Perfect Storm: A Cautionary Examination into Zero-Day Exploits in the Cloud

IBM defines the term zero-day exploit as “a cyberattack vector or technique that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware” ("What Is"). This definition is extremely broad and can thus be applied to a myriad of vulnerabilities, from cryptographic weakness to SQL injection to firewall failures. To make things more concrete, a recent example of this is the MoveIt data breach. MoveIt is a file transfer software that was first released by IpSwitch in 2019, which consolidates file transfer into a single software and was initially advertised as a “secure managed file transfer software” (“MOVEit Secure”). In late May of 2023, data began to be transferred by hundreds of MoveIt deployments to unauthorized actors and gained access to data from over 1,000 organizations, affecting at least 60 million individuals and costing all victims involved an estimated $10.6 billion dollars (Alder). The culprit? A zero-day exploit wherein web-portal users were able to inject SQL to install a sophisticated web shell allowing them to elevate their own permissions on the system, and then leverage their elevated permissions by downloading a user’s data.

The development of zero-day exploits typically doesn’t take very long, and once realized, they often persist for years. A report of zero-day exploits found that 55 of the 159 observed would take attackers between zero to 10 days to setup, and only 12 took greater than 120 days (Ablon and Bogart). With such low development times, exploits that are discovered for one system may be used on others containing similar vulnerabilities within days (or even hours). Additionally, it was found in the same report that exploits have an average lifespan of 6.9 years upon discovery, with 25% surviving less than a year and a half and another 25% surviving more than 9.5 years (Ablon and Bogart). Low development time may also imply that exploit development could be done by individuals with access to few resources. Exploits requiring few

resources are very worrisome, since there are simply more people in the world capable of discovering and capitalizing on vulnerabilities.

Since 1988, IBM has had 7327 zero-day vulnerabilities, accounting for three percent of their overall vulnerabilities ("What Is"). While this might not sound like an incredibly large share, IBM's website states that "those (zero-day vulnerabilities) in widely-used operating systems or computing devices—are among the most severe security risks, because they leave huge numbers of users or entire organizations wide open to cybercrime until the vendor or the cybersecurity community identifies the problem and releases a solution" ("What Is"). Therein lies severe risk - if discovered, a system-wide vulnerability may lead to company-wide catastrophes.

This potential risk becomes particularly daunting when one begins to consider the mass cloud migration which has swept businesses around the world. Due in part to the pricing edge at-scale cloud providers can offer, businesses of various sizes have found it both more convenient and cost-effective to migrate their services to the cloud, rather than dealing with the risk in startup capital, fragility, implementation intricacies, and knowledge requirements generally associated configuration of on-prem servers (Flexera). It is of note that, presently, cloud providers have existed for many decades, implement advanced security protocols, and have a staggering amount of funding at their disposal to help prevent and detect critical system vulnerabilities. However, the mass conglomerate of organizations on the cloud also enriches the value of it as a target for potential attackers - all of the data, compute resource, and ransom potential under one architectural scheme sets an enormous price tag on the discovery of could exploitation methods, which will be further discussed later on in this paper.

As of 2023, 44% of traditional small businesses, 66% of small tech companies, and 74% of enterprises utilize cloud services (Slingerland, "101 Shocking"). Global end-user spending on public cloud is projected to rise to ~$599 billion in 2023, up approximately 20% from the $500 billion spent in 2022 (Slingerland, "Cloud Computing"). The presence of the cloud is massive and ever-expanding, and somewhat monopolized. As of Q2 of 2023, Google Cloud Platform accounted for 11% of the cloud market share, Azure had 22%, and AWS had 32%, totaling 65% of the total market. With so much of the market dominated by merely three cloud providers, another threat presents itself: a cloud oligopoly. If there are few severe cloud vulnerabilities in these providers, this shift to oligopoly can be viewed as a positive thing from a security perspective - cloud providers have no doubt collectively dedicated much time, thought, testing, and resources towards the development of their infrastructure when compared to the average business employing on-prem services. Thus, by creating a standardized off-prem avenue for business infrastructure, big cloud has likely minimized the potential for businesses to experience vulnerabilities due to suboptimal decision-making along their server setup journeys.

The "big three" offer many additional cutting-edge services, attracting even more customers, such as finely tunable machine learning models, easy-to-obtain data analytics, security monitoring, and IoT. With the addition of each of these, more business needs will undoubtedly be centralized and fulfilled by and in the cloud, but also, as with the introduction of any new software to a system, the potential for vulnerabilities is also introduced.

