

## Der Staatliche Dienst für Sonderkommunikation und Informationsschutz hat vor neuen Cyberangriffen gewarnt

29.01.2022

Das ukrainische CERT-UA Emergency Response Team, das innerhalb des Staatlichen Dienstes für Sonderkommunikation und Informationsschutz tätig ist, hat vor versuchten Cyberangriffen auf ukrainische Organisationen und Einrichtungen gewarnt, die das legitime Programm Remote Utilities nutzen. Dies berichtete das Zentrum für strategische Kommunikation und Informationssicherheit am Samstag, den 29. Januar.

*Das ist eine maschinelle Übersetzung eines Artikels aus der [Onlinezeitung Korrespondent.net](#). Die Übersetzung wurde weder überprüft, noch redaktionell bearbeitet und die Schreibung von Namen und geographischen Bezeichnungen entspricht nicht den sonst bei [Ukraine-Nachrichten](#) verwendeten Konventionen.*

???

Das ukrainische CERT-UA Emergency Response Team, das innerhalb des Staatlichen Dienstes für Sonderkommunikation und Informationsschutz tätig ist, hat vor versuchten Cyberangriffen auf ukrainische Organisationen und Einrichtungen gewarnt, die das legitime Programm Remote Utilities nutzen. Dies berichtete das Zentrum für strategische Kommunikation und Informationssicherheit am Samstag, den 29. Januar.

„Die massiven Cyberangriffe, die am 13. und 14. Januar stattfanden, dauern an“, teilte das Zentrum in einer Telegrammbotschaft mit.

Demnach läuft seit Freitag ein Mailing mit Gerichtsanhängen. Obwohl die Mails von offiziellen Adressen der Justiz stammen, sind die Anhänge gefälscht und die Links in der E-Mail mit Schadsoftware versehen.

„Das Problem wird durch die Tatsache verschärft, dass die Mails von den echten Mailservern der Justiz stammen. So passieren die E-Mails Spamfilter und sind vertrauenswürdig. Es ist möglich, dass nur einzelne Gerichtsadressen kompromittiert sind, obwohl nicht ausgeschlossen werden sollte, dass der gesamte Mailserver kompromittiert wurde“, heißt es in dem Bericht.

Da die Rolle der E-Mail als offizielles Kommunikationsmittel in Gerichtsverfahren in der Ukraine gesetzlich gestärkt wurde, wird sich nach Ansicht der Agentur „ein solcher Angriffsvektor in Zukunft weiter entwickeln.

Es wird auch festgestellt, dass die E-Mails einen Link zu passwortgeschützten RAR- und/oder ZIP-Archiven (z. B. Trial Request #997836477463567677822.rar\_pass\_123.zip) enthalten, die auf den öffentlichen Diensten Google Drive und DropMeFiles abgelegt sind.

Wenn der Empfänger ein solches Archiv herunterlädt und entpackt, werden Remote Utilities auf seinem Computer installiert. Dies ermöglicht dem Empfänger einen geheimen Fernzugriff auf das Gerät durch Dritte. Die Fähigkeit des Programms, die Aktivitäten nach einem Neustart des Computers zu aktualisieren, wird durch die Erstellung des RManService gewährleistet.

„Solche Cyberangriffe sind eine systematische Aktivität, die sich gegen ukrainische Regierungsbehörden (aber nicht nur) richtet und von CERT-UA unter der Kennung UAC-0096 verfolgt wird“, so der Dienst.

Um die Malware zu entfernen, empfiehlt der Staatssicherheitsdienst, den RManService zu stoppen, das Verzeichnis %PROGRAMFILES%\Remote Utilities Host\ zu löschen, den Registrierungsschlüssel HKLM\SOFTWARE\Usoris&

Übersetzung: **DeepL** — Wörter: 360

Namensnennung-Keine kommerzielle Nutzung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland Sie dürfen:

- das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen
- Bearbeitungen des Werkes anfertigen

Zu den folgenden Bedingungen:

**Namensnennung.** Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen (wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt).

**Keine kommerzielle Nutzung.** Dieses Werk darf nicht für kommerzielle Zwecke verwendet werden.

**Weitergabe unter gleichen Bedingungen.** Wenn Sie dieses Werk bearbeiten oder in anderer Weise umgestalten, verändern oder als Grundlage für ein anderes Werk verwenden, dürfen Sie das neu entstandene Werk nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

- Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter welche dieses Werk fällt, mitteilen. Am Einfachsten ist es, einen Link auf diese Seite einzubinden.
- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

**Haftungsausschluss**

Die Commons Deed ist kein Lizenzvertrag. Sie ist lediglich ein Referenztext, der den zugrundeliegenden Lizenzvertrag übersichtlich und in allgemeinverständlicher Sprache wiedergibt. Die Deed selbst entfaltet keine juristische Wirkung und erscheint im eigentlichen Lizenzvertrag nicht.

Creative Commons ist keine Rechtsanwaltsgesellschaft und leistet keine Rechtsberatung. Die Weitergabe und Verlinkung des Commons Deeds führt zu keinem Mandatsverhältnis.

Die gesetzlichen Schranken des Urheberrechts bleiben hiervon unberührt.

Die Commons Deed ist eine Zusammenfassung des Lizenzvertrags in allgemeinverständlicher Sprache.