CYBERCRIME COMPETENCE CENTER NEWS
INFORMATIONEN · TIPPS · RECHERCHEN · BERICHTE

- **Sollte dieser Newsletter bei Ihnen nicht einwandfrei angezeigt werden, beachten Sie bitte die beigefügte Version als PDF.**

Massive Welle von Datenverschlüsselungen (Ransomware)

Art der Bedrohung

Verschlüsselung von Privat- und Firmendaten mit anschließender Erpressung zur Bezahlung eines Geldbetrages mittels BitCoin zur Erlangung des Entschlüsselungs-Codes / Programms

Modus Operandi

Derzeit werden nahezu täglich Schadensmeldungen in Bezug auf die Verschlüsselung von Computer- und Serverdaten durch so genannten „Ransomware[1]“ von Unternehmen an die C4-Meldestelle bekannt gegeben.

Es erscheint daher unerlässlich, neuerlich vor der aktuellen Welle von Mails mit gefährlichem Inhalt, insbesondere angeblichen „papierlosen Rechnungen“, zu warnen. Es ist dabei unerheblich, von welchem augenscheinlichen Absender die E-Mails stammen, sie haben alle nur eines gemeinsam, den Empfänger zum Herunterladen und Öffnen einer als Rechnung oder Zustellverständigung getarnten Anlage zu verleiten.

Nach dem Öffnen der Anlage wird durch das Schadprogramm weiterer Schadcode nachgeladen und findet in weiterer Folge die Verschlüsselung des Computersystems sowie aller Netzwerkdaten, für welche der betroffene Benutzer eine Zugriffsberechtigung hatte, statt.

Eine Wiederherstellung oder Entschlüsselung der Daten ohne den erforderlichen „Key“ ist auf Grund der hohen Qualität der Verschlüsselung derzeit nahezu unmöglich. Für die Erlangung desselben wird eine „Lösegeldforderung“ (Ransom) in Form von BitCoins[2], bezahlbar über Tornetz[3]-Zugänge in das Dark-Net[4], gefordert.

Wir raten derart geforderte Zahlungen nicht zu leisten. Die Bezahlung sollte das allerletzte Mittel

---

[1] Quelle Wikipedia: https://de.wikipedia.org/wiki/Ransomware

[2] Quelle Wikipedia: https://de.wikipedia.org/wiki/Bitcoin

[3] Quelle Wikipedia: https://de.wikipedia.org/wiki/Tor_(Netzwerk)

[4] Quelle Wikipedia: https://de.wikipedia.org/wiki/Darknet

sein, wenn Sie auf die verschlüsselten Daten keinesfalls verzichten können. Besser beraten sind Sie, wenn Sie zeitgerecht die finanziellen Mittel in eine entsprechende BackUp-Lösung und Strategie sowie Sicherheitssoftware investieren.

Zudem können unter Umständen von der Schadsoftware in der Windows-Registry gespeicherte Zugangsdaten und Passwörter, unter anderem für FTP-, Remote- und E-Mail-Accounts ausgelesen und per Mail an eine vom Täter adressierte Stelle im Internet versandt werden. Bei den aktuellen Versionen der Schadsoftware erfolgt ebenfalls zu diesem Zeitpunkt die Löschung der sog. „Shadow Copy", welche bei Vorversionen dieser Schadsoftware in manchen Fällen noch eine Teilwiederherstellung der Daten zuließ.

Derzeit aktuell werden in Massen-E-Mails „Rechnungen" zugestellt, welche den Eindruck erwecken sollen, dass sie von A1 (Bild 1) oder dem Verbund (Bild 2) stammen, jedoch kann es sich bei jeder zugestellten „Rechnung" um gezielt übermittelte Schadsoftware handeln. Insbesondere bei Zustellverständigungen von DHL, UPS und der Post, bei welchen ebenfalls ein Download der „Verständigung" stattfinden soll, ist besondere Vorsicht geboten.

Bei der aktuell am häufigsten auftretenden „Ransomware" handelt es sich um „Cryptolocker", gefolgt von „Cerber", jedoch treten auch immer wieder ältere und bereits bekannte Varianten in Erscheinung.

Eine neue Herausforderung stellt zudem die Ransomware SATAN[5] dar, welche vom „Entwickler" als kostenloses Baukasten-System zur Verfügung gestellt wird. Lediglich eine Beteiligung am erpressten Lösegeld in der Höhe von 30% wird gefordert, ermöglicht aber auch nicht versierten und mit dem Dark-Net nicht verhafteten Nutzern den Einsatz von Schadsoftware. Somit kann generell von einer massiven Steigerung der künftigen Bedrohung durch so genannte Verschlüsselungs-Trojaner ausgegangen werden, wobei derzeit schon anzunehmen ist, dass die Dunkelziffer der gemeldeten Schadensfälle sehr hoch ist.

