r-tec cyber security

an accompio company

Cyber Security Lagebericht 2025

Reale Angriffe, echte Einsätze – Erkenntnisse aus 123 Vorfällen im r-tec Cyber Defense Center

Maurice Fielenbach

Inhaltsverzeichnis

Lagebericht 2025

Vom Trend zur Maßnahme: Was diesen Bericht anders macht

Mit dem Lagebericht 2025 verfolgt r-tec das Ziel, die zentralen Erkenntnisse aus insgesamt 123 bewältigten Cybersicherheitsvorfällen kompakt und praxisorientiert darzustellen. Anstelle eines weiteren breit angelegten Trenddokuments werden in diesem Dokument, anhand realer, anonymisierter Einsatzberichte unseres Computer Emergency Response Teams, Learnings und Handlungsempfehlungen aus kuratierten Vorfällen herausgearbeitet und verdichtet.

Das Format ist bewusst nicht als repräsentatives Gesamtbild angelegt. Vielmehr ist es unser Anspruch, durch die Auswahl exemplarischer Fälle ein breites Spektrum möglicher Bedrohungsszenarien abzudecken, von Phishing-Kampagnen über Ransomware bis hin zu Insider-Bedrohungen. Die Fälle wurden so zusammengestellt, dass Organisationen jeder Größe und Branche relevante Erkenntnisse für ihre eigene Sicherheitsstrategie ableiten können sollten. Dieser Bericht hat seinen Zweck erfüllt, wenn er Leser dabei unterstützt, Widerstandsfähigkeit aufzubauen, bevor der nächste Vorfall den Alltag übernimmt.

Wir haben drei unabhängige Experten gebeten, den Bericht vorab einzusehen und fachlich einzuordnen. Ihre Einschätzungen bestätigen, was wir im Alltag beobachten – und schärfen den Blick für das, worauf es ankommt.

Begleiten Sie uns auf eine Reise durch die Bedrohungslandschaft des vergangenen Jahres – von Ransomware-as-a-Service und Malvertising über Cloud-Insider-Fälle bis hin zu jahrzehntealter Malware, die in Produktionsnetzen wieder aufwacht.

»Wissenstransfer aus der Einsatzpraxis ist eine relevante Ressource in der Cybersecurity. Wer reale Angriffsmuster transparent dokumentiert und daraus übertragbare Handlungsempfehlungen ableitet, stärkt nicht nur einzelne Organisationen, sondern hebt das Sicherheitsniveau eines ganzen Ökosystems. Genau das leistet dieser Bericht.«

Prof. Dr. Norbert Pohlmann,

Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes - eco.

Executive Summary

Cyberangriffe sind längst Alltag, nicht nur für IT-Fachkräfte und -Entscheider, sondern für nahezu jede Organisation. Während sich Ziele und Intentionen von Bedrohungsakteuren über Jahrzehnte kaum verändert haben, entwickeln sich jedoch Vorgehensweisen, Toolchains sowie Quantität und Qualität der Angriffe spürbar weiter. Dieser Lagebericht bündelt Kernerkenntnisse aus über 120 Cybersecurity-Incidents, die das r-tec CERT 2025 bewältigt hat und bildet damit eine belastbare Grundlage, um Entwicklungen greifbar zu machen, die zugleich exemplarisch für breitere Trends stehen.

Eine zentrale Beobachtung 2025 war der sichtbare Einfluss von KI. Large Language Models erleichtern die Skalierung professioneller Phishing-Kampagnen, unterstützen Social Engineering durch Voice- und Deepfake-Ansätze und beschleunigen Malware- sowie Exploit- und Zero-Day-Entwicklung. Mit agentischen Ansätzen werden zudem einzelne Angriffsschritte zunehmend teilautomatisiert. Dadurch schwankt die technische Ausprägung einzelner Infektionsketten teils stärker, die insgesamt höhere Schlagzahl verändert jedoch spürbar den Incident-Response- und SOC-Betrieb.

