Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

Deutsche Institutionen über TerminalFix-Kampagne kompromittiert

Mehrstufiger Angriff führt zu Datenabfluss und Ransomware-Installation

BITS-B Nr. 2026-287419-1032, Version 1.0, 04.09.2026

Kritikalität*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Bitte prüfen Sie selbstständig, für welche Stellen in Ihrer Organisation die hier genannten Informationen relevant sind und leiten Sie das Schreiben entsprechend weiter – sofern die TLP-Einstufung dies zulässt.

Sachverhalt

Im August 2026 wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) über die Kompromittierung des Netzwerks einer staatlichen Institution informiert. Anschließende Analysen zeigen, dass der Tathergang mit Beobachtungen von mehrstufigen Angriffen übereinstimmt, die Microsoft kürzlich als TerminalFix-Kampagne in seinem Blog vorgestellt hatte [MS26]. Der Ablauf dieser Attacken stellt sich basierend auf dem Microsoft Blog sowie dem BSI bekannten Erkenntnissen wie folgt dar:

1. Internetnutzer rufen eine kompromittierte Webseite auf, auf die sie z.B. mittels Phishing/Social-Engineering geführt werden oder von Nutzern regelmäßig besucht werden (Water-Holing). Dort fordert man sie dazu auf, eine CAPTCHA Prüfung auszuführen. Dabei wird suggeriert, dass das Ausführen eines Befehls in Windows Terminal oder PowerShell notwendig ist. Er wird hierzu ein schädlicher PowerShell-Befehl in die Zwischenablage kopiert, der dann vom Nutzer als Befehl ausgeführt werden muss.
2. Der schädliche Befehl lädt ein ZIP-Archiv herunter, entpackt es und führt dieses aus. Zeitgleich wird die angeblich erfolgreiche Bearbeitung des o.g. CAPTCHAs angezeigt, um Misstrauen vonseiten des Opfers zu verhindern.

* 1 / Grau: Maßnahmen sollten in absehbarer Zeit erwogen werden. Keine wesentlichen Beeinträchtigungen zu erwarten.
2 / Gelb: Maßnahmen müssen zeitnah ergriffen werden. Temporäre Beeinträchtigungen des Regelbetriebs möglich.
3 / Orange: Maßnahmen müssen unverzüglich ergriffen werden. Massive Beeinträchtigung des Regelbetriebs möglich.
4 / Rot: Maßnahmen müssen sofort ergriffen werden. Geschäftskritische Beeinträchtigung möglich.

3. Im ZIP-Archiv befinden sich sowohl eine ausführbare als auch eine maliziöse .dll-Datei, die per DLL-Sideloading zusammenwirken.
4. Die DLL führt im Hintergrund weitere PowerShell-Aktivitäten aus und lädt PNG-Dateien von der Angreifer-Infrastruktur. Diese Bilder enthalten weiteren Schadcode, der von der Malware auf dem System zusammengesetzt wird.
5. Die Malware nistet sich persistent auf dem Zielsystem ein. Hierfür werden
    1. ein Registry-Run-Eintrag,
    2. eine z.B. stündlich wiederkehrende Aufgabe sowie
    3. versteckte Daten und Verzeichnisse angelegt.
6. Es kommt zum Ausspähen der Infrastruktur. Untersucht werden Domänen, Rechtevergaben, das Active Directory, betriebene Server, vorhandene Backup-Systeme uvm. Nach aktuellem Kenntnisstand dient dieser Schritt zur Analyse, welchen Wert das kompromittierte System für weitere Angriffe haben könnte.
7. Der Angreifer richtet ggf. direkt Online-Speicher z. B. in der Azure-Cloud, um Daten später dorthin exfiltrieren zu können. Hierzu nutzen Angreifer dann auch von den Cloud-Anbietern herausgegebene Werkzeuge wie azcopy im Falle von Azure.
8. Ein Reverse-Tunnel wird eingerichtet. Hierzu installieren die Angreifer eine Python-Laufzeitumgebung. Die dazugehörige .py-Datei baut über TLS auf Port 443 und WebSockets eine Verbindung zur Infrastruktur der Täter auf. Durch den Angreifer in der Python-Laufzeitumgebung übertragene und ausgeführte Befehle werden u. U. nicht protokolliert.

Beim BSI eingegangene Meldungen weisen zusätzlich darauf hin, dass im Rahmen dieser Angriffe versucht wurde, Ransomware zu installieren und im Rahmen von Double Extortion auch Daten auszuleiten bzw. die Opfer im Anschluss mit der Veröffentlichung zu erpressen.