Empfohlene Vorgangsweisen:

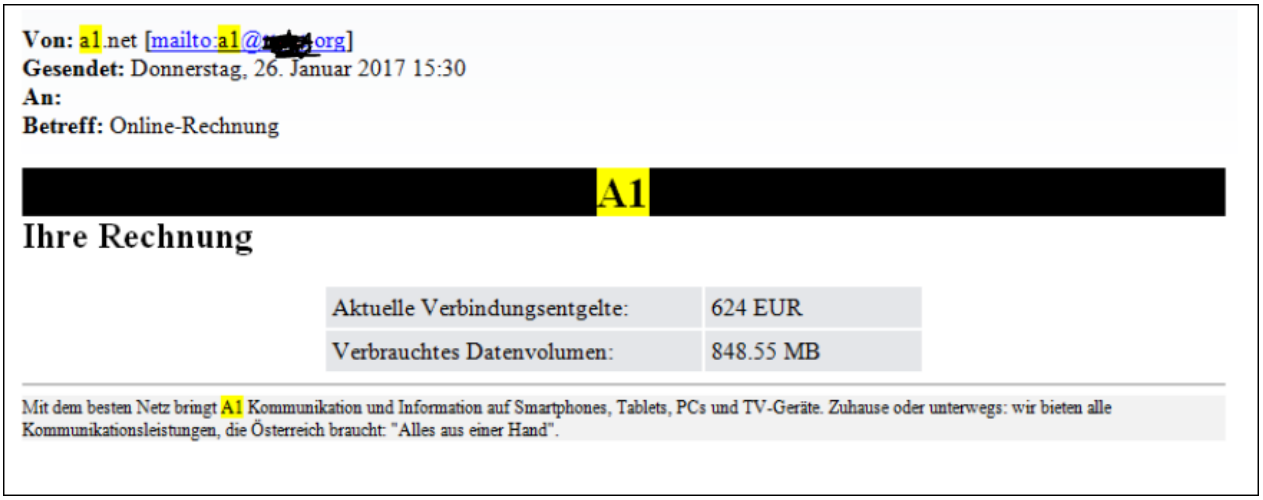
- Seien Sie vorsichtig beim Erhalt von E-Mails, deren Absender Sie nicht kennen oder wenn Sie keine entsprechenden Mitteilungen erwarten.
- Kontrollieren Sie nach Möglichkeit die tatsächliche Absenderadresse, achten Sie auf Ungereimtheiten. Bei angeführten Weblinks legen Sie den Mauszeiger über den entsprechenden Link, ohne diesen zu aktivieren. Sollte die Web-Link-Adresse aufscheinen, kontrollieren Sie, ob diese tatsächlich zu einem vertrauenswürdigen Absender gehört.
- Achten Sie auf die Schreibweise und Rechtschreibung solcher Nachrichten, Täter verwenden hier gerne Übersetzungsprogramme, wodurch die Bedrohung leichter erkennbar ist.
- Öffnen Sie keinesfalls Ihnen unbekannte Dateianhänge, ohne sich vorher von deren „Echtheit" zu überzeugen. Insbesondere bei übermittelten „Rechnungen", sollten Sie derzeit besondere Vorsicht walten lassen.
- Wenn Sie sich unsicher sind, öffnen Sie derartige Dateien in einer gesicherten Umgebung (Sandbox, virtuelle Systeme mit Option auf Rücksetzung) oder bedienen Sie sich unterstützender Seiten im Internet (z.B. Virustotal.com).
- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe

[5] Quelle futurezone.at: https://futurezone.at/digital-life/satan-kostenlose-ransomware-aus-dem-baukasten/242.664.890

Passwörter für verschiedene Accounts und Anwendungen.

- Legen Sie sich eine BackUp-Strategie für Ihre Daten zu. Trennen Sie das BackUp-Medium nach der Sicherung vom System und lösen Sie Share-Links zu BackUp Servern nach erfolgter Sicherung wieder auf, um ein Übergreifen durch die Schadsoftware zu verhindern.
- Beschränken Sie die Benutzerrechte der jeweiligen User so weit als möglich und arbeiten Sie nur unter dem Administrator-Account, wenn dies unbedingt notwendig ist.
- Wir raten den geforderten Betrag nicht zu bezahlen! Wenn eine Wiederherstellung der Daten für Sie unumgänglich ist, gibt es dafür aber derzeit kaum Alternativen. Eine Garantie auf eine solche, selbst nach Bezahlung, gibt es nicht, jedoch liegt es im „Geschäftsmodell" der Täter, einer solchen nachzukommen! Eine letztendliche Entscheidung darüber müssen Sie für sich selbst treffen.
- Beachten Sie die Sicherheitshinweise und Tipps, für einen Sicheren Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: http://www.bmi.gv.at.

