

Згенеровано сертифікат від платформи Prometheus

PR Prometheus <certificates@prometheus.com.ua>
Кому: [redacted]@ukr.net *Підроблена адреса відправника*

Certificate.pdf
PDF 32 КБ

Шановний учаснику!

Ваш сертифікат готовий і знаходиться у вкладенні.
Автоматичне сповіщення від Prometheus.
Дякуємо за те, що навчалися разом із нами.

З повагою, Prometheus.

Попередній перегляд недоступний

<https://a3ufz.xsjdsb.icu/wp-json/prometheus-plus/certs-at-home/downloads>

☐	13:16	 FILE VIEW fileview.ukr.net	
☐	13:15	 Certificate.pdf file:///C:/Users/[redacted]/Downloads/Certificate.pdf	
☐	13:15	 укрнет - Поиск в Google google.com	
		certificate (1).zip	20.05.2026 13:16 Сти
		certificate.zip	20.05.2026 13:16 Сти
		Certificate (1).pdf	20.05.2026 13:16 Мис
		Certificate.pdf	20.05.2026 13:15 Мис

Общая информация

С весны 2026 года CERT-UA фиксирует многочисленные случаи отправки электронных писем среди правительственных организаций с использованием скомпрометированных учетных записей, в том числе с использованием предмета получения сертификатов через онлайн-платформу Prometheus.

Как правило, к вложению к электронной почте прикрепляется PDF-документ со ссылкой, переход которого приводит к загрузке архива ZIP, содержащего файл JS.

Упомянутый файл JS классифицируется как **OYSTERFRESH**, который обеспечивает отображение приманочных документов, запись в реестре операционной системы в запутанной и закодированной форме программного обеспечения **OYSTERBLUES**, а также загрузку и запуск компонента **OYSTERSHUK**, который действует как декодер для упомянутых OYSTERBLUES. Для декодирования, последовательного разворота строк, преобразования ROT13 и декодирования URL используются последовательно.

В свою очередь, OYSTERBLUES получает информацию о компьютере, включая его имя, учетную запись пользователя, версию ОС, время последней загрузки ОС и список расширенных процессов, после чего он отправляет эти данные на сервер управления с помощью запроса HTTP POST и ожидает ответа на JS-код, который выполняется с помощью функции *eval*.

Известно, что на следующем этапе компонент рамки Cobalt Strike может быть загружен на компьютер.

Как правило, для UAC-0057 (UNC1151) инфраструктура скрыта за Cloudflare, и значительная часть используемых доменных имен относится к TLD *.icu*.

Чтобы снизить вероятность реализации описанной киберугрозы, целесообразно применять известные базовые подходы к уменьшению поверхности атаки, в частности, ограничить возможность запуска *wscript.exe* для обычных учетных записей пользователей.

Графические изображения:

Рис.1 Пример электронной почты и PDF-вложения

Рис.2 Програмный засіб OYSTERFRESH

Рис.3 Програмный засіб OYSTERSHUCK

Рис.4 Програмный засіб OYSTERBLUES

Індикатори кіберзагроз

Файли:

d2b9c4a805c402dd697f23dd7c58a8c0 423960447b834691a80d884a7ed69476 20ecfa351609ade2bcc0f4ada30a532f fd488c39400a756456f0cb7ea90c92a0 29692522c85162302e95046839785364 279beb63fb7881bfd87aa35d6dbabe11 77fcc59a130a56e0eff282c9264159c3	ea8f6076e232efd9104ab282cd31bf249d0e6ddd6032b9a52d a7ae0604ce1521f31cdcb11ca24520588ae3e2823ad44fe570 65752ab1d78b215e70a543b790a1946b9e316474fce114bd20 b8c679550fedcddb1806ca9b7e39f0f6f10e21b666e069c1a0 859462bc01536e70ca024f0457f03f6f3f7833d13a032bf30e 9647ea4412ee4071dc18189e593595241eedd69c0a61bfe008 10a83a7e45de345d72d203e0ee6414f057b00d0bdd48bf2141
2002c7268ac90ae34012ac060f030377	b7b679cc1c4c72d9c6066cea7494d8372acf089b1a64b25ea4
ab1a67562a8c19aae22ad3db049d4b89 08a0d912c526a56be8185684f10a3c16 9905e21c43a4bcdb702281f078ef4a4f	904685ae9056856132b8a2837b41676fe67038558ce62b6100 bd680322ef5ebbf87cc3fad49702e948d206f85ae90eb334ac cf635a7a9753058eb92f839686149a1d8792d2f107e78c3175
3e79907378e5c0bc210ea0721bdcc612 0e8f5d6f44ad8a7b568b781bc78318ba 0c910962e4d6586db01877348cb6b928	662a78fbfe426fa0b7101a0eea0388752d623582d561379ac3 e210d8de1c092a4c714c547667e6a67ece801788639a5196e8 07ff534b425b09123577067d4aebcdec523acbec8d1b18017

00f20761abcc156451a3c560b0a6637a	b640a99ab2af33024af7217de718cc5fde9c44b819d4f0943a8
f1402bab6f695b14e1ca6a36439a5d33 ce5d94ca2a066e831f8fd8f995f29314 48c1066946723823bbada44097acbac6 fe0446756933f05a2bc312c51d50ce83	129125d09c785ad5d9f0cc730a2c2c08c957baa4a126907aa5e a21e15c7ff7a6e2cf8e28758f0be6718319f15ee5a8c225b9a! 6861ccc49586bc4e41b0947ac23a47409a29569540abb4bbf3! 83c1a1770944c8c01308c25d328abfea6bab663a7b320b9829f
e9e419c980b80c290872590731148793 d9f6a4f2f687249262af746f4575e156	2c1fbacc065176ac8baf8c78235997f36daad8806549357a76! 6c3744295c4e0cff59f9d0e982980cfe7e81c8b2421c7aa24b8
11590720540e152070274c2053da5c45 5cef2203c5b9f9d2df02409d938561af 38849b099db8a92b71325073ee5f3779	1cf6a8d2bc1b50ab687e6a74d027450593aeed525243e58a1e! 2752cc0ab3b011e2469ddebald91755555e6fd2047ec1a5427! 4095aecbea955b1441fef58cfc5f138a0c60823fb9a383949f4
dfd94f13aa23b7fe11f88ad35f767684 10alb41352dc90e5b6060eb88d1e843b aec2b8b354a54328b0943bde455a1d43 c71f5e1d08de6082dbb26712bcfab25e	0bb7cf24b3c830b1f86df26fb4f07a4b93b636de27864f120f! a019345bcb8cc34defac8e873087289b0feaeeb3f74d027dde! bb5dcf4147d03267a9be8ba43c09260c9e587cd2712b27d2ef! 378cb2a897aa9b9ac5cf14e2926b7da633a667fbfb86c6e888c
562e9a8f70196717cd0a6e5c6b2337ea 72116196bc5187f073e300e117d3e2ff 67565b9637d7005d9c4588d548d759a9 73ce230eb83d2547f502242067e4e3b2	845474a60e029ac8b361a89edfee507d59318c52c6e48f36e6! 0f2d779f41e25ca9c22a274d5de2301b9e6cef74efc0b235f9! 596e6e927d016caeede57a1639e847c91166dac6971173b0f3! 446cabdbdbf2c9724c92a0d40106c768b8dfd502356d4332a6c

Xocmosi:

```
%LOCALAPPDATA%\Google\Chrome\UserData\Profile\Extensions\ghbmnnjooekpmoecnnniinnbdlolhl
%APPDATA%\EdgeMachineData\
%PROGRAMDATA%\WindowsEdgeApp\
%APPDATA%\EdgeMachineData\EdgeTaskMachine.js
%APPDATA%\EdgeMachineData\MicrosoftEdgeUpdate.exe
%PROGRAMDATA%\WindowsEdgeApp\EdgeApp.exe
%PROGRAMDATA%\WindowsEdgeApp\EdgeSystemConfig.dll
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Blue\Oyster'
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftEdgeUpdate'
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\WindowsEdgeStartup'
MicrosoftEdgeUpdateTaskMachine
```

Мережеві:

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
hXXps://a3ufz.xsjsdb[.]icu/wp-json/prometheus-plus/certs-at-home/downloads
hXXps://a3ufz.xsjsdb[.]icu/wp-json/prometheus-plus/devops_and_kubernetes/marketing-ana
hXXps://a3ufz.xsjsdb[.]icu/wp-json/prometheus-plus/veteran-circle/system-team-managemen
hXXps://advancedaisolutionsforeveryone.alsi[.]icu/study/mathematics/calculus/practice-p
hXXps://alerteddatalistsclients.alertapp[.]icu/c7b054f1/files/uploaded/3000108836624430
```

hXXps://best-seller.lavanille[.]buzz/drawing/equipment
hXXps://easiestnewsfromourpointofview.algsat[.]icu/uploads/certs/4e5d6fasd234dfdf/scrip
hXXps://easiestnewsfromourpointofview.algsat[.]icu/uploads/files/SGVsbG8sIHdvcmxkIQ==/
hXXps://ifo-jupyter.natter[.]icu/wp-content/plugins/elementor/assets/lib/eicons/css
hXXps://mickeymousegamesdealer.alexavegas[.]icu/wp-content/uploads/2026/03/certificate
hXXps://mickeymousegamesdealer.alexavegas[.]icu/wp-content/uploads/2026/03/tags
hXXps://productionsamplesoftheyear.cgdirector[.]icu/wp-content/plugins/contact-form-7/r
ifo-jupyter.natter[.]icu
natter[.]icu
a3ufz.xsjdsb[.]icu
xsjdsb[.]icu
easiestnewsfromourpointofview.algsat[.]icu
algsat[.]icu
best-seller.lavanille[.]buzz
lavanille[.]buzz
mickeymousegamesdealer.alexavegas[.]icu
alexavegas[.]icu
alerteddatalistsclients.alertapp[.]icu
alertapp[.]icu
productionsamplesoftheyear.cgdirector[.]icu
cgdirector[.]icu
advancedaisolutionsforeveryone.alsi[.]icu
alsi[.]icu

[Попередня](#)

[Лікарні, органи місцевого самоврядування та оператори FPV - у фокусі кластера кіберзагроз UAC-0247 \(UAC-0244\)](#)