CASE STUDY

EZMONITOR

HELPS MICROSOFT TAKE DOWN OVER 700 VULNERABLE URLS

KEYTOS

COMPANY OVERVIEW

Microsoft develops, licenses, and supports a range of software products and services. The company offers products including operating systems, productivity applications, server applications, development tools, video games, and cloud services. The company operates globally with offices in more than 190. Countries. Microsoft twelve months revenue as of March 31, 2022 was $192.557 Billion, a 20.37% increase over the previous year.

EZMONITOR

CHALLENGE

As one of the largest companies in the world, Microsoft creates thousands of websites every year. To achieve this large scale, these sites are created and managed different teams, distributing the management across thousands of engineers across multiple business groups. This setup made it impossible for Microsoft to centrally manager all websites' DNS life-cycle. Engineers would forget to decommission sites and their respective DNS, leaving an open door for any would-be phishing attackers eager to impersonate Microsoft. Without the ability to centrally manage all of their DNS lifecycles, Microsoft could not truly secure against subdomain takeover attacks.

SOLUTION

While Microsoft has many cloud security products such as Microsoft defender for web applications, Azure Sentinel, and many more, these services miss this vulnerability since they monitor for misconfigurations of existing resources.

Since EZMonitor does not depend on the existing Azure resources, we can monitor all Microsoft domains without the need for monitoring their internal controls or subscriptions. Using Certificate Transparency logs, EZMonitor was able to centralize the monitoring of all Microsoft domains and create an alert every time a domain was longer in use and the DNS entry has not been deleted.

RESULTS

We started working with Microsoft since day one. When our engineers discovered the vulnerability, we immediately reported the new vulnerability to Microsoft MSRC. After a month of internal testing, we found 243 Microsoft domains that were vulnerable to takeover. At this point, we contacted our contacts in Microsoft Security and worked with them to take those domains down. Since then, our tool has come out of beta and has helped Microsoft remove over 700 vulnerable DNS. These are domains that without the help of EZMonitor could have ended up as phishing sites used to attack Microsoft customers.

While this case study focuses on how EZMonitor was used to help Microsoft prevent phishing attacks by detecting this specific vulnerability, this barley scratches the surface of what EZMonitor does for companies around the world. EZMonitor helps organizations gain visibility into their internal and external certificates, this visibility helps prevent outages due to expiring certificates, detects shadow IT Certificate Authorities and more. To learn more about EZMonitor full capabilities, book a domain SSL scan analysis (value of $1000) for free: https://calendly.com/keytos/freesslscan