NSFOCUS

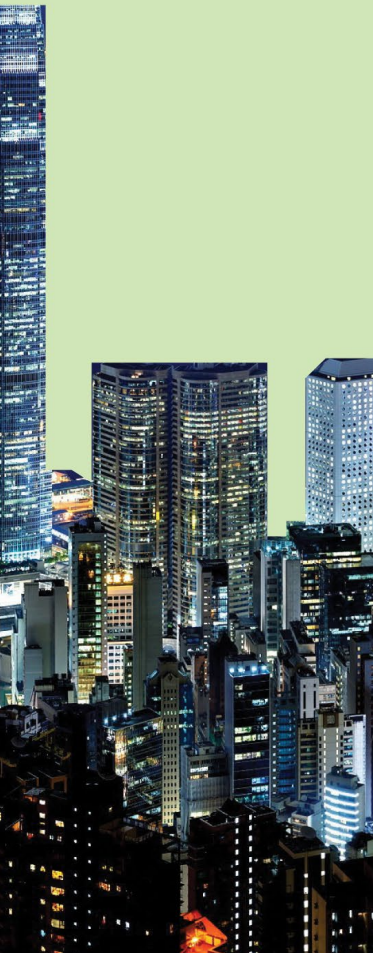
CASE STUDY

NSFOCUS Protects 2016 G20 Summit from 100,000+ Cyber Attacks

AN INTELLIGENT HYBRID SECURITY APPROACH FOR G20

NSFOCUS solutions that were deployed to protect the G20 Summit include:

- NSFOCUS Threat Intelligence (NTI) Portal and Threat Intelligence
- NSFOCUS Web Vulnerability Scanning System (WVSS)
- NSFOCUS Web Application Security
- NSFOCUS Next Generation Intrusion Prevention System (NGIPS) and Threat Analysis System (TAS)
- NSFOCUS Anti-DDoS System (ADS)



Overview

In September 2016, the world's attention was on the Group of Twenty (G20) Summit in Hangzhou, China. Established in 1999, the G20 Summit provides a global platform to discuss financial stability and policy — and is attended by prominent world leaders representing the top 20 global economies, including the United States, Russia, France and Germany, among others. The importance and global visibility of the G20 Summit makes the event a clear target for cybercriminals interested in gaining access to critical data and applications. As the world's most visible heads of state prepared to descend on the Summit, so did hackers across the globe — putting all the Summit's cyber assets and associated networks at risk.

NSFOCUS was commissioned by China's Ministry of Public Security to protect the G20's cyber infrastructure. Securing the G20 Summit is no small task and required a high level of coordination, security strategy, and best-in-class technology solutions from NSFOCUS to protect the information that would inevitably be targeted by highly sophisticated cybercriminals. NSFOCUS was selected to protect G20 assets based on its proven, 16-year track record as China's largest security company, its suite of global threat intelligence solutions, and its history of securing large global events, including the 2008 Olympics in Beijing and the World Internet Conference.

Securing the G20 Network — Keeping Hackers Out

Preparing to defend the G20 Summit from hackers was a national effort and involved all levels of government to ensure that all cyber assets would remain secure before, during and following the event. **NSFOCUS was charged with protecting 12,729 key G20 applications** — including the Summit's official website and other critical web pages. Complicating the task was the wide variety of stakeholders whose security efforts needed to be coordinated as part of this effort — including the national government, provincial governments, financial institutions, infrastructure owners, communications providers and global media outlets.

NSFOCUS responsibilities for the G20 Summit included:

- Designing and building a Security Operations Center to collect, analyze, and act on real-time threat intelligence
- Penetration testing of the assigned assets
- Conducting large scale DDoS drills in advance of the Summit
- Performing web application attack drills against assigned cyber assets
- Establishing an Emergency Cyber Response Team to conduct incident response planning and investigation in real-time
- Providing continuous web application scanning and monitoring
- Ensuring DDoS attack mitigation before, during, and after the Summit

NSFOCUS implemented an Intelligent Hybrid Security approach — built on a foundation of real-time global threat intelligence to provide unified, multi-layer protection that could not be penetrated by the hundreds of thousands of attempted threats before and during the Summit. In order to combat these threats and ensure the security of the summit, NSFOCUS deployed an integrated and layered suite of solutions. Knowing that real-time, global threat intelligence would be critical to success, NSFOCUS first established a Monitoring Command Center that would track and action threats in real-time using its NSFOCUS Threat Intelligence (NTI) portal and Threat Situational Awareness (TSA) dashboard. The company's Web Vulnerability Scanning System (WVSS) was deployed to perform continuous web application vulnerability scanning and monitoring, and its Web Application Security was used for dealing with the identified vulnerabilities. Both the NSFOCUS Next Generation Intrusion Prevention System (NGIPS) and Threat Analysis System (TAS) were used to detect and thwart targeted attacks. Finally, NSFOCUS Anti-DDoS System (ADS) was used to prevent outages and ensure critical applications were up and running at all times.

In the 6 months leading up to the event, **NSFOCUS successfully identified more than 611,000 security and web vulnerabilities, of which 190 were high-risk**.

As Hackers Descend, NSFOCUS Defends Against 100,000+ Web Attacks

Once the Summit convened, hackers intensified their attacks on G20 networks and applications. During the Summit, **the NSFOCUS team successfully blocked approximately 169,919 web attacks** – including a Trojan malware that was intended to steal credentials.

Over the course of the event, beginning on September 1, NSFOCUS defended and mitigated against:

- More than two million web attacks — including **133,254 attacks directly targeting the G20 network**
- **1,984 DDoS attacks targeting the G20 network**, protecting against 41.2 TB of malicious traffic, the equivalent of one attempt every two minutes
- **1.9 million attacks targeting key service providers** associated with the Summit

Many of the DDoS attacks thwarted by NSFOCUS were hybrid UDP, ACK and SYN flood. The longest attack lasted for 10 minutes with a total of 10 Gbps of traffic, and the largest peak flow deflected at any point was 7 Gbps. In total, **NSFOCUS scrubbed more than 41 terabytes of traffic**. Attacks originating from the United States, Russia and Brazil were the most prevalent.

Protection on a Global Scale, In Any Environment

"During the course of the conference, NSFOCUS protected G20 assets and affiliates against a non-stop barrage of attacks. Hundreds of thousands of attacks executed over the course of several days presents a significant danger to even the most secure of networks. It's worrying, but not surprising, to see such a force unleashed on the summit. NSFOCUS is proud to have defeated these attacks on a key leadership forum like G20."

— Dr. Richard Zhao, SVP, Global Threat Research, NSFOCUS

NSFOCUS' real-time coordination with multiple vendors across challenging environments proves its ability to work with global enterprises of any size to successfully defend critical applications. NSFOCUS' success in combatting attacks during the G20 Summit is a testament to the strength of its global research team and suite of security solutions.

G20 2016 CHINA PROTECTED BY NSFOCUS

To learn more about NSFOCUS solutions visit: www.nsfocusglobal.com, or email sales@nsfocusglobal.com.

NSFOCUS

3979 Freedom Circle
Suite 900
Santa Clara CA 95054
Phone: 1 408-907-6638
www.nsfocusglobal.com

NSFOCUS NUMBERS AT A GLANCE

- Identified 611,000 security and web vulnerabilities before the Summit started
- Defended and mitigated against 133,254 cyber attacks against G20 assets during the Summit
- Thwarted 1,984 DDoS attacks against the G20 network
- Prevented 1.9 million attacks against key service providers