Darüber hinaus hat 2025 erneut gezeigt, dass einzelne, siloartig betriebene Security-Lösungen nicht mehr ausreichen. Ein wirksamer Schutz entsteht erst durch einen Layered-Security-Ansatz, der blinde Flecken einzelner Komponenten ausgleicht und durch Rückfall-Mechanismen stabil bleibt. Konkret bedeutet das, dass zum Beispiel EDR, SIEM, Firewall, Identity Protection, Dark Web Monitoring, Angriffsfrüherkennung und Threat Hunting als Gesamtsystem zusammenwirken müssen, damit aus Signalen zeitnah Maßnahmen werden, um somit ein hohes Schutzniveau zu erreichen.

Auch der Perimeter blieb ein wiederkehrender Schmerzpunkt, nicht zuletzt durch die anhaltend hohe Zahl veröffentlichter Schwachstellen in extern erreichbaren Appliances und Gateways. Gleichzeitig erschwert die schier endlose Flut neuer, innovativer Lösungsansätze den Fokus auf Bewährtes.

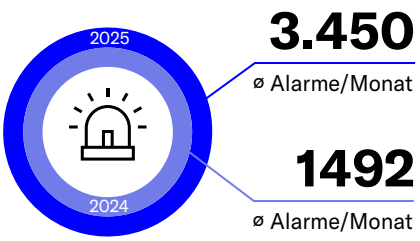
Auch 2025 prägten Supply-Chain-Vorfälle die öffentliche Diskussion, unter anderem im Zusammenhang mit Kampagnen wie Shai Hulud oder React2Shell. Im Vergleich zum Vorjahr war erneut ein erhöhtes Aufkommen entsprechender Ereignisse und Prüfbedarfe zu verzeichnen. Bemerkenswert war dabei, dass der operative Aufwand häufig weniger durch nachgewiesene Ausnutzung entstand, sondern durch unklare Betroffenheit in der eigenen Lieferkette.

Und zuletzt bleibt der Faktor Mensch ein zentrales Einfallstor. Neben klassischem Phishing etablierten sich 2025 insbesondere ClickFix-Angriffe, bei denen Nutzer durch geschickt inszenierte Anleitungen Schadcode eigenhändig ausführen, sowie Malvertising über Suchanzeigen, das Nutzer in alltäglichen Routineentscheidungen trifft. Auch gezielte Ansprachen über gefälschte Bewerberprofile und Insider-Risiken durch unzureichend gesteuerte Dienstleisterzugänge prägten das Bild.

Über das r-tec Cyber Defense Center

Das r-tec Cyber Defense Center vereint Security Operations Center (SOC) und Computer Emergency Response Team (CERT) und stellt damit sowohl die proaktive, kontinuierliche Überwachung seiner Kundenumgebungen als auch die ad-hoc Reaktion auf Sicherheitsvorfälle rund um die Uhr sicher.

Grafik 1 – Teamgrößen



Grafik 2 – Alarme

Das r-tec SOC überwacht Kundeninfrastrukturen auf Basis verschiedener Technologien und bewertet eingehende Alarme aus unterschiedlichen Sicherheitslösungen. Durch Automatisierung werden Alarme angereichert und priorisiert, wo möglich werden erste Containment-Maßnahmen eingeleitet. Bestätigte Sicherheitsvorfälle werden anschließend sowohl an die betroffene Organisation als auch an das r-tec CERT eskaliert.

135.100
Geräte im Monitoring

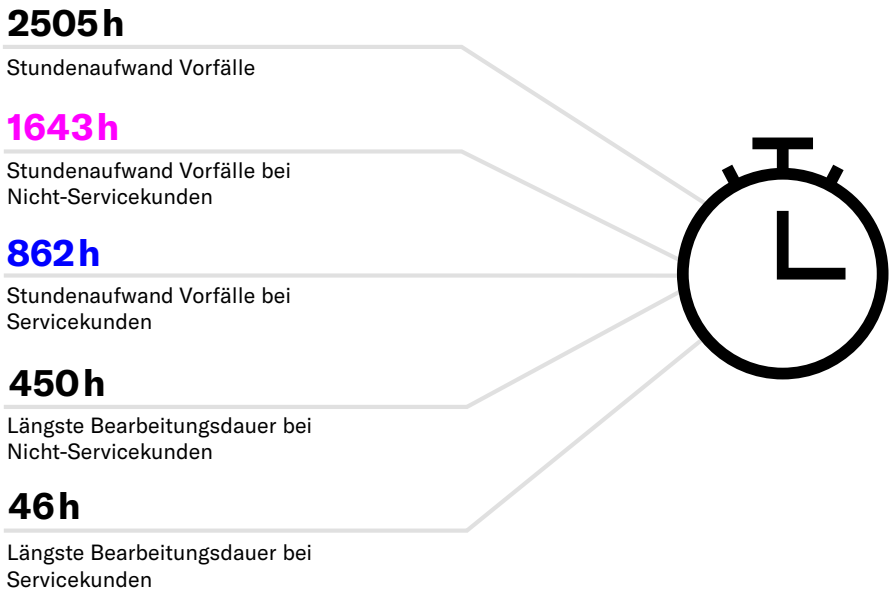
3,9TB
SIEM Logvolumen/Tag

Grafik 3 - Geräte

Keyfacts

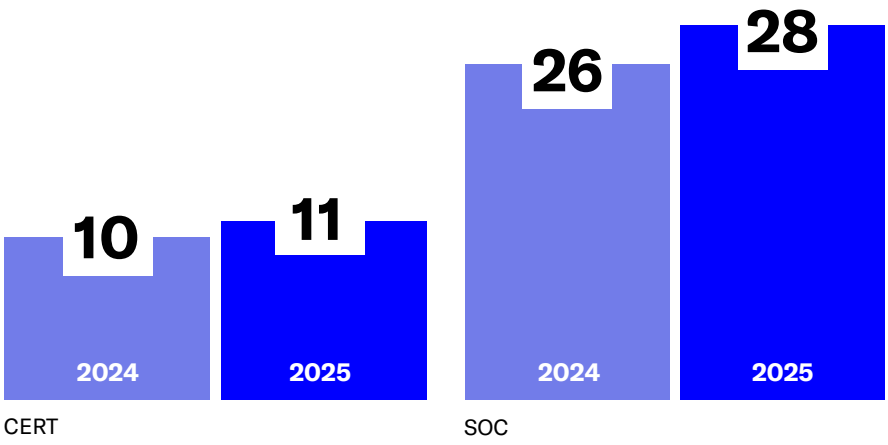
Das CERT agiert hingegen als 24/7-Reaktionsteam. Es übernimmt sowohl bestätigte Vorfälle aus dem SOC als auch Incident-Response-Einsätze für Kunden mit entsprechenden Leistungen – von Forensik und Malware-Analyse bis Krisenmanagement und Wiederanlaufbegleitung.

Bearbeitungsdauer von Security Incidents



Grafik 4 – Bearbeitungsdauer von Security Incidents

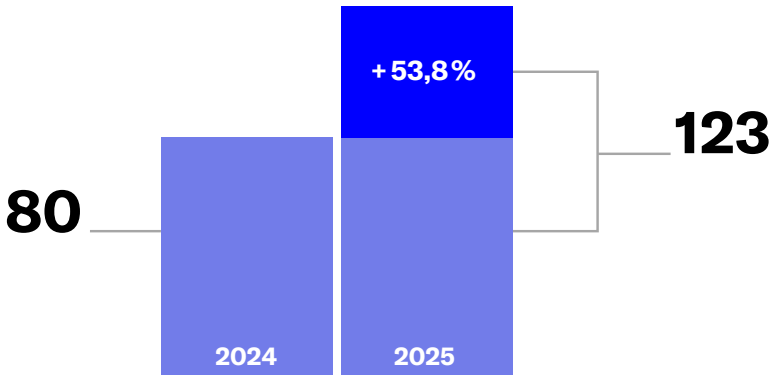
Teamgrößen



Grafik 5 – Veränderungen Teamgrößen

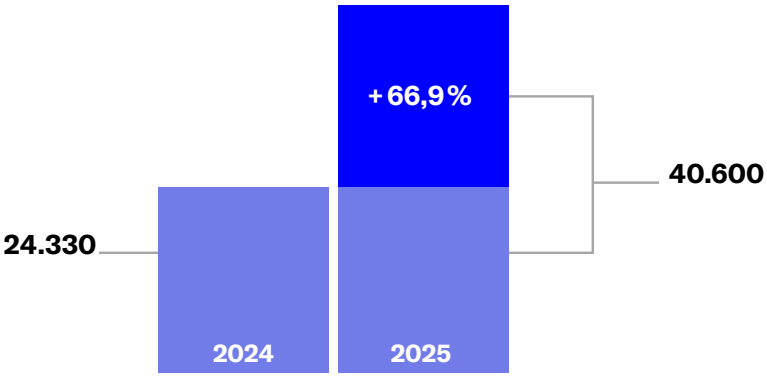
Keyfacts

Vorfälle



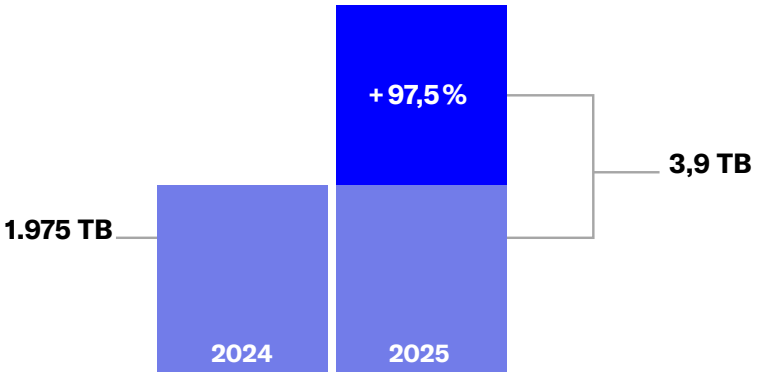
Grafik 6 – Prozentuale Veränderungen Vorfälle

Geräte im EDR-Monitoring



Grafik 7 – Prozentuale Veränderungen Geräte

SIEM-Logvolumen / Tag



Grafik 8 – Prozentuale SIEM-Volumen

Lageberícht 2025

Qilin – Das Fabeltier, das erst anklopft, Sie bestiehlt und zum Schluss die Bude anzündet

Bedrohungsakteur	Quilin, mutmaßlich Russland
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	450h

Der zeitlich umfangreichste Vorfall 2025 war ein Ransomware Einsatz, ausgelöst durch Qilin. Die Gruppe wurde erstmals nach einem Rebranding 2022 in freier Wildbahn beobachtet und trat zuvor als „Agenda“ auf. Qilin arbeitet als Ransomware as a Service. Die Plattform und Werkzeuge liefert die Ransom-Gruppe, sogenannte Affiliates führen eigenständig Angriffe durch und die Einnahmen werden geteilt. Der Qilin Dark Web Blog führt mittlerweile rund 1400 veröffentlichte Opfer. Die Dunkelziffer wir jedoch sehr viel höher sein, da eine Veröffentlichung eines Opfers ausbleibt, sofern der Lösegeldforderung nachgegangen wird.

Abbildung 1 –Qilin Dark Web Data Leak Site

Erkannt wurde der Vorfall durch das betroffene Unternehmen in der Nacht von 19. auf den 20. Juli 2025. Aufgrund fehlender Incident Response Pläne und Playbooks verzögerte sich die Hinzunahme eines Incident Response Dienstleisters um vier Tage, wodurch r-tec erst am 23. Juli 2025 zu diesem Vorfall hinzugezogen wurde.

Lessons Learned – Krisenführung ist eine Fähigkeit, keine Ad hoc Leistung (Reaktion)

Ein Incident Response Ablauf muss vor dem Vorfall stehen und nicht erst im Vorfall entstehen. Rollen, Entscheidungswege, Kommunikationslinien und Freigaben müssen geübt sein, damit Zeit nicht in Koordination verloren geht. Gerade bei Ransomware entscheidet die frühe Führung, ob es bei Eindämmung bleibt oder zu flächigem Ausfall kommt. Readiness Maßnahmen sind damit kein Zusatz, sondern Teil der eigentlichen Reaktionsfähigkeit.

Die forensischen Analysen zeigten Brute Force Aktivitäten, die bereits Wochen vor den ersten erfolgreichen VPN-Anmeldungen begannen. Erkennbar waren Anmeldeversuche unter anderem aus Russland, Südafrika und der Niederlande, bis am 14 Juli 2025 eine erste erfolgreiche VPN-Authentifizierung nachweisbar war. Innerhalb von neun Stunden nach der erfolgreichen Infektion des Unternehmensnetzwerks eskalierte der Angreifer in den Kontext eines Domänenadministrators und etablierte Persistenzen auf mindestens zwei Domänencontrollern. In den folgenden Tagen nutzte der Bedrohungsakteur den stabilisierten Zugriff zur Vorbereitung einer Datenexfiltration. Dabei wurde unter anderem die Software „FTK“ missbraucht, eine Anwendung, die ironischerweise zur Erstellung forensischer Speicherabbilder genutzt wird. Ziel war eine Kopie der Active Directory Datenbank und relevanter Registry Artefakte, um Namen von Mitarbeitenden, Passwort-Hashes, Adressen und Telefonnummern auszuleiten.

Line	Tag	Update Timestamp	Parent Path	Name	Update Reasons
=	▣	= 2025-07-14 00:00:00		.txt	
4501262	☐	2025-07-14 19:44:58	.\Users\Administrator.INTERN\AppData\Local\DesktopCentral_Agent	dcagenttrayicon.log	DataExtend
4499931	☐	2025-07-14 19:33:37	.\Users\Administrator.INTERN\AppData\Local\DesktopCentral_Agent	dcagenttrayicon.log	DataExtend|Close
4496585	☐	2025-07-14 19:17:10	.\Users\Public\Desktop	Exterro FTK Imager.lnk	FileDelete|Close
4496584	☐	2025-07-14 19:17:10	.\Users\Public\Desktop	RustDesk.lnk	FileDelete|Close
4495811	☐	2025-07-14 19:15:57	.\Users\Administrator.INTERN\Desktop	NTDS	FileDelete|Close
4495792	☐	2025-07-14 19:15:56	.\Users\Administrator.INTERN\Desktop	SYSTEM	FileDelete|Close
4495637	☐	2025-07-14 19:14:57	.\Users\Administrator.INTERN\AppData\Local\DesktopCentral_Agent	dcagenttrayicon.log	DataExtend
4494478	☐	2025-07-14 19:10:24	.\Users\Administrator.INTERN\Desktop	SYSTEM	DataExtend|FileCreate|BasicInfo
4494477	☐	2025-07-14 19:10:24	.\Users\Administrator.INTERN\Desktop	SYSTEM	DataExtend|FileCreate|BasicInfo
4494476	☐	2025-07-14 19:10:24	.\Users\Administrator.INTERN\Desktop	SYSTEM	DataExtend|FileCreate
4494475	☐	2025-07-14 19:10:24	.\Users\Administrator.INTERN\Desktop	SYSTEM	FileCreate
4494187	☐	2025-07-14 19:09:14	.\Users\Administrator.INTERN\Desktop	NTDS	BasicInfoChange|Close
4494186	☐	2025-07-14 19:09:14	.\Users\Administrator.INTERN\Desktop	NTDS	BasicInfoChange
4494185	☐	2025-07-14 19:09:14	.\Users\Administrator.INTERN\Desktop	NTDS	FileCreate|Close
4494184	☐	2025-07-14 19:09:14	.\Users\Administrator.INTERN\Desktop	NTDS	FileCreate
4492359	☐	2025-07-14 19:07:30	.\Users\Public\Desktop	Exterro FTK Imager.lnk	DataExtend|FileCreate|Close
4492358	☐	2025-07-14 19:07:30	.\Users\Public\Desktop	Exterro FTK Imager.lnk	DataExtend|FileCreate
4492357	☐	2025-07-14 19:07:30	.\Users\Public\Desktop	Exterro FTK Imager.lnk	FileCreate

