**ЗАПОРІЗЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ**

**ДЕПАРТАМЕНТ ОСВІТИ І НАУКИ**

пр. Соборний, 164, м. Запоріжжя, 69107, тел. (061) 239-02-60; факс (061) 239-01-69
e-mail: osvita@zoda.gov.ua, код ЄДРПОУ 02143429

05.12.2017 № 4566/03.2-13 На №_____від_____

Керівникам органів управління освітою райдержадміністрацій, міськвиконкомів та ОТГ

Керівникам закладів освіти обласного підпорядкування

Ректорам, директорам вищих навчальних закладів I-IV рівнів акредитації

Директорам професійно-технічних навчальних закладів

Керівникам закладів освіти приватної форми власності

Щодо кібератак на державні інформаційні системи та збору окремих даних щодо цих систем

На виконання листа обласної державної адміністрації від 05.12.2017 № 10476/08-41 та за інформацією Служби безпеки України, наданою облдержадміністрації листом від 27.11.2017 № 59/53-4299н/т, Департамент освіти і науки облдержадміністрації повідомляє про можливу підготовку до чергової хвилі кібератак на інформаційні системи органів державної влади та місцевого самоврядування, державних підприємств, установ та організацій шкідливим програмним забезпеченням «Ransomware».

Крім цього, зафіксовано чисельні факти ураження державних інформаційних систем двома різновидами вірусу типу «PSCrypt».

Так, за результатами дослідження першого різновиду вірусу встановлено, що на електронні адреси надходять листи зі шкідливим вкладенням, яке є архівним файлом та містить фішингові документи типу «Рахунок на оплату» з javascript кодом всередині для завантаження файлу «load.exe» з мережі Інтернет (http://porohforeveyoung.ru:80/texting/load.exe, IP-адреса - 49.51.38.216, Китай).

Завантажений файл перейменовує себе та переміщається в наступне місце: \Users\%usemame%\AppData\Roaming\Microsoft\<random 8 numb>\<random 8 numb.exe> та додається до автозавантаження системи. Після цього завантажує з мережі Інтернет файл http://porohforeveyoung.ru:80/london/schosh.exe, зберігаючи його за адресою:

C:\Users\%usemame%\AppData\Local\Temp\@random 8 numb>.exe. Шкідлива програма «schosh.exe» робить автоматичне розповсюдження файлу «paxunok.html> по всім директоріям та шифрує файли на диску. Крім цього, цей файл створює два *.bat файли. Перший за адресою: C:\Windows\system32\cmd.exe /c C:\Users\ADMINI~l\AppData\Local\Temp\ t4AlE.tmp.bat, який, в свою чергу, проводить видалення тіньових копій «Windows» за допомогою команди «vssadmin.eve DeleteShadows/All/Quiet», видаляє гілку реестра «reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"/fl» і змінює атрибути файлу «attrib Default.rdp -s -h». Далі починає працювати другий *.bat файл «C:\Windows\system32\cmd.exe /c C:\Users\ ADMINI~l\AppData\Local\Temp\t276.tmp.bat», який також видаляє тіньові копії «Windows» за допомогою команди «vssadmin.eve DeleteShadows/All/Quiet», видаляє дві гілки реєстру: «reg delete "HKEY_CURRENT_USER\Software\ Microsoft\Terminal Server Client\Servers" /f», «reg delete "HKEY_CURRENT_USER\ Software\Microsoft\Terminal Server ClientYDDefault" /va /f», змінює атрибути файлу «attrib Default.rdp -s -h» та відновлює попередню гілку реєстру командою «regadd "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\ Servers"».

Водночас, другий різновид вірусу розповсюджується через електронні листи зі шкідливим вкладенням, що надходять на адреси місцевих державних органів влади. Вкладення є архівним файлом, який містить сканований паспорт, ІПН та довіреність із javascript кодом для завантаження файлу «svc.exe» з наступних посилань: http://poperediylimtkv.com/hiloddfvnc.exe (IP-адреса - 192.177.208.63, Україна); http://vkmodule.com.ua/images/svc.exe (IP-адреса - 212.26.135.68, Україна).

В подальшому даний файл самовиконується та шифрує дані на диску та залишає файл з реквізитами для оплати у сумі 3500 грн на Біткоїн гаманець.

Враховуючи викладене, для попередження інфікування та шифрування інформаційних систем органів державної влади та місцевого самоврядування, державних підприємств, установ та організацій Запорізького регіону через наявні можливості просимо осіб, відповідальних за забезпечення кібербезпеки виконати наступні першочергові заходи:

1. Забезпечити неприпустимість відкриття вкладень у підозрілих повідомленнях, а також у повідомленнях з нестандартним текстом, що спонукає до переходу на підозрілі посилання.
2. Системним адміністраторам і адміністраторам безпеки звернути увагу на фільтрування вхідних/вихідних інформаційних потоків, зокрема поштового веб-трафіку; внести доповнення до системи фільтрування та заблокувати доступ до «porohforeveyoung.ru», «poperediylimtkv.com», «book-house.org» та «vkmodule.com.ua».
3. Встановити патч, що виправляє вразливість CVE-2017-0263.
4. Оновити антивірусну базу даних до останньої доступної версії.
5. Унеможливити користувачам працювати з правами адміністратора.

6. Обмежити можливість запуску виконуваних файлів *.exe. на комп'ютерах користувачів з директорій %TEMP%, %APPDATA%.

Заступник директора департаменту –
начальник управління В.М. Захарчук

Євтушенко 239 04 96
Венгеров 224 64 43