In 2016, the leading cloud provider was AWS with a market share of 31%, with the second largest being Microsoft's Azure with a formidable but rather unalarming 9%, and Google Cloud being the fourth-largest with a seemingly insignificant 4% (Panettieri). Thus, in the past seven years, each of the big three providers (each of whom had gargantuan funding backing their

expansion efforts, the likes of which can only be matched by a select few mega-corporations and billionaires) has grabbed more of the cloud market pie while competition has shrunk away. Thus, based on existing trends and the high startup capital required to compete, it is a reasonable inference that the cloud space will only become increasingly exclusive in terms of providers with real competitive merit as time passes.

Should one of the big three experience an exploit (assuming the exploit cannot also be applied to the other cloud providers), organizations have the option to switch to a new provider. It is certain that many will, for the reputation of the exploited provider will be permanently marred, and security is king - particularly when you have a large brand, capital, and valuable information to protect. It is quite likely that the result would be a cloud economy that more closely resembles a monopoly, where companies are at the mercy of even fewer cloud providers, and prices for the goods and services of all companies which utilize the cloud go up. This scenario would rock the global economy, and its possibility should sound an alarm to policymakers both within and outside of the US. The question may then arise: if everyone uses the same cloud, and then that cloud is exploited due to some unforeseen flaw, what happens to everyone's data? Is it lost? Leaked? What of their machine learning models, IoT devices, and other infrastructure built on top of that cloud? Will their operations immediately halt? Is this a contingency that many companies (and even more worryingly, governments) have planned for?

On the other hand, an organization utilizing multiple competing clouds can also raise security risks. Although its prevalence decreased slightly between 2022 and 2023 (from 89% to 87%), multi-cloud is still an incredibly popular model wherein businesses will utilize multiple clouds (sometimes both public and private) for their needs (Flexera). Multi-cloud, depending on how it's used, can increase the probability of a company experiencing an exploitation incident by

effectively widening their attack surface. Using two public cloud providers, for example, means that a company is susceptible to zero-day exploits from more vectors than they otherwise would have been, effectively increasing their probability of a breach. They now have multiple encryption keys, security configurations, network configurations, and login credentials that can be stolen and exploited. This issue is worsened if they store the same sensitive data on both clouds.

As cloud-run automation of services and business operations increases each year (a trend which will probably continue in the next five years), one would expect the amount of manual inspection of cloud services, and the number of people involved in infrastructure on a per-company basis to decrease. In the context of zero-day exploits, this transformation could manifest as a potential delay in threat reporting. Specifically, if an exploit manages to elude the detection mechanisms of automated cloud-run anomaly and vulnerability detection, the consequence may be a deceleration in identifying and addressing the impact on cloud customers.

In terms of raw counts, the number of zero-day vulnerabilities (with respect to technology as a whole, not necessarily the cloud) has risen significantly in 2023. According to Darren Turner, the NSA's cybersecurity directorate chief of critical networks defense, the rise could be attributed to the phenomenon that "once one zero day has been discovered, that can help generate other, similar vulnerabilities — which may be one reason why the use of such vulnerabilities is increasing over the long term" (Bracken). Naturally, one would expect the rate of software bugs on a per-software basis to decrease over time as developers become more security-savvy. However, with the amount of software increasing each year, and many of the major cloud providers rolling out new services on top of their existing architecture, the potential for zero-day exploits is also created ("Software - Worldwide"). Naturally though, the number of new features

rolled out by cloud providers must eventually plateau, and one would expect the number of annual exploits discovered to decrease each year in the absence of new releases.

One of the most significant challenges with zero-day vulnerabilities is that both public and private cloud providers simply don’t know what they don't know. As Dijkstra once asserted, "Program testing can be used to show the presence of bugs, but never to show their absence" ("Dijkstra Quotes”). It is impossible to prove the absence of vulnerabilities in a cloud system. Thus, the solution to zero-day vulnerabilities presents an unsatisfying reality: stringent coding standards, robust testing, rollback capability, and the implementation of bug bounties. Fortunately for the global economy, major cloud providers such as AWS seemingly already incorporate all these elements (Bugbounter). While release rollbacks are valuable, they necessitate that the person rolling back a release knows which version lacks the vulnerability, a process that may entail significant time for diagnosis. This valuable time introduces a window during which the provider or its customers could be actively exploited.