Bild 1:



Von: a1.net [mailto:a1@[redacted].org]
Gesendet: Donnerstag, 26. Januar 2017 15:30
An:
Betreff: Online-Rechnung

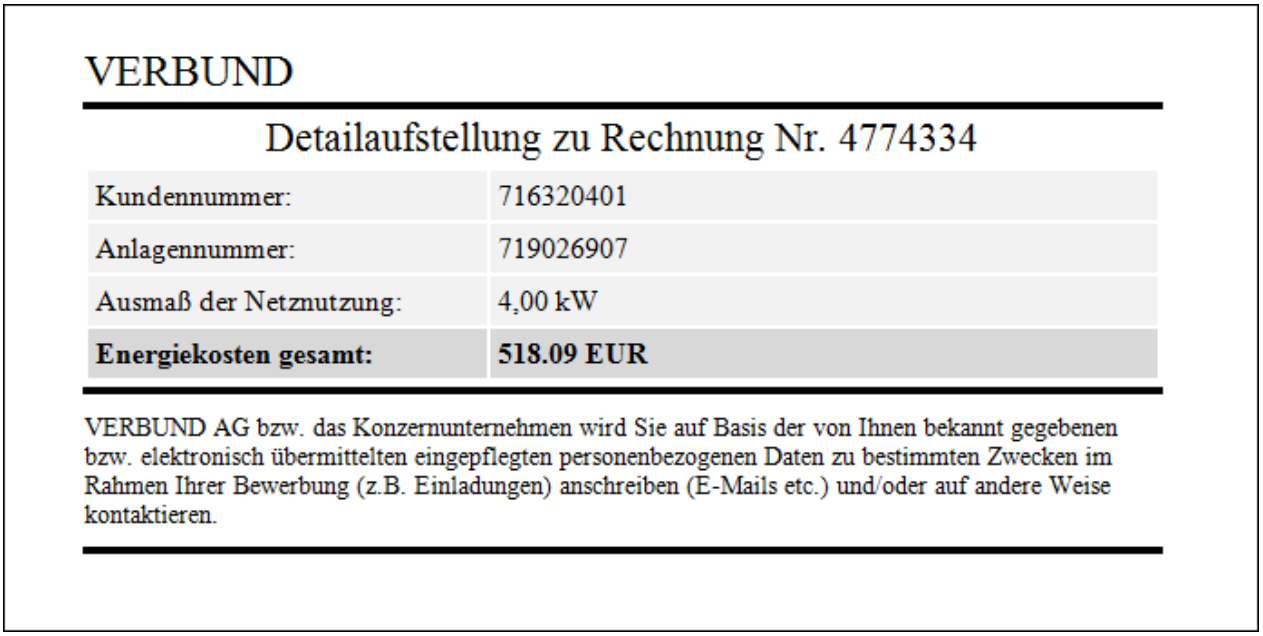
[redacted]A1[redacted]

Ihre Rechnung

Aktuelle Verbindungsentgelte:	624 EUR
Verbrauchtes Datenvolumen:	848.55 MB

Mit dem besten Netz bringt A1 Kommunikation und Information auf Smartphones, Tablets, PCs und TV-Geräte. Zuhause oder unterwegs: wir bieten alle Kommunikationsleistungen, die Österreich braucht: "Alles aus einer Hand".

Bild 2:



