APT5: Citrix ADC Threat Hunting Guidance

Executive summary

APT5 has demonstrated capabilities against Citrix® Application Delivery Controller™ (ADC™) deployments ("Citrix ADCs"). Targeting Citrix ADCs can facilitate illegitimate access to targeted organizations by bypassing normal authentication controls. As such, NSA, in collaboration with partners, has developed this threat hunting guidance to provide steps organizations can take to look for possible artifacts of this type of activity. Please note that this guidance does not represent all techniques, tactics, or procedures (TTPs) the actors may use when targeting these environments. This activity has been attributed to APT5, also known as UNC2630 and MANGANESE.

Introduction

NSA recommends organizations hosting Citrix ADC environments take the following steps as part of their investigation. Treat these detection mechanisms as independent ways of identifying potentially malicious activity on impacted systems. Artifacts may vary based on the environment and the stage of that activity. As such, NSA recommends investigating any positive result even if other detections return no findings.

File Integrity

A malicious actor enabling continued access will likely require modification to legitimate binaries. Therefore, NSA recommends organizations regularly check key executables in their environments for any deviations from the known good copies associated with their running version. Key executables are those binaries essential for proper execution of the Citrix ADC appliance. These files include, but may not be limited to: nsppe, nsaaad, nsconf, nsreadfile, and nsconmsg. The following command can be executed from a shell to facilitate this comparison:

```
cd /netscaler ; for i in "nsppe nsaaad nsconf nsreadfile nsconmsg"; do md5 ${i} ; done
```

The MD5 hashes should be compared to known good hashes from the vendor or hashes of the respective binaries from a known good copy downloaded from the vendor. Any deviation requires further investigation.

Additionally, the following command can indicate tampering by one APT5 technique. This is indicated by one line of output, but no output otherwise:

```
procstat -v $(pgrep -o -i nsppe) | grep "0x10400000 " | grep "rwx"
```

NSA also recommends that organizations take scheduled tech support bundles[1] and/or snapshots of their running environment and store them in an offline or otherwise immutable location to create a forensic history of systems. These backups can be used to compare running instances or to reconstruct events if suspicious activity is identified.

Behavioral Checks

In addition to any alterations of legitimate binaries, some of APT5's activities may be visible in various system logs. NSA recommends that organizations leverage off-device logging mechanisms for all system logs, to include `dmesg` and `ns.log`, and actively monitor them for the following activity:

- Instances of pb_policy appearing in logs without being linked to expected administrator activity.
    - The actors have been seen leveraging tools that run '`pb_policy`' twice. This creates the following logs in `ns.log`:

```
<local0.info> [hostname] pb_policy: Changing pitboss policy from X to Y
<local0.info> [hostname] pb_policy: Changing pitboss policy from Y to X
```

      Where X and Y are constant values for your system.

- Gaps in logs, or mismatches between logs on the device and in your remote logging solution.
- Legitimate user account activity without a corresponding record of a valid SAML token being issued by the identity provider for the environment.
- Unauthorized modification of user permissions.
- Unauthorized modifications to the crontab file and/or existence of suspicious file(s) in /var/cron/tabs/ and other locations.
    - Files related to this activity have been discovered in /tmp for some, but not all, impacted organizations.
    - The command below can assist in finding files that have been associated with this activity. While these files have not been discovered in all environments, their presence may be indicative of actor activity if discovered.

```
find / -type f -name "res*" | grep -E 'res($|\.[a-z]{3})$'
```

Detections

Provided below are YARA signatures that can be used to detect malware seen being used by the actors in this campaign:

```
rule tricklancer_a {

  strings:
    $str1 = "//var//log//ns.log" nocase ascii wide
    $str2 = "//var//log//cron" nocase ascii wide
    $str3 = "//var//log//auth.log" nocase ascii wide
    $str4 = "//var//log//httpaccess-vpn.log" nocase ascii wide
    $str5 = "//var//log//nsvpn.log" nocase ascii wide
    $str6 = "TF:YYYYMMddhhmmss" nocase ascii wide
    $str7 = "//var//log//lastlog" nocase ascii wide
    $str8 = "clear_utmp" nocase ascii wide
    $str9 = "clear_text_http" nocase ascii wide
  condition:
   7 of ($str*)
}

rule tricklancer_b {

  strings:
    $str1 = "nsppe" nocase ascii wide
    $str2 = "pb_policy -h nothing" nocase ascii wide
    $str3 = "pb_policy -d" nocase ascii wide
    $str4 = "findProcessListByName" nocase ascii wide
    $str5 = "restoreStateAndDetach" nocase ascii wide
    $str6 = "checktargetsig" nocase ascii wide
    $str7 = "DoInject" nocase ascii wide
    $str8 = "DoUnInject" nocase ascii wide
  condition:
    7 of ($str*)
}

rule tricklancer_c {

  strings:
    $str1 = "is_path_traversal_or_vpns_attack_request" nocase ascii wide
    $str2 = "ns_vpn_process_unauthenticated_request" nocase ascii wide
    $str3 = "mmapshell" nocase ascii wide
    $str4 = "DoUnInject" nocase ascii wide
    $str5 = "CalcDistanse" nocase ascii wide
    $str6 = "checkMyData" nocase ascii wide
    $str7 = "vpn_location_url_len" nocase ascii wide
  condition:
    5 of ($str*)
}
```

Mitigations

In the event that you have results from the above detection methodology, NSA recommends the following steps to mitigate the activity, to the extent applicable in your environment:

- Move all Citrix ADC instances behind a VPN or other capability that requires valid user authentication (ideally multi-factor) *prior* to being able to access the ADC.
- Isolate the Citrix ADC appliances from the environment to ensure any malicious activity is contained.
- Restore the Citrix ADC to a known good state.

Even if you do not have any indications of malicious activity, ensure that your Citrix ADC appliances are running a current version with the latest updates.

Conclusion

The indicators and context from this analysis can be used by organizations for defensive purposes against this malicious activity. NSA requests that any additional insights and/or discoveries be shared with the NSA Cybersecurity Collaboration Center in order to enhance understanding of this activity and so that it can be used to improve the overall security posture of the Defense Industrial Base, DoD, and USG.

Acknowledgements

NSA would like to acknowledge Citrix and additional industry partners for their contributions to this guide.

Additional information

[1] https://support.citrix.com/article/CTX227560/citrix-adc-logs-collection-guide

[2] https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/

Disclaimer of endorsement

Trademark recognition

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

General Cybersecurity Inquiries: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov