НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

О целенаправленной рассылке ВПО под видом легитимного ПО Trueconf

ALRT-20240724.1 | 24 июля 2024 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Описание угрозы	По каналам НКЦКИ получены сведения о массовой рассылке фишинговых электронных писем, содержащих вложение в виде PDF-файла с именем "ВКС 25.07.2024.pdf". Указанный файл замаскирован под письмо с атрибутикой Министерства энергетики Российской Федерации, информирующее о запланированной видеоконференции, на которую необходимо зарегистрироваться по ссылке hxxps://e-trueconf[.]ru/c/782687231[.]html. После перехода по указанной фишинговой ссылке начинается процесс загрузки вредоносного файла “trueconf.ru.exe”. В случае запуска этого файла происходит внедрение модулей ВПО, маскирующихся под легитимные службы Windows. Основной функционал ВПО — сбор информации с зараженного хоста. ВПО осуществляет взаимодействие по протоколу HTTP с доменным именем cr87986[.]tw1[.]ru.
Рекомендации по нейтрализации угрозы	1. Обновить используемые антивирусные средства. 2. Проверить на ресурсах ИТС и в сетевом трафике наличие индикаторов компрометации (раздел “IOC”). 3. Провести мероприятия, нацеленные на повышение бдительности и осведомленности сотрудников вашей компании в части противодействия фишинговым атакам и иным методам социальной инженерии. 4. При получении электронных писем с приложенными файлами производить их проверку антивирусными средствами или средствами динамического анализа. В случае выявления признаков компрометации ИТС вашей организации просим сообщить об этом в НКЦКИ.
IOC	1. Почтовый адрес: novikovsa@ggnpsale.ruВложение к почтовому письму “ВКС 25.07.2024.pdf” (SHA-256: b362c56a150c46d6a977a35b1f3879c5c169f101a2e88679a84bd289e6c64761) 2. Домены и почтовые адреса в этих доменах: ggnpsale[.]ru e-trueconf[.]ru mvdpmr[.]ru mvdpnr[.]rue-mail-password[.]ru e-connection[.]ru

3. Центр управления ВПО:

Доменное имя: cr87986[.]tw1[.]ru
IP-адрес: 5.23.51.23

4. URL-адрес:

hxxps://e-trueconf[.]ru/c/782687231[.]html
hxxp://cr87986[.]tw1[.]ru/L1nc0ln.php

5. Коллекция имен ВПО и их контрольные суммы:

trueconf.ru.exe

SHA-256: 216d45e0ce2aa886d9732008a2c70bdd1e80e1711ff1f71f0f5c4aa3ae941772
SHA-1: b453d3df84fea2d4d0c51bb2a757327d7887c411
MD5: 96a7ce8bda9e00ed4341638aeac4e08c

Файл trueconf.ru.exe является контейнером для следующих файлов:

- clamer.exe (Trojan-Spy.MSIL.Stealer.gfj)
  Контрольные суммы:
  SHA-256: 6dc66244c1a36581963301fc48149f775ad5c773e315fc28fd864339471c4962
  SHA-1: 4e2b168965d2972597401901e9fd8d8265bf40cd
  MD5: 38710d3374787dbb59c3690f332b722a

- dwatj.exe, conhost.exe, smss.exe
  Контрольные суммы:
  SHA-256: 763c1f21d22b7215d36e2dbd52d141d71d9e540c19f631f63f151c283b91f0d8
  SHA-1: b06b7e8c83df5980802e6b04d4639de0550c2ff4
  MD5: 365630241faf63fc7ab0c37bcac6e426