СБУ заблокувала масову кібератаку спецслужб РФ на комп’ютерні мережі українських органів влади

ssu.gov.ua/novyny/sbu-zablokuvala-masovu-kiberataku-spetssluzhb-rf-na-kompiuterni-merezhi-ukrainskykh-orhaniv-vlady

Кіберфахівці СБУ виявили факти цілеспрямованого розповсюдження спецслужбами РФ шкідливого програмного забезпечення. Замовники планували вразити комп’ютерні мережі органів державної влади, місцевого самоврядування та об’єктів критичної інфраструктури.

Фахівці СБ України встановили, що на початку червня цього року було здійснено масову розсилку електронних листів із підміною адреси відправника. Повідомлення, зокрема, нібито від Управління патрульної поліції Києва містили шкідливі вкладення і були надіслані на адреси низки державних установ.

Шкідливе програмне забезпечення ініціює всталення клієнтської частини програми (засіб віддаленого адміністрування) на уражений комп’ютер. Це дає можливість іноземній спецслужбі віддалено здійснювати повний контроль над ПК. Встановлено контрольно-командні сервери , які в т. ч. знаходяться на території РФ.

Кіберфахівці СБ України рекомендують провести термінову перевірку інформаційно-телекомунікаційних систем, зокрема використовуючи індикатори, що опубліковані в платформі «MISP-UA» для виявлення їх можливої компрометації та вжиття оперативних запобіжних заходів.

Індикатори компрометації:

Назва файлу	sha1	sha256
Електронний запит.rar	ce4bf04087f7a011ef020fce81d00a393e37f679	ad15d2d402b03d0dc0fb55842c8159 b868448b8459b4c468b325c225393cfcf4
Електронний запит.pdf.rar	2ed6b02df189dbb1d07d76886957d5f7cdcd1463	23388220f257056878c17c5f4f44d1b1a8 478328bbbd14a450ea9bd141021763
Код доступу 030621.txt	e285193b27d5ea1c644973993415bbf9baad86a0	bf135c2003dee739fa69e7f2ee7d460d61 edddfff3747920ee0dbeb1c9f311b2
Електронний запит.pdf.exe	9480842a7a94c378ed27771c724bada5bdb758c4	e065fb7712e0c7a8ba1db464bd8d97443 b10d7162c9930fc5a9576c7871e4c78

Командно-контрольні сервери:

- 178.210.76.171 (Ru-Center, РФ),
- 176.9.64.70 (Hetzner, Німеччина)
- 185.231.68.230 (Zomro, Нідерланди)

Доменне ім’я:

«rmssrv.ru»

З’єднання здійснюється на порт 5651, 8080 та 81

Для очищення уражених комп’ютерів від зазначеного ШПЗ потрібно:

- зупинити сервіс з ім’ям Remote Utilities – Host
- видалити директорію C:\Program Files (x86)\Remote Utilities – Host\