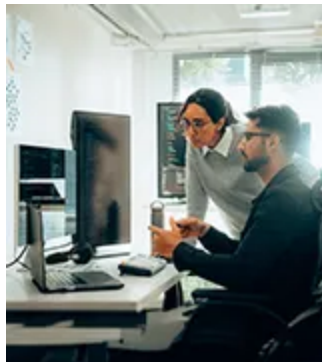


PLAY Ransomware Group Gains Access via Citrix Bleed Vulnerability

 kroll.com/en/insights/publications/cyber/play-ransomware-gains-access-citrix-bleed-vulnerability



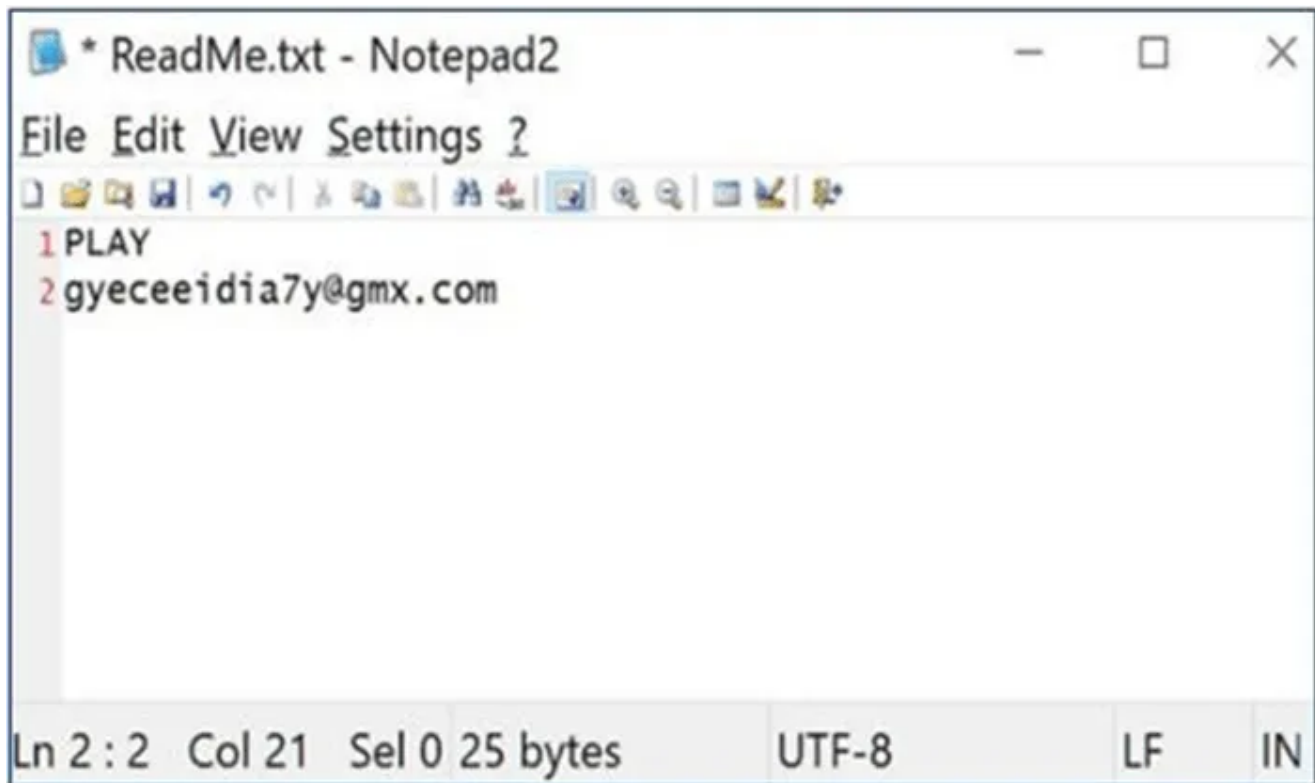
In November 2023, the Cybersecurity & Infrastructure Security Agency (CISA) published guidance for addressing vulnerability CVE-2023-4966, affecting Citrix NetScaler ADC and NetScaler Gateway. This vulnerability is also known as Citrix Bleed.

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.”

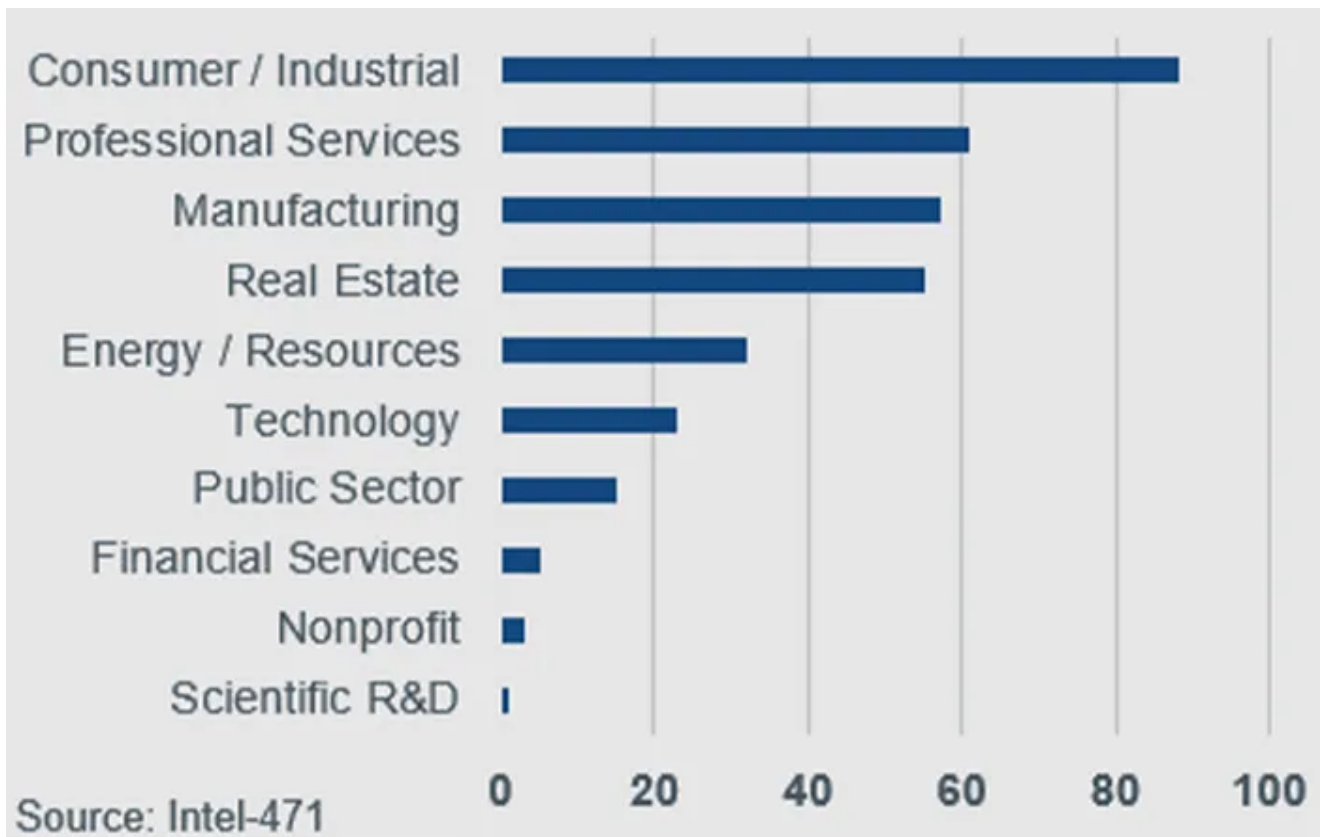
The vulnerability has been widely exploited by many types of attackers, including the PLAY Ransomware group, as shown in the case we investigate below.

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



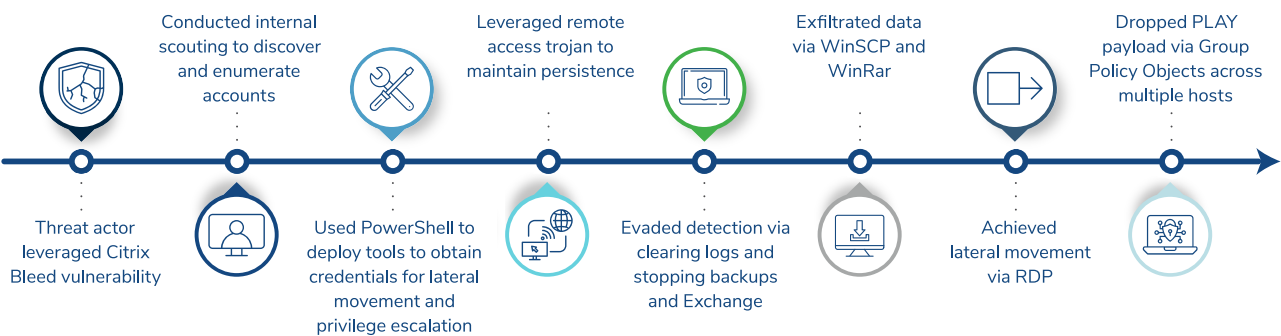
Industries Targeted by PLAY Group

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.

