Case Study

Optiv’s ThreatDNA™ Advisory Helps Clients Prevent Malware Attack

OVERVIEW
Organizations around the world use Citrix server software to provide remote access to hybrid cloud and SaaS applications and deliver web, traditional and cloud-native applications to their users. Unfortunately, a vulnerability affecting Citrix Application Delivery Controller (ADC) and several versions of Gateway was identified which would allow a threat actor to execute code on a server without authentication.

Along with our trusted sources, like the SANS institute, Optiv identified a way to exploit this vulnerability, though at the time of the threat advisory, no proof of concept code had been released in the wild. Shortly after the advisory was released, SANS identified an exploit attempt on a honeypot server, confirming that at least one threat actor was attempting to weaponize the vulnerability.

HOW OPTIV HELPED
Optiv released an initial threat advisory detailing the nature of the vulnerability as well as specific work-around mitigation procedures so clients could determine if their servers were vulnerable and take steps to block hostile scripts. We followed this up with two advisories four days later confirming the release of multiple exploits, shortly followed by confirmed malicious attacks and uploaded payloads. These advisories also contained indicators of compromise (IOC) and recommendations for remediation, allowing clients to quickly identify whether they had been targeted and begin remediation efforts. Our ThreatDNA™ team also included all of the IOCs into our intelligence feed, which integrated them into devices managed by Optiv and configured to receive the feed.

CHALLENGES
- No official patch available from Citrix at the time
- Multiple exploits significantly increased the likelihood of attacks
- SANS reports indicated heavy exploitation and botnet activity
- Threat actors attempted to remove evidence of exploitation

SOLUTION
- Implement war room protocols and mitigation
- Integrate IOCs into security controls for improved protection
- Update all devices configured to receive Optiv’s ThreatDNA™ intelligence feed

RESULTS
- Optiv’s ThreatDNA™ advisory alerted subscribers before any confirmed exploits
- Automatically integrated IOCs and mitigation steps on devices managed by Optiv
- Payload script identified and published

NEXT STEPS
- Continue to vigilantly monitor logs
- Install official patch as soon as it becomes available

Optiv is a market-leading provider of end-to-end cybersecurity solutions. We help clients plan, build and run successful cybersecurity programs that achieve business objectives through our depth and breadth of cybersecurity offerings, extensive capabilities and proven expertise in cybersecurity strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

©2020 Optiv Security Inc. All Rights Reserved.