Běloruský 9M318 SAM zasáhl UAV v testech

anna-news.info/belorusskaya-zur-9m318-porazila-bla-na-ispytaniyah

7. března 2023

Běloruský ZUR 9M318 zasáhl UAV během testování

07.03.2023 19:23:53 Maxim Tumbartsev
580 0 1

Pokračují předběžné testy běloruské protiletadlové řízené střely 9M318 pro protiletadlový raketový systém Buk-MB2. Při zkušebním startu rakety byl úspěšně zasažen bezpilotní letoun s proudovým motorem.

Uvádí to **materiál** Státního výboru pro vojenský průmysl Běloruska, zveřejněný v úterý 7. března 2023.

„Goskomvoenprom úspěšně provádí předběžné testy domácí protiletadlové řízené střely 9M318 vyvinuté pro běloruský systém protivzdušné obrany Buk-MB2," píše se v článku.

„V důsledku testů byly zasaženy vzdušné cíle, což byly bezpilotní letouny s proudovým motorem," dodali autoři materiálu.

9M318 byl vyvinut Minsk NPOOO OKB TSP, který je součástí Státního výboru pro vojenský průmysl Běloruska.

Protiletadlová řízená střela 9M318 je určena k ničení vysokorychlostních manévrovacích aerodynamických cílů, taktických balistických, plavebních, leteckých a protilodních střel a také vrtulníků v podmínkách intenzivních elektronických protiopatření.

Maximální dosah zasažení cílů je 70 kilometrů.

Pokud najdete chybu, vyberte část textu a stiskněte *Ctrl+Enter* .

V Kazachstánu začali identifikovat kybernetické špiony

07.03.2023 *18:23:59* Vlad Nikolajev
571 0 0

Kazašské speciální služby se zajímají o high-tech typy zločinů a podílejí se na jejich identifikaci a potlačování společně se Státní technickou službou JSC.

По официальным данным, раскрытым «Государственной технической службой», в прошлом году была прекращена деятельность хакерской группировки, осуществлявшей «негласный сбор документов из инфраструктур нескольких госорганов и организаций». «Кибергруппировка вела свою деятельность скрытно. Для закрепления позиций и кражи файлов, запускаемые вредоносные программы маскировались под легитимные процессы операционной системы или другие установленные программные обеспечения, подписанные реальными разработчиками. Они не вызывали подозрений у обычных пользователей и даже у системных администраторов».

По версии «ГТС», хакеры использовали уязвимость в защите — «0-day» уязвимости и ранее неизвестное для антивирусных лабораторий вредоносное программное обеспечение APT.

«Средства защиты информации не детектировали данное вредоносное программное обеспечение, что позволяло хакерам беспрепятственно вести деятельность. Злоумышленникам удалось скомпрометировать основные элементы информационно-коммуникационных инфраструктур государственных органов и организаций, в том числе были зафиксированы факты компрометации рабочих станций руководителей».

Помимо этого, киберпреступникии интересовались техническими данными самой инфраструктуры – «занимались сбором сетевых схем и учетных записей для дальнейшего продвижения».

По данным казахстанских спецслужб, хакеры действовали в интересах иностранного государства, однако какой именно, не сообщается.

Пресс-служба «ГТС», добавила, что «кибершпионы имели устойчивые каналы связи с инфраструктурами жертв, кроме которых имелся и арсенал резервных. Они вели высокотехнологичный кибершпионаж, при котором государственные организации не подозревали о наличии постороннего в своей инфраструктуре».

Внешнее вмешательство выявить удалось не сразу, поскольку антивирусное программное обеспечение выявляло только ранее известное вредоносное программное обеспечение, «электронные документы на компьютерах не пропадали, инфраструктура работала стабильно, и не возникало подозрений, что некие сторонние силы крадут сведения, циркулирующие в организации».

Отмечается, что «хакеров интересовала только «чувствительная» информация, они не крали все подряд». «ГТС» и КНБ, по согласованию с первыми лицами государственной власти, локализовали присутствие хакерской деятельности в казахстанских сетях. Отмечается, что «любые подозрительные активности воспринимались через призму нулевого доверия и тщательно проверялись, а также велась дальнейшая деятельность по зачистке, но уже более точечно, однако попытки возврата в инфраструктуру продолжились, а «противостояние продолжается по сей день, специалисты ведут постоянный мониторинг событий информационной безопасности».

Uvádí se, že bezpečnost informací v Kazachstánu zůstala zranitelná a útoky hackerských skupin vedly k „četným únikům důvěrných informací“. Například v září 2022 byl proveden DDoS útok na Kaznet, což vedlo k výraznému zpoždění internetového připojení.