PLAY Ransomware Group Gains Access via Citrix Bleed Vulnerability

By George Glass, Laurie Lacono, Keith Wojcieszek

Published: 2024-06-11 · Archived: 2026-04-05 14:46:45 UTC

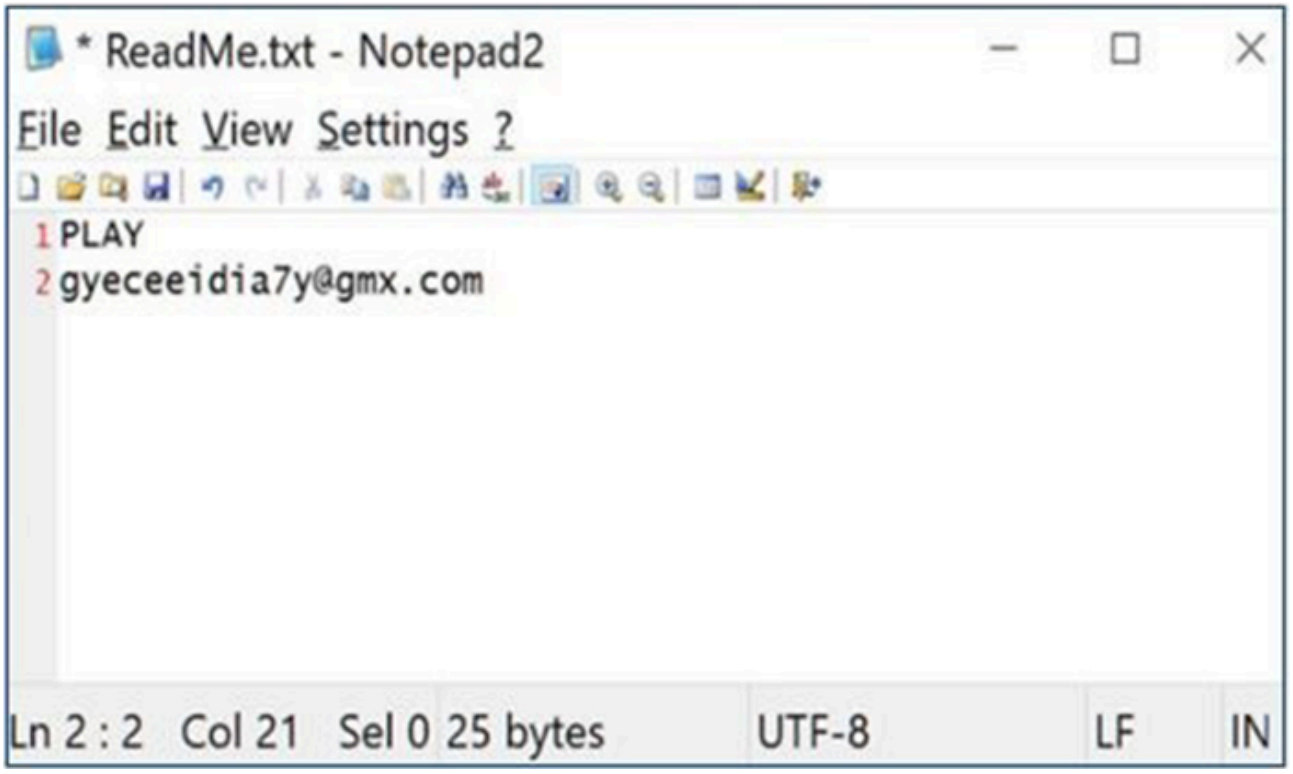
In November 2023, the Cybersecurity & Infrastructure Security Agency (CISA) published guidance for addressing vulnerability CVE-2023-4966, affecting Citrix NetScaler ADC and NetScaler Gateway. This vulnerability is also known as Citrix Bleed.

According to CISA: “The affected products contain a buffer overflow vulnerability that allows for sensitive information disclosure when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server. Customers using Citrix-managed cloud services or Citrix-managed Adaptive Authentication are not impacted. Exploitation of this vulnerability could allow for the disclosure of sensitive information, including session authentication token information that may allow a threat actor to “hijack” a user’s session.”