Aus beim BSI eingegangenen Meldungen geht der Einsatz der Malware LoremIpsumLoader (aka AxolotLoader) im Rahmen der Angriffskampagne hervor [BV26a][BV26b]. Nach Kenntnislage des BSI wird diese Malware derselben finanziell motivierten Gruppe zugeordnet, welche für die Ransomware und Leak-Seite Rhysida verantwortlich ist.

Bewertung

Die beobachteten TerminalFix-Angriffe stellen eine Weiterentwicklung der bereits bekannten ClickFix-Attacken dar. Während Letztere in der Vergangenheit in der Regel lediglich einzelne Rechner kompromittierten, besteht TerminalFix eine weitere Möglichkeit, tiefer in Netzwerke einzudringen sowie Vertraulichkeit, Verfügbarkeit und Integrität der IT ganzer Organisationen zu beeinträchtigen. Für IT-Sicherheitsverantwortliche ergibt sich somit die Herausforderung, beide Angriffstechniken unterscheiden zu können und bei Vorfällen passende Gegenmaßnahmen anzustoßen.

Nach derzeitigen Erkenntnissen wird die aktuelle Kampagne von Tätern aus dem Cybercrime-Bereich durchgeführt. Diese handeln opportunistisch und sind ausschließlich finanziell motiviert. Ein Zusammenhang mit staatlichen bzw. politisch motivierten Akteuren konnte bislang nicht hergestellt werden. Das für das Captcha verwendete Javascript konnte in historischen Daten auf mehreren Hundert Webseiten festgestellt werden.

Die Ransomware und Leak-Seite Rhysida wird der finanziell motivierten Gruppe Vice Spider (aka Vice Society, White Nefas, White Hekate, DEV-0832, Vanilla Tempest) zugeordnet. Nach Kenntnislage des BSI ist die Gruppe seit mindestens Mitte 2021 aktiv. Anfänglich nutzen die Angreifer die Leak-Seite Vice Society und eine Vielzahl von Ransomware-Familien, welche zumeist nicht von der Gruppe selbst entwickelt wurden. Seit Juni 2023 nutzt die Gruppe nahezu exklusiv die Ransomware Rhysida und die zugehörige Leak-Seite.

Nach Kenntnislage eines kommerziellen Dienstleisters des BSI folgt in 92 % der Fälle auf die Nennung auf der Leak-Seite Rhysida auch eine Datenveröffentlichung. Dabei vergehen zwischen Nennung auf der Leak-Seite und Veröffentlichung von gestohlenen Daten im Durchschnitt 11 Tage. Eine Auswertung der Leak-Seite zeigt keinen signifikanten Fokus auf Deutschland als Region. Die Angreifer zeigen einen starken Fokus auf den Bildungs- und Gesundheitssektor. Der Verwaltungssektor ist mit etwas Abstand zu den erst genannten Sektoren unter den Top 5 der meist angegriffenen Sektoren auf der Leak-Seite Rhysida.

Maßnahmen

Microsoft weist in seinen Blog insbesondere auf folgende Schutzmaßnahmen hin:

- Einsatz aktueller Network- und Endpoint-Protection
- Verwendung von Browsern mit SmartScreen-Unterstützung, um Phishing o.ä. erkennen zu können
- Nutzung von Cloud-basierter Malware-Erkennung
- Aktivierung von PowerShell Script Block Logging zur Dokumentation von PowerShell Prozessen
- Betrieb von PowerShell im Constrained Language Mode, um die Ausführung gefährlicher PowerShell-Befehle zu verhindern
- Betrachtung kompromittierter Rechner als Einstiegspunkte ins Netzwerk für lateral Movement, nicht als isolierte Systeme.

Sollten Sie Anzeichen für eine Kompromittierung feststellen können, bitten wir um eine sofortige Kontaktaufnahme mit dem BSI über die etablierten Kommunikationskanäle. Falls bereits ein Datenabfluss oder eine Ransomware-Infektion stattgefunden hat, bietet das BSI zusätzlich Unterstützung auf seiner Webseite an [BSI20].

Referenzen

[BSI20] BSI - Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall

[MS26] Microsoft - TerminalFix campaign deploys a reverse tunnel through multistage intrusion:
https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/

[BV26a] BlueVoyant - Lorem Ipsum Malware: Trojanized MS Teams Installers Deliver Multi-Stage Loader and Backdoor:
https://www.bluevoyant.com/blog/lorem-ipsum-trojanized-microsoft-teams-installers-multi-stage-loader-backdoor

[BV26b] BlueVoyant - Lorem Ipsum Revisited:
https://www.bluevoyant.com/blog/orem-ipsum-clickfix-rapid-brigantine

Versionsverlauf

Version 1.0 — 04.09.2026

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.