PLAY Ransomware Payload Delivery Process



The actor then used Powershell to deploy tools, including Mimikatz, which was leveraged to obtain credentials for lateral movement and privilege escalation. They maintained their persistence in the network via a remote access trojan and used several tactics to evade detection, such as clearing logs and stopping services (e.g., back-ups and Exchange). Data was exfiltrated from the system via WinSCP and compressed using WinRar. Lateral movement was achieved via RDP and the ultimate execution of the PLAY payload was delivered via Group Policy Objects across multiple hosts.

Kroll Intrusion Lifecycle Stage	ATT&CK Technique
---------------------------------	------------------

Initial Exploitation	T1133 External Remote Services
----------------------	--------------------------------

Internal Scouting	T1087.002 – Account Discovery – Domain Account T1482 – Domain Trust Discovery T1069.002 – Permission Groups Discovery – Domain Groups T1018 – Remote System Discovery
-------------------	--

Kroll Intrusion Lifecycle Stage

ATT&CK Technique

Toolkit Deployment

T1219 – Remote Access Software
T14189 – Service Stop (Back-ups, Exchange services)
T1059.001 – Command & Scripting Interpreter – PowerShell (for Toolkit Deployment)

Exfiltration

T1048.003 – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol (WinSCP)
T1560.001 – Archive via Utility (WinRar)

Lateral Movement

T1003.004 – OS Credential Dumping: LSA Secrets (Mimikatz)
T1021.001 – Remote Services – Remote Desktop Protocol

Mission Execution

T1486 – Data Encrypted for Impact
T1657 – Financial Theft

Key Recommendations

The similarities between ransomware variants provide opportunities for defenders to protect themselves against a number of different attackers by setting up overarching rules capable of detecting and defeating this type of activity. To defend against threat actors like PLAY, Kroll's [CTI](#) team advises organizations to take the following next steps:

- Enforce multi-factor authentication (MFA) for VPN access. Phishing-resistant MFA, such as FIDO, is essential to prevent phishing attacks. FIDO security keys or authenticators are the only devices that are effective at preventing phishing attacks.
- Prioritize patching for vulnerabilities that impact VPN appliances.
- Enable risk profiling or conditional access policies for remote access. This can deny access to a user attempting to log in under suspicious circumstances, and can also be configured to only allow limited access if the user's authentication context has elevated risk criteria.
- Enable role-based access control to enforce the principle of least privilege; only users requiring remote access to a resource should have it. Regularly audit access control policies to ensure only required access is provisioned.
- Ensure user accounts are not vulnerable to credential stuffing and password spraying by enforcing a banned password policy. The policy should ban passwords that are known to be weak, contain company or organizational words or passwords that have been discovered in previous breaches.

[Stay Ahead With Kroll >](#)

Cyber and Data Resilience

Incident response, digital forensics, breach notification, security strategy, managed security services, discovery solutions, security transformation.

[Cyber and Data Resilience](#)

Cyber Threat Intelligence

Threat intelligence are fueled by frontline incident response intel and elite analysts to effectively hunt and respond to threats.

[Cyber Threat Intelligence](#)

Incident Response and Litigation Support

Kroll's elite security leaders deliver rapid responses for over 3,000 incidents per year and have the resources and expertise to support the entire incident lifecycle, including litigation demands. Gain peace of mind in a crisis.

[Incident Response and Litigation Support](#)

Cyber Risk Retainer

Kroll delivers more than a typical incident response retainer—secure a true cyber risk retainer with elite digital forensics and incident response capabilities and maximum flexibility for proactive and notification services.

[Cyber Risk Retainer](#)

Malware Analysis and Reverse Engineering

Kroll's Malware Analysis and Reverse Engineering team draws from decades of private and public-sector experience, across all industries, to deliver actionable findings through in-depth technical analysis of benign and malicious code.