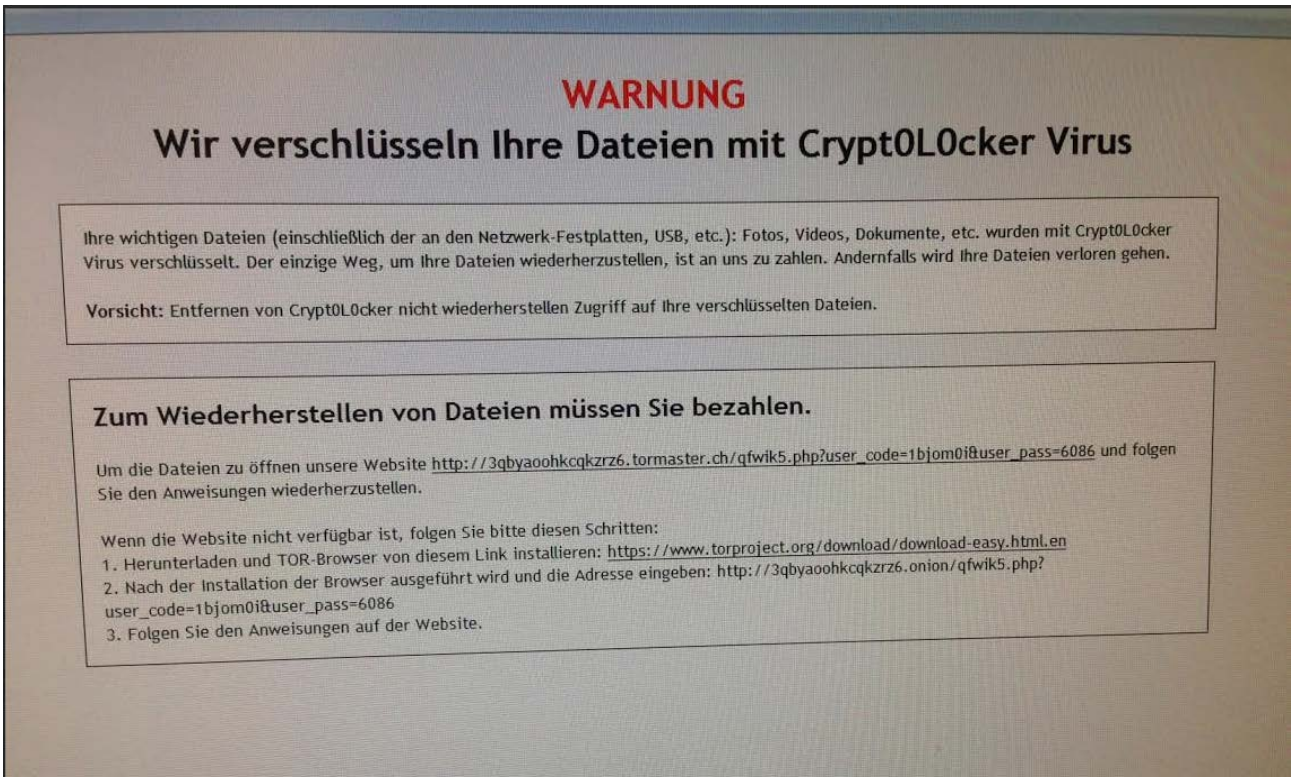
VERBUND

Detailaufstellung zu Rechnung Nr. 4774334

Kundennummer:	716320401
Anlagennummer:	719026907
Ausmaß der Netznutzung:	4,00 kW
Energiekosten gesamt:	**518.09 EUR**

VERBUND AG bzw. das Konzernunternehmen wird Sie auf Basis der von Ihnen bekannt gegebenen bzw. elektronisch übermittelten eingepflegten personenbezogenen Daten zu bestimmten Zwecken im Rahmen Ihrer Bewerbung (z.B. Einladungen) anschreiben (E-Mails etc.) und/oder auf andere Weise kontaktieren.

Nach der Verschlüsselung erscheint die Aufforderung zur Bezahlung:



Weiterführende und erklärende Links:

Wikipedia – CryptoLocker (englisch): was ist CryptoLocker und dessen Geschichte (https://en.wikipedia.org/wiki/CryptoLocker)

Watchlist-Internet – Falsche Verbund-Rechnung: Aufbereitung und Warnung vor dem gegenständlichen Phänomen (https://www.watchlist-internet.at/gefaelschte-rechnungen/falsche-verbund-rechnung-verbreitet-schadsoftware/)

BleepingComputer.com - Spyware And Malware Removal Guides Index (englisch): Listung und Informationen zu den einzelnen (Crypto-)Malware-gruppen: https://www.bleepingcomputer.com/forums/t/171335/spyware-and-malware-removal-guides-index/?p=1307244

MalwareHunterTeam.com – ID Ransomware (englisch): Möglichkeit der Feststellung, welche Ransomware für die Verschlüsselung eingesetzt wurde (https://id-ransomware.malwarehunterteam.com/index.php)

Kaspersky.com – Ransoware Decryptor: Informationen und die Möglichkeit der Wiederherstellung von verschlüsselten Dateien in Bezug auf einige (ältere) Verschlüsselungs-Trojaner (https://noransom.kaspersky.com/)

CERT.at – Empfehlungen zu Ransomware: https://www.cert.at/static/downloads/specials/20160325-cert.at-report-ransomware.pdf

No More Ransom Projekt: Initiative zur Wiederherstellung von Daten nach Angriffen mit Ransomware (https://www.nomoreransom.org/)

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG