ПРОКУРАТУРА НА РЕПУБЛИКА БЪЛГАРИЯ

СОФИЙСКА ГРАДСКА ПРОКУРАТУРА

Пр. пр. № 8547/2020г.
Гр. София, 10.09.2021г.

ДО
ВСС
НА ВНИМАНИЕТО НА
КАЛИНА ЧАПКЪНОВА
ПРЕДСЕДАТЕЛ НА КОМИСИЯ
„ПРОФЕСИОНАЛНА КВАЛИФИКАЦИЯ И
ИНФОРМАЦИОННИ ТЕХНОЛОГИИ“
КЪМ ПЛЕНУМА НА
ВИСШИЯ СЪДЕБЕН СЪВЕТ
НА ВАШ ИЗХ. № ВСС-12988/2021г.

Във връзка с решение по протокол № 19/02.09.2021г. на комисия „Професионална квалификация и информационни технологии“ към Пленума на Висшия съдебен съвет, Ви уведомяваме, че разследването по досъдебно производство № 552/2020г. по описа на СО СГП, пр. пр. № 8547/2020г. по описа на СГП към момента не е приключило.

В хода на провежданото разследване са разпитани множество свидетели, приобщени са документи, изготвени са компютърно технически експертизи.

Вещите лица при изготвянето на техническо компютърната експертиза за функционирането на ЦССРД са установили, подозрителни събития за достъп до системата, за които считам, че следва да Ви уведомя. Събитията са разделени в няколко групи:

Подозрителни събития, свързани с липсващи записи или модификации: Историческите записи на уеб приложението са регистрирани в периода 12.09.2015г. до 13.04.2020г., като за определени дни липсват цели файлове, за една част от логовете има следи от модифициране на самите файлове, но не може да бъде установено какво точно е било редактирано.

Подозрителни събития свързани с Windows Event логове: В Windows System Event файла на сървъра с базата данни има следи от изтриването на исторически записи, свързани с три ключови Windows журнални файлове, което се случва на 31.01.2017г., при преглед на историческите заявки към уеб приложението не са открити следи свързани с популярни уеб атаки или други подозрителни действия. Windows Security Event журналните записи на двата сървара са запълнени с десетки хиляди неуспешни опити за достъп на 13.04.2020г., което автоматично е довело до изтриване на стари записи. Буди

подозрение фактът, че това така наречено наводняване на логове с нови записи се случва в деня, в който трябва да бъдат извлечени журнални записи от двете машини за изследване.

Подозрителни събития, свързани с исторически уеб заявки към приложението: Търсене на аномалии, свързани с потребителски имена установява, че няма нито един запис с конкретно потребителско име в периода 30.12.2016г. до 31.12.2017г., за сравнение, преди 30.12.2016г. има близо 16 милиона такива записи и след 31.12.2017г. близо 33 милиона.

На повече от 80 различни дати са открити данни за свързани с популярни вектори за кибератака, за които уеб сървърът на приложението връща HTTP статус код 200 успешна заявка. Това означава, че атакуващият е получил достъп до данните в приложението. Значителното количество пробиви в системата, както и големият период, в който те са имали място от 2015г. до 2020г., показва, че нейната сигурност е била силно пренебрегната, не е имало проследимост за осъществяваните опити за нерегламентиран достъп, не е съществувал механизъм за ежедневен контрол на сигурността на системата и данните в нея, като цяло не е имало яснота дали и какви данни са били достъпвани, променяни или изтривани.

Регистрирани са успешни свързвания на 13.04.2020г. с анонимен потребител от IP адреси регистрирани в Канада, Унгария, Хондурас, Казахстан, Русия, Саудитска Арабия, Хонконг и Великобритания.

Регистрирани са повече от 5000 заявки през октомври 2016г. от IP адрес на Pronet Telecom LTD, гр. Костинброд, свързани с популярен инструмент за SQL Injection. За 90% от заявките, уеб сървърът връща HTTP статус код 200 успешна заявка, тоест атакуващият е получил достъп до системата. Трябва да се отбележи, че данни за подобна атака са документирани в експертиза, свързана с кибератаката срещу НАП. IP адресът документиран там също е регистриран на оператора Pronet Telecom LTD.

15.09.2021г.
гр. София

ПРОКУРОР:
/М. Неңкова/

ПРОКУРАТУРА НА РЕПУБЛИКА БЪЛГАРИЯ

СОФИЙСКА ГРАДСКА ПРОКУРАТУРА

Пр. пр. № 8547/2020г.
Гр. София, 16.09.2021г.

ВИСШ СЪДЕБЕН СЪВЕТ
ВСС-12 988 17 09 21

П О С Т А Н О В Л Е Н И Е
гр. София, 16.09.2021г.

Марина Ненкова – прокурор при СГП, като се запознах с материалите по досъдебно производство № 552/2020г. по описа на СО СГП, пр. пр. № 8547/2020г. по описа на СГП,

У С Т А Н О В И Х:

Досъдебното производство е образувано на 01.04.2020г. и водено за престъпление по чл. 319а, ал. 1 от НК.

Наблюдаващият прокурор със справка рег. № 8547 от 14.09.2021г., във връзка с решение по протокол № 18/30.08.2021г. и справка № 8547 от 15.09.2021г., във връзка с решение по протокол № 19/02.09.2021г. на комисия „Професионална квалификация и информационни технологии“ към Пленума на Висшия съдебен съвет, е уведомил че в хода на провежданото разследване по досъдебното производство вещите лица при изготвянето на техническо компютърната експертиза за функционирането на ЦССРД са установили, подозрителни събития за достъп до системата.

Предвид изложеното и на основание на чл. 198, ал.1 от НПК,

П О С Т А Н О В И Х:

РАЗРЕШАВАМ разгласяване на информацията отразена в справка рег. № 8547 от 14.09.2021г. изпратена на ВСС и справка рег. № 8547 от 15.09.2021г. изпратена на комисия „Професионална квалификация и информационни технологии“ към Пленума на Висшия съдебен съвет, касаеща подозрителни събития за достъп до Централизираната система за случайно разпределение на делата.

НЕ РАЗРЕШАВАМ достъп и запознаване с материалите по делото на този етап от провежданото разследване.

Препис от постановлението да се изпрати на Калина Чапкънова – Председател на комисия „Професионална квалификация и информационни технологии“ към Пленума на Висшия съдебен съвет.

16.09.2021г.
гр. София

ПРОКУРОР:
/М. Ненкова/

Гр. София, 1040, бул. “Витоша” № 2, тел.02/9813344, факс 02/9808849, e-mail: sgp@prb.bg