World (2017).

Customer Case Study

In September 2017, the CybelAngel platform detected sensitive files belonging to a customer on the unprotected NAS drive of one of the customer's third-party partners, an IT consulting firm. These files included IP addresses, server configurations, and credentials of the customer, which could have been used to penetrate their internal network. An alert was issued to the customer instantly via the CybelAngel SaaS platform, which enabled the customer to take down implicated servers and change their credentials. Two weeks later, a member of the customer's IT security team observed a hacking attempt that utilized the data which had been exposed by the IT consulting firm. This disturbing case evidences that threat actors are actively monitoring for and exploiting data exposures on internet-connected storage, and it underscores the importance of the roles that data leak detection and threat intelligence play in minimizing enterprise cybersecurity risks.

III. EASE OF THREAT ACTOR ACCESS TO CONNECTED STORAGE

Findings from CybelAngel's continuous scanning of internet-connected storage clearly indicate that there is widespread exposure of enterprises' sensitive information on connected storage devices, often at the hands of third parties. But even if enterprises' sensitive information is exposed on connected storage, how feasible is it for threat actors, who lack powerful scanning tools like CybelAngel, to actually detect and access the information?

It's important to remember that CybelAngel is one of the most advanced data leak detection technologies, incorporating artificial intelligence and years of machine learning evolution, battle-tested by sophisticated enterprises. Those skeptical that threat actors could practicably find and use the information exposed on connected storage - without the help of enterprise-grade tools - might point out that many third-party data leaks garnering press attention are actually uncovered by cybersecurity researchers, rather than threat actors. Examples might include the open Trello boards containing passwords and login credentials that were detected by InfoSec blogger Brian Krebs,[9] or the thousands of sensitive corporate documents exposed by automotive supplier Level One Robotics, which were uncovered by UpGuard researcher Chris Vickery.[10]

[9] Brian Krebs, Further Down the Trello Rabbit Hole, Krebs on Security (2018), https://krebsonsecurity.com/2018/06/further-down-the-trello-rabbit-hole/
[10] Stacy Cowley, 'Big Red Flag': Automakers' Trade Secrets Exposed in Data Leak, The New York Times (2018), https://www.nytimes.com/2018/07/20/business/suppliers-data-leak-automakers.html

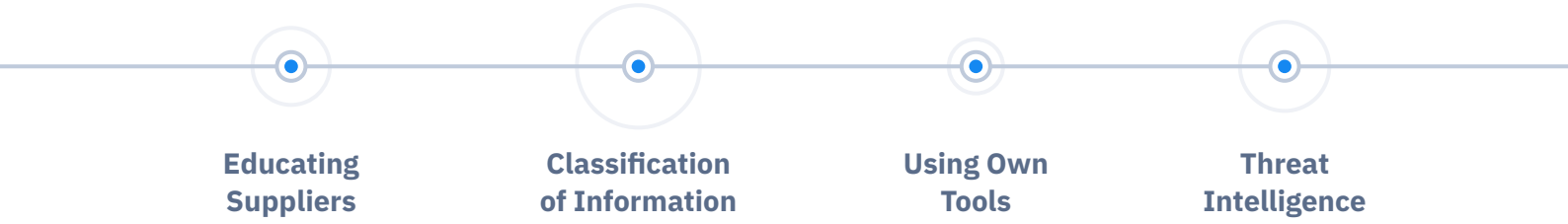
To determine the ease with which an average threat actor could access sensitive information exposed on connected storage, select CybelAngel researchers temporarily secluded themselves from the CybelAngel platform, and attempted to scan connected storage using only open source tools that could be used by a threat actor with moderate technical ability. These researchers were able to use those open source tools to scan 10% of the range of IPv4 on FTP over the course of 10 days. After those 10 days of scanning, our researchers had uncovered a total of 76,000 connected servers allowing anonymous access. These connected servers contained over 11 million documents. Our researchers were able to determine that 1,000 of these documents contained personally identifiable information (PII). Our researchers also discovered 11,000 folders and/or file paths that they determined were related to organizations, and within those folders and file paths, our researchers discovered 1,000 documents with file names that included the term “client”.

Open source tools cannot scan the various layers of the internet as fast or as efficiently as enterprise-grade solutions can. Such tools also cannot crawl, index, or filter the data and documents that they do find in the same manner as enterprise-grade solutions. But what our researchers did demonstrate is that threat actors of relatively little means are ultimately capable of eventually finding the sensitive information that third parties are frequently exposing through connected storage. And as threat actors become more organized and increasingly capable, the potential for damage becomes exponentially greater. Consider the series of SamSam ransomware attacks on US hospitals in early 2018. An organized group of threat actors scanned the internet for exposed RDP connections, which they used to infect internal networks with SamSam ransomware. In one instance, this group was able to use a hospital’s third-party vendor’s compromised remote access to install ransomware and successfully obtain a Bitcoin ransom.[11] Fortunately, modern IT departments can stay ahead of threat actors like these with enterprise-grade platforms like CybelAngel, which continuously monitors every layer of the internet for exposure, and which utilizes AI and machine learning to assess the information it finds and provide immediate alerts to customers.

[11] Charlie Osborne, US hospital pays $55,000 to hackers after ransomware attack, ZDNet (2018), https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/

IV. CONCLUSION

What can enterprises do to mitigate the risks of connected storage?



Increasingly complex third-party ecosystems, with a penchant for accessing and sharing information via internet-connected storage, are spawning one of the most severe cybersecurity challenges in enterprise IT. Yet too many IT departments remain fixated on the robustness of their network perimeter, and overlook the significant risk of their own third-party vendors or suppliers leaking sensitive information from connected storage. As the above has demonstrated, the frequency and magnitude of connected storage leaks cannot be overstated, and threat actors with any meaningful technical ability are capable of accessing and opportunistically utilizing those leaks. The key to mitigating the damage of the virtually inevitable leakage of sensitive information is simply to be the first to know a leak has occurred. Digital risk management platforms like CybelAngel are providing that vital threat intelligence to modern enterprises every day, as it is our stated goal to alert our customers to every cybersecurity blind spot that develops in the evolving IT ecosystem.

CybelAngel is a leading digital risk management platform providing enterprises with actionable threat intelligence that enables effective remediation and improved cybersecurity posture.