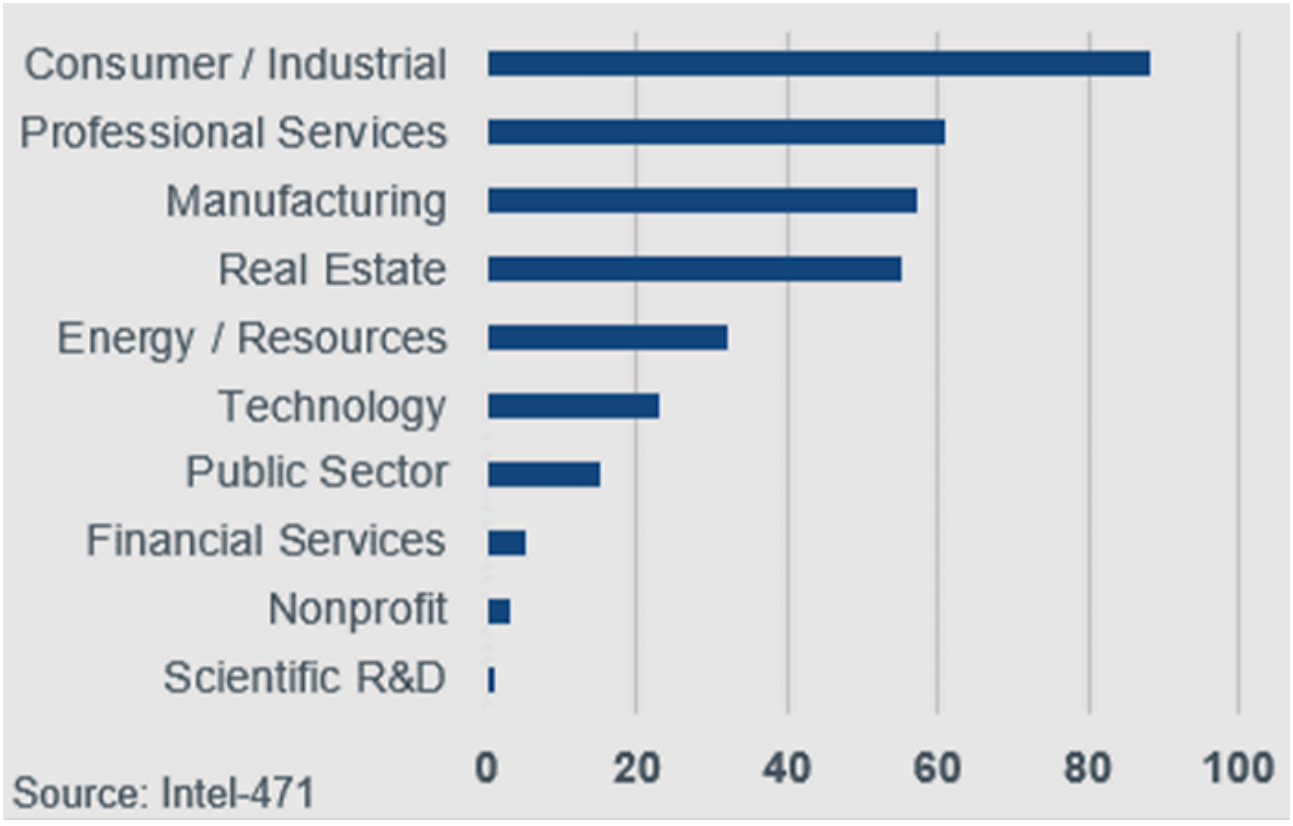
The vulnerability has been widely exploited by many types of attackers, including the PLAY Ransomware group, as shown in the case we investigate below.

PLAY Ransomware: The “Double Extortion” Group

PLAY Ransomware, also known as PLAY or PlayCrypt, is a ransomware-as-a-service (RaaS) group first observed in June 2022. The group both encrypts and exfiltrates victim data to demand a “double extortion” ransom to: (1) receive a decryption tool and (2) avoid data publication on its dark web data leak site. The group is known to primarily target small-to-medium sized organizations, managed service providers (MSPs) and government entities. Kroll’s analysis has found that, of the group’s known victims, PLAY heavily focuses on entities in North America (60%) and Europe (33%).



Play Ransom Note – ReadMe.txt



Industries Targeted by PLAY Group

PLAY is known to use intermittent or “partial” encryption on files to render the data unusable. Rather than encrypting entire files, PLAY targets only specific data segments of each processed file. This allows for faster

overall encryption and can decrease the detection rate of antivirus software using static analysis to detect ransomware infections.

Using Citrix Bleed Vulnerability to Target a Professional Services Firm

The following infographic illustrates activities observed by Kroll's Cyber Threat Intelligence (CTI) team following a four-day period after PLAY used the Citrix Bleed vulnerability to gain access to a professional services firm. Once inside the network, the threat actor conducted internal scouting to discover and enumerate domain accounts, trusted domains, permission groups and remote systems.