Abbildung 2 – NTDS Active Directory Datenbank Data Collection

Qilin agierte in dem Fall erwartbar destruktiv nach dem Muster der Double Extortion. Auf eine umfassende Datenexfiltration folgten die gezielte Löschung von Backups und anschließend die Verschlüsselung sämtlicher Server-Systeme.

Im Vergleich dazu setzen andere Ransomware-Gruppierungen, wie World Leaks, zunehmend auf sogenannte Exfiltration-Only-Ansätze. Dabei wird auf eine flächendeckende Verschlüsselung verzichtet und stattdessen ausschließlich der Abfluss sensibler Daten zur Erpressung genutzt. Diese Vorgehensweise gilt als schneller umsetzbar und leichter zu skalieren. Zudem ist der Erpressungsdruck bei größeren Organisationen häufig auch ohne Verschlüsselung hoch, da Datenabfluss und drohende Veröffentlichung in vielen Fällen den größeren Schaden darstellen, insbesondere wenn belastbare Backup- und Wiederanlaufkonzepte vorhanden sind.

Lessons Learned – Domänenkontrolle beginnt mit Sichtbarkeit und endet bei Wiederanlauf (Detektion & Reaktion)

Angreifer verschaffen sich nach dem ersten Zugriff schnell erhöhte Berechtigungen und stellen dauerhaften Zugang mithilfe von Persistenzmechanismen her. Für eine Erkennung respektive Aufklärung braucht es belastbare Telemetrie, ausreichend Retention und Log Kanäle, die forensisch verwertbar sind, inklusive zentraler Korrelation. Parallel müssen Backup Schutz und Wiederanlauf als Sicherheitskontrolle verstanden werden, nicht als reines IT-Thema. Wer Backups nicht gegen Löschung und Manipulation absichert, verliert im Ernstfall die Handlungsoptionen.

Lagebericht 2025

Astaroth – Wenn der Höllenfürst einen Nebenjob im Banking annimmt

Bedrohungsakteur	unbekannt, mutmaßlich Brasilien
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	30h

In der okkultistischen Mythologie gilt Astaroth als Herzog der Hölle, Gebieter über 40 Legionen. Sein digitaler Bankingtrojaner Namensvetter, erstmals 2017 beobachtet, agiert weniger mystisch, dafür umso pragmatischer. Die Malware-Familie zielt auf die Exfiltration hochsensibler Zugangsdaten wie zu Banking-/ oder Krypto-Anwendungen ab. Unsere Beobachtungen zeigen eine klare geografische Schwerpunktsetzung in Lateinamerika. Zur Verteilung des Banking-Trojaners treten neben Chat-Plattformen

Lessons Learned – Download Governance ist ein Sicherheitskontrollpunkt (Prävention)

Viele Infektionsketten starten mit einem Download, der technisch vermeidbar wäre, organisatorisch aber geduldet wird. Ein belastbares Softwareinventar je Nutzergruppe ist die Voraussetzung, um restriktive Regeln ohne Produktivitätsbruch umzusetzen. Danach müssen Installationswege und Ausnahmeprozesse klar definiert sein, damit Umgehungen nicht zur Norm werden. Webfilter und Proxy Policies entfalten Wirkung erst, wenn sie in den Arbeitsprozess integriert sind.

Charakteristisch sind bei Astaroth-Infektionen insbesondere Köderdokumente mit Steuer-, Rechnungs- und Behörden-Narrativ, die Empfänger zum Download von nachgelagerter Malware verleiten sollen. Ab September 2025 registrierte r-tec eine neue Kampagnenwelle. In einem der untersuchten Fälle erhielten mehrere Mitarbeitende eine scheinbar legitime E-Mail, in der sich ein Link befand, welcher wiederum auf eine ZIP-Datei verwies.

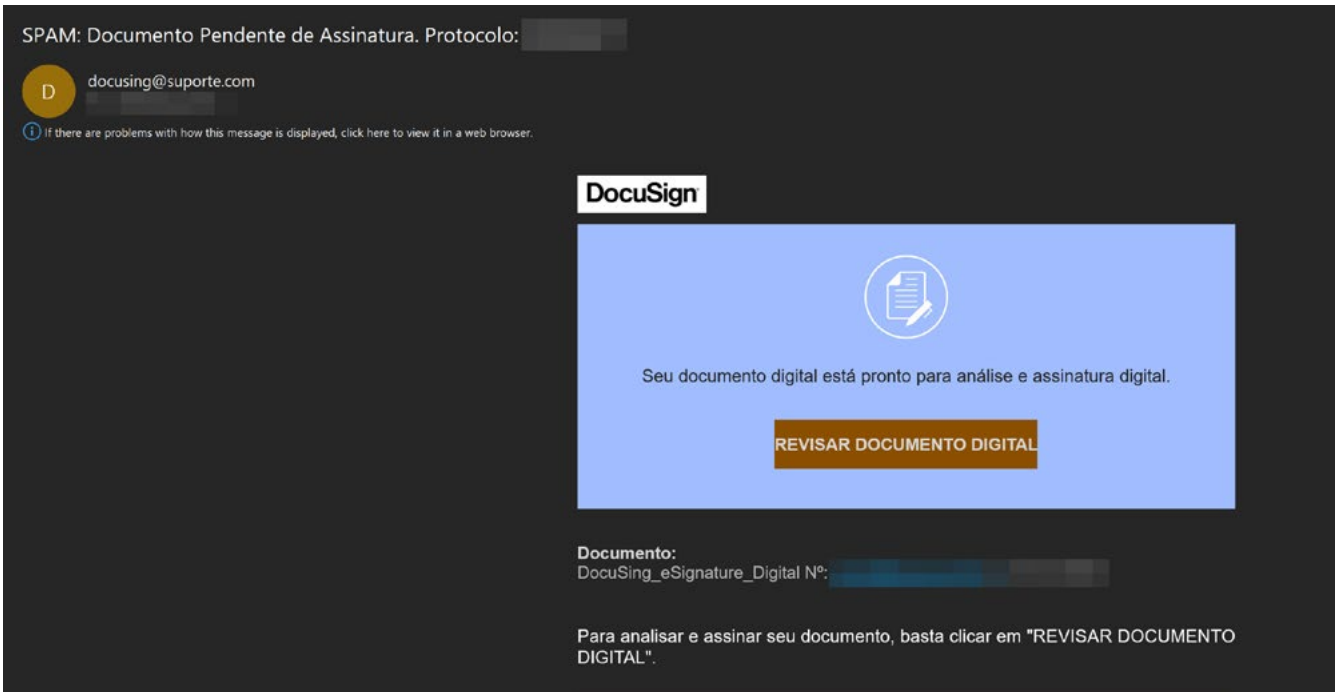


Abbildung 3 – Astaroth Spearphishing E-Mail

Die heruntergeladene ZIP-Datei enthielt den primären Malware-Loader. Nach dessen Ausführung wurde weiterer JavaScript-Schadcode nachgeladen und im Arbeitsspeicher ausgeführt. Anschließend wurde eine zufällig benannte Visual-Basic-Skriptdatei im Pfad C:\Users\Public\ abgelegt und über die Script-Host-Anwendungen cscript.exe und wscript.exe ausgeführt. Im weiteren Verlauf kamen Process Injection und Process Hollowing zum Einsatz, um die Erkennung der Malwareinfektion zu erschweren. Hierbei wurden legitime Windows-Anwendungen ausgeführt und anschließend Schadcode in deren Prozesse eingebracht.

Obwohl Microsoft Defender for Endpoint im Einsatz war, wurde die Infektion erst drei Tage nach der erstmaligen Ausführung des Loaders erkannt, da kein kontinuierlicher SOC-Betrieb zur dauerhaften Überwachung vorhanden war. Zusätzlich wirkten fehlkonfigurierte Defender-Richtlinien der automatischen Eindämmung entgegen, sodass Prozesse nicht automatisiert beendet wurden. In der Folge konnte im Rahmen der forensischen Untersuchungen ein Datenabfluss von im Browser gespeicherten Zugangsdaten nachgewiesen werden.

Lessons Learned – EDR benötigt Betriebsdisziplin und regelmäßige Wirksamkeitsprüfungen (Detektion & Reaktion)

Erkennung allein reicht nicht, wenn automatische Eindämmung durch Fehlkonfiguration ausfällt oder Alarme nicht bearbeitet werden. EDR Policies müssen anhand realistischer Testszenarien technisch regelmäßig geprüft werden, inklusive Block, Containment und Prozessbeendigung. Ohne kontinuierliche Überwachung werden selbst hochwertige Signale zu späten Informationen. Wirksam ist EDR erst, wenn Triage, Eskalation und Reaktion als verbindlicher Betrieb organisiert sind.

»Der Lagebericht zeigt, dass Unternehmen in Deutschland weiterhin im Fokus von Cyberkriminellen aus der ganzen Welt stehen. Wie groß ein Unternehmen ist oder in welcher Branche es agiert, spielt keine Rolle – jedes Netzwerk kann ein lohnendes Ziel sein.«

Rüdiger Trost
Lead Cybersecurity Expert, WithSecure

PDF zu JPG zu RAT zu „Warum ich?“ – Ein Konvertierungserlebnis der besonderen Art

Bedrohungsakteur	unbekannt
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	70h

Der CERT-Alltag 2025 war geprägt von einer hohen Bandbreite verschiedenster Malware-Familien, insbesondere Infostealer, Trojaner und Remote Access Tools. Parallel dazu wurde kriminelle Infrastruktur punktuell durch behördliche Maßnahmen gestört, unter anderem im Rahmen von Operation Endgame [01], die gegen zentrale Enabler wie Loader, Botnet und Infostealer Strukturen vorging. Dennoch blieb der Druck hoch, da Verteilungsmuster erfahrungsgemäß schnell nachwachsen.

Neben Phishing und Messengerdiensten als etablierte Verteilwege für Malware war 2025 ein deutlich erhöhtes Aufkommen initialer Infektionen über maliziöse Werbeanzeigen im Browserumfeld zu beobachten. Suchanzeigen und Werbeeinblendungen führten auf Download Seiten, die auf den ersten Blick legitim wirkten. Ein besonders prägnantes Cluster waren vermeintliche Dateikonverter, etwa PDF zu DOCX oder PDF zu JPG. r-tec konnte bei eigenen Kunden ein mittleren zweistellige Infektionszahl frühzeitig erkennen und eindämmen. Charakteristisch war, dass die Software im Vordergrund oft wie erwartet funktionierte. Im Hintergrund persistierte sich hingegen ein Remote-Access-Trojaner. Ergebnis war eine weitreichende Kontrolle des infizierten Systems im Kontext des ausführenden Benutzers.

01 https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/Endgame/Endgame_node.html

