SKYBOX® SECURITY

2019 VULNERABILITY AND THREAT TRENDS

Mid-Year Update

EXECUTIVE SUMMARY

Vulnerabilities don’t exist in a vacuum.

The risk they pose to your organization depends on a variety of internal and external factors that are in a near–constant state of change. Keeping up with that change is vital to limiting your organization’s risk of attack. That’s why we publish this report — to give CISOs and security leaders the perspective they need to see the trends shaping the threat landscape and, in turn, their defense strategy.

The *2019 Vulnerability and Threat Trends: Mid–Year Update* examines new vulnerabilities published in the first half of 2019, newly developed exploits, new exploit–based malware and attacks, current threat tactics and more. Such analysis helps to provide much needed context to the thousands of vulnerabilities published every year. The insights and recommendations provided are here to help align security strategies which can effectively manage the complex challenges of the current threat landscape. Incorporating such intelligence in vulnerability management programs will help put vulnerabilities in a risk–based context and focus remediation on the small subset of vulnerabilities most likely to be used in an attack.

Download the full report at skyboxsecurity.com/trends-report >

KEY FINDINGS

Only a tenth of vulnerabilities have a developed exploit.

The good news is that of the more than 7000 vulnerabilities published in the first half of 2019, a small fraction will ever have an exploit, with less than one percent exploited in the wild. The bad news: increasing network complexity makes it difficult to understand which of those vulnerabilities are exposed to potential attacks or exist on important assets, representing a critical risk.

Cloud container vulnerabilities in steady climb.

As use of various cloud services has grown, so too have their vulnerabilities. Vulnerabilities in container software have increased by 46 percent in the first half of 2019 compared to the same period in 2018. Looking at the two year trend of container vulnerabilities published in first halves, container vulnerabilities have increased by 240 percent.

Trend of broad–reaching vulnerabilities continues, with heavy concentration in CPU side-channel info leaks.

Vulnerabilities often exist across programs or software modules which share code. In the first half of 2019, chip-level vulnerabilities like Spectre/Meltdown were particularly numerous, making collateral damage of "downstream technology" such as operating systems or browsers running on affected architecture. In the first half of 2019, 40 vulnerabilities had the capability to impact three or more vendors.

Tide turns away from cryptomining — ransomware, botnets and backdoors fill the vacuum.

In 2018, malicious cryptomining reigned supreme as the cybercriminal tool of choice. But with the decline in cryptocurrency value, and with Coinhive shutting down, attackers have turned back to their old reliables. Usage of ransomware, botnets and backdoors jumped 10, eight and 18 percentage points, respectively, between the first half of 2018 and the same period this year.

Recommendations

In order to accurately prioritize remediation, organizations have to keep up with the threat landscape as it evolves. As trends in vulnerabilities, exploits and threats shift, so too must defense strategies. Whether you're protecting against the rise of cryptominers, safeguarding OT in critical infrastructure or simply trying to keep up with what patch to deploy next, incorporating accurate and up–to–date intelligence will give you the edge you need to be proactive against a dynamic threat landscape.

Like vulnerabilities, your security program doesn't exist in a vacuum. Having the ability to correlate vast and varied intelligence sources from within your infrastructure as well as the vulnerabilities and threats in play will create defense than the sum of its parts.

Establish risk–based vulnerability management

In order to focus remediation on the right vulnerabilities, you need to assess occurrences against the latest threat intelligence, as well as the relationship of vulnerable assets to the security controls that could protect them. This way, action will be focused on the small subset of vulnerabilities posing a critical risk to your business.

Secure your entire hybrid network

Security programs today need to be able to assess vulnerabilities across the entire network on demand. Organizations need to ensure they have reliable coverage to assess and prioritize vulnerabilities in on–prem, public and private clouds and operational technology systems to truly understand the risk to their organization as a whole.

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 130 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060