Cloud providers would be wise to publicize generous bounty rewards, encouraging bug hunters to share information with them rather than with cyber-criminals on the dark web. Depending on the exploit, its discreet revelation to the company could be invaluable, considering the scale and reputation value of major cloud providers such as Microsoft, potentially worth billions (Redmond).

In conclusion, the pervasive use of cloud services coupled with the concentration of market share among a few major providers presents a perfect storm of damage potential in the realm of zero-day exploits. Control over issues caused by exploits of the ever-expanding public cloud are concentrated in the hands of few, whose foresight or lack thereof will impact billions. The rapid development and deployment of zero-day exploits, with an average lifespan of nearly

seven years, accentuate the persistent nature of these threats, the absence of which can never truly be proven. Thus, it is up to consumers, cloud providers, and governments to make wise decisions to mitigate the presence of and lessen the damage caused by the exploitation of such vulnerabilities.

Based upon the above trends, I predict that in five years zero-day exploits in the cloud will be less frequent but instances will have an increasing potential for catastrophic personal and economic damage. My prediction is dependant upon trend of cloud adoption continuing to be prevalent, and an increase or at least flatlining of the aggregate market shares for Azure, AWS, and Google Cloud, all of which I expect to hold true for the foreseeable future.

Works Cited

Ablon, Lillian, and Andy Bogart. "Zero Days, Thousands of Nights." Rand Corporation, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf. Accessed 21 Nov. 2023.

Alder, Steve. "SEC Launches Investigation into Progress Software's Moveit Hack." Hipaajournal, hipaajournal, 17 Oct. 2023, www.hipaajournal.com/sec-launches-investigation-into-progress-softwares-moveit-hack/.

Bracken, Matt. "Cisa Sees Increase in Zero-Day Exploitation, Official Says." CyberScoop, 3 Nov. 2023, cyberscoop.com/cisa-zero-day-ransomware/#:~:text=%E2%80%94%20The%20exploitation%20of%20zero%2Dday,in%20the%20cyber%20threat%20landscape.

Bugbounter. "The Marketplace." Amazon, Board of Trade, 1987, aws.amazon.com/marketplace/pp/prodview-joes5hm2bgmie.

"Dijkstra Quotes - Brainyquote." Brainyquote, www.brainyquote.com/authors/edsger-dijkstra-quotes. Accessed 22 Nov. 2023.

Flexera. "2023 State of the Cloud Report." 2023,

https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2023.pdf. Accessed 20 Nov. 2023.

Haranas, Mark. "Cloud Market Share Q2 2023: AWS, Microsoft, Google Battle." CRN, 9 Aug. 2023, www.crn.com/news/cloud/cloud-market-share-q2-2023-aws-microsoft-google-battle/4.

"MOVEit Secure Managed File Transfer Software: Progress." Progress.Com, Progress Software Corporation, 2023, www.progress.com/moveit?gclid=Cj0KCQiApOyqBhDlARIsAGfnyMr-4FHzVtJu6Zuo7wFSJ7lyJXKFpL4u-0mKKmGhKVqG8fHKIybd3ygaAmFsEALw_wcB.

Panettieri, Joe. "Cloud Market Share 2016: AWS, Microsoft, IBM, Google -." ChannelE2E, 4 Feb. 2016, www.channele2e.com/post/cloud-market-share-2016-aws-microsoft-ibm-google.

Redmond, Tony. "Microsoft Cloud Revenues Hit $111.6 Billion." Office 365 for IT Pros, 27 July 2023, office365itpros.com/2023/07/27/microsoft-cloud-revenue-110b/.

Slingerland, Cody. "101 Shocking Cloud Computing Statistics (Updated 2023)." CloudZero, BB Agency, 20 Oct. 2023, www.cloudzero.com/blog/cloud-computing-statistics/#:~:text=About%2044%25%20of%20traditional%20small,companies%20and%2074%25%20of%20enterprises.

Slingerland, Cody. "Cloud Computing Market Size and Key Insights You Need to Know in 2023." CloudZero, BB Agency, 25 Aug. 2023, www.cloudzero.com/blog/cloud-computing-market-size/.

"Software - Worldwide: Statista Market Forecast." Statista, Aug. 2023, www.statista.com/outlook/tmo/software/worldwide.

"What Is a Zero-Day Exploit?" IBM, Mar. 2023, www.ibm.com/topics/zero-day.