МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

пр. Перемоги, 10, м.Київ, 01135, тел. (044) 481-32-21, факс (044) 481-47-96
E-mail: mon@mon.gov.ua, код ЄДРПОУ 38621185

Начальникам обласних, Київського міського управлінь освітою, ректорам (директорам) навчальних закладів усіх рівнів акредитації, керівникам державних підприємств та організацій, що знаходяться у сфері управління Міністерства освіти і науки України

Щодо протидії загрозам функціонуванню інформаційно-телекомунікаційним системам

У зв'язку із виявленням загроз сталому функціонуванню автоматизованих систем Міністерства освіти і науки України, установ та закладів освіти, державних підприємств, що знаходяться у підпорядкування Міністерства, виникла гостра потреба у ефективній протидії таким загрозам.

У зв'язку з цим, направляємо копію листа Служби безпеки України від 21.07.2017 № 30/1/1-5414 «Щодо загроз функціонуванню інформаційно-телекомунікаційних систем» для ретельного опрацювання та застосування наданих рекомендацій у подальшій роботі для забезпечення кібербезпеки ваших інформаційно-телекомунікаційних систем.

Додаток: згадане (на 5 арк.).

Заступник Міністра Р. В. Греба

Тр.

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки
вул. Володимирська, 33, м. Київ, 01601
Тел. (044) 256-91-64, E-mail: htcu@ssu.gov.ua
Код ЄДРПОУ 00034074

21.07.2017 № 30/1/1-5414

На №_____ від _____

Міністерство освіти і науки України
01135, Україна, м. Київ, просп. Перемоги, 10

Щодо загроз функціонуванню інформаційно-телекомунікаційних систем

Департаментом у ході виконання заходів із контррозвідувального захисту інтересів держави у сфері інформаційної безпеки виявлено загрози сталому функціонуванню автоматизованих систем державних органів влади, у тому числі Міністерство освіти і науки України.

27 червня 2017 року відбулась низка потужних кібератак на комп'ютерні мережі банківського, енергетичного, транспортного секторів, об'єктів зв'язку та інших важливих об'єктів критичної інфраструктури України, що викликало значний резонанс у суспільстві.

Ураження інформаційних систем відбувалось за допомогою модифікованого шкідливого програмного забезпечення (шифрувальника) під умовною назвою WannaCry2 або Petya.A / Petya.C., частина програмного коду якого раніше фіксувалась під час атаки на Укрзалізницю у грудні 2016 року. Об'єктами стали комп'ютери та серверне обладнання на операційній системі Windows. Відбувається повне або часткове шифрування файлів з розширенням doc, txt, exl.

Встановлено що, одним із шляхів поширення вірусу Petya.A було оновлення програмного забезпечення, призначене для документообігу, підготовки бухгалтерської та фінансової звітності.

У той же час, версія причетності російських спецслужб до здійсненої кібератаки залишається основною, оскільки після перерахунку необхідних коштів, уражені комп'ютери так і не були розблоковані, що підтверджує припущення про добре сплановану кібероперацію проти України напередодні Дня Конституції.

Аналіз здійснених кібератак свідчить про системні прорахунки з боку керівників органів державної влади та об'єктів критичної інформаційної інфраструктури у забезпеченні кібербезпеки їх інформаційно-телекомунікаційних систем.

Не зважаючи на здобутий досвід, надані СБ України рекомендації за наслідками кібератак на фінансовий сектор, яка мала місце наприкінці 2016 року, спостерігається [illegible] вання з боку відповідальних осіб

виконання базових вимог чинного законодавства у сфері технічного захисту інформації.

Поряд з цим, продовжують фіксуватися численні порушення персоналом об'єктів критичної інфраструктури базових вимог законодавства про захист інформації в інформаційно-телекомунікаційних системах, які створюють сприятливі умови для реалізації кіберзагроз. Зокрема:

- використання особистих технічних засобів у складі виробничих АС (USB-флеш накопичувачі);

- підключення до комп'ютерів підприємств технічних засобів із модулями передачі даних (Bluetooth, GSM тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;

- використання персоналом виробничих мереж для доступу до особистої електронної пошти, загальнодоступних та соціально-орієнтованих ресурсів мережі Інтернет;

- незахищеність ІТС за допомогою актуальних версій антивірусного програмного забезпечення.

Крім того, усвідомлюючи настання відповідальності за невжиття заходів із забезпечення кібербезпеки, окремі посадові особи несвоєчасно проінформували уповноважених суб'єктів забезпечення кібербезпеки щодо виявлених фактів вірусного ураження та намагалися привести функціонування комп'ютерних систем у штатний режим власними силами, що призвело до настання більш важких наслідків та ускладнило процес документування кіберінцидентів.

З метою протидії загрозам вчинення цілеспрямованих кібератак, а також блокуванню роботи автоматизованих систем Міністерства освіти і науки України, вважається за доцільне:

1. Забезпечити неприпустимість відкриття вкладень у підозрілих повідомленнях (у листах від адресатів, щодо яких виникають сумніви; наприклад: автор з невідомих причин змінив мову спілкування; тема листа є нетиповою для автора; спосіб, у який автор звертається до адресата, є нетиповим тощо; а також у повідомленнях з нестандартним текстом, що спонукають до переходу на підозрілі посилання або до відкриття підозрілих файлів – архівів, виконуваних файлів та ін.).

2. Системним адміністраторам та адміністраторам безпеки звернути увагу на фільтрування вхідних/вихідних інформаційних потоків, зокрема поштового й веб-трафіку.

3. Контактні електронні поштові скриньки, які зазначаються на офіційних веб-сайтах державних органів перевести з символьного типу до графічного, для ускладнення процедури автоматичного збору та аналізу відомостей потенційними зловмисниками в майбутньому.

4. Встановити офіційний патч Microsoft Security Bulletin MS17-010-Critical.

5. На мережевому обладнанні та груповими політиками заблокувати на системах та серверах порти 135, 445, 1024-1035 TCP.

6. В разі інфікування персонального комп'ютера не перезавантажувати систему.

7. Обмежити можливість запуску виконуваних файлів (*.exe) на комп'ютерах з директорій %TEMP%, %APPDATA%.

8. Для можливості відновлення зашифрованих файлів скористатися програмами ShadowExplorer або PhotoRec.

На сьогоднішній день, спеціалістами СБ України вивчається можливість дешифрування зашифрованих даних та встановлені ідентифікатори компрометації, необхідні для повної перевірки інформаційно-телекомунікаційних систем Міністерства освіти і науки України (додаток). Рекомендації щодо захисту комп'ютерів від кібератаки Petya Ransomware знаходяться за посиланням: https://ssu.gov.ua/ua/news/1/category/2/view/3659#sthash.sxaIJ8o9.fTyl G9AU.dpbs.

Крім того, відповідно до наказу Адміністрації Держспецзв'язку від 10.06.2008 № 94, яким затверджено "Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах", суб'єкти координації у разі виявлення спроби вчинення несанкціонованих дій, невідкладно інформувати Департамент безпеки інформаційно-телекомунікаційних систем Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

З метою своєчасного запобігання та припинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, просимо терміново інформувати співробітників ДКІБ СБ України щодо несанкціонованих дій відносно державних інформаційних ресурсів.

За результатами розгляду вказаного листа та вжитих заходів просимо поінформувати.

Додаток: ідентифікатори компрометації на 1 арк., не таємно.

Начальник Департаменту **О. Климчук**

Ідентифікатори компрометації

http://www.1c-sed.com.ua/downloads/9/zvit9.php
http://upd.me-doc.com.ua/
http://1c-sed.com.ua/

Дата та версія для оновлення M.E.Doc що містили бекдор
14.04.2017 01.175-10.01.176
15.05.2017 01.180-10.01.181
22.06.2017 01.188-10.01.189

Перелік веб-шеллів:
hxxp://me-doc.com.ua/TESTUpdates/med.php [1 KB 11/12/14 12:00:00 AM]
hxxp://me-doc.com.ua/TESTUpdates/medoc_online.php [16 KB 5/31/17 2:45:00 PM]
hxxp://me-doc.com.ua/TESTUpdates/MedocZarplata/index.old.php [1 KB 11/11/14 12:00:00 AM]
Веб-шелл просить авторизації - або по COOKIE або по параметру в URI.

Процеси, що відбувались на уражених ПЕОМ:
- на комп'ютері реєструється подія, Logon'е (код події 4624);
- на комп'ютері реєструється подія, Logon'у (код події 4672);
- на комп'ютері реєструється запуск служби PSEXESVC (код події 7045);
- на комп'ютері запускається процес типу:
%WINDIR%\rundll32.exe
"C:\Windows\perfc.dat",#1,
"%HOSTNAME%\%USERNAME%:%PASSWORD%"
- на комп'ютері створюється файл « C:\Windows\dllhost.dat », представляє собою PsExec;
- на комп'ютері в директорії «%TMP%» створюється виконуючий файл з довільним іменем.mimikatz;
- на комп'ютері реєструється багато подій, які свідчать про спроби авторизації з явно вказаними аутентифікаційними даними на інших комп'ютерах в мережі (код події 4648); при цьому, активність йде на мережеві порти 445/tcp або 139/tcp.

Зібрану інформацію шкідливий код збирає та записує в реєстр Windows в директорію HKEY_CURRENT_USER\SOFTWARE\WC.

Перелік Індикаторів, повязаних з активністю бекдорів (з квітня по т.ч.)

82.221.131.52
82.221.128.27
130.185.250.171
176.123.2.250
193.29.187.78
176.31.182.167
hxxps://bankstat.kiev.ua
hxxps://capital-investing.com.ua
hxxps://transfinance.com.ua
hxxps://invest-trade.com.ua
hxxps://banky.com.ua
Microsoft Help Service (имя службы для VBS-бекдора)
Windows Help Service (имя службы для VBS-бекдора)
37.59.10.101
api.telegram.org
149.154.167.200
149.154.167.197
149.154.167.198
149.154.167.199

У разі виявлення чи детектування системами інформаційної безпеки випадків ураження ПЕОМ чи інформаційної інфраструктури просимо повідомити за вказаними фактами ДКІБ СБ України на електронну адресу research@dis.gov.ua, з зазначенням

Ідентифікатори компрометації

http://www.1c-sed.com.ua/downloads/9/zvit9.php
http://upd.me-doc.com.ua/
http://1c-sed.com.ua/

Дата та версія для оновлення M.E.Doc що містили бекдор
14.04.2017 01.175-10.01.176
15.05.2017 01.180-10.01.181
22.06.2017 01.188-10.01.189

Перелік веб-шеллів:
hxxp://me-doc.com.ua/TESTUpdates/med.php [1 KB 11/12/14 12:00:00 AM]
hxxp://me-doc.com.ua/TESTUpdates/medoc_online.php [16 KB 5/31/17 2:45:00 PM]
hxxp://me-doc.com.ua/TESTUpdates/MedocZarplata/index.old.php [1 KB 11/11/14 12:00:00 AM]
Веб-шелл просить авторизації - або по COOKIE або по параметру в URI.

Процеси, що відбувались на уражених ПЕОМ:
- на комп'ютері реєструється подія, Logon'е (код події 4624);
- на комп'ютері реєструється подія, Logon'у (код події 4672);
- на комп'ютері реєструється запуск служби PSEXESVC (код події 7045);
- на комп'ютері запускається процес типу:
%WINDIR%\rundll32.exe
"C:\Windows\perfc.dat",#1,
"%HOSTNAME%\%USERNAME%:%PASSWORD%"
- на комп'ютері створюється файл « C:\Windows\dllhost.dat », представляє собою PsExec;
- на комп'ютері в директорії «%TMP%» створюється виконуючий файл з довільним іменем.mimikatz;
- на комп'ютері реєструється багато подій, які свідчать про спроби авторизації з явно вказаними аутентифікаційними даними на інших комп'ютерах в мережі (код події 4648); при цьому, активність йде на мережеві порти 445/tcp або 139/tcp.

Зібрану інформацію шкідливий код збирає та записує в реєстр Windows в директорію HKEY_CURRENT_USER\SOFTWARE\WC.

Перелік Індикаторів, повязаних з активністю бекдорів (з квітня по т.ч.)

82.221.131.52
82.221.128.27
130.185.250.171
176.123.2.250
193.29.187.78
176.31.182.167
hxxps://bankstat.kiev.ua
hxxps://capital-investing.com.ua
hxxps://transfinance.com.ua
hxxps://invest-trade.com.ua
hxxps://banky.com.ua
Microsoft Help Service (имя службы для VBS-бекдора)
Windows Help Service (имя службы для VBS-бекдора)
37.59.10.101
api.telegram.org
149.154.167.200
149.154.167.197
149.154.167.198
149.154.167.199

У разі виявлення чи детектування системами інформаційної безпеки випадків ураження ПЕОМ чи інформаційної інфраструктури просимо повідомити за вказаними фактами ДКІБ СБ України на електронну адресу research@dis.gov.ua, з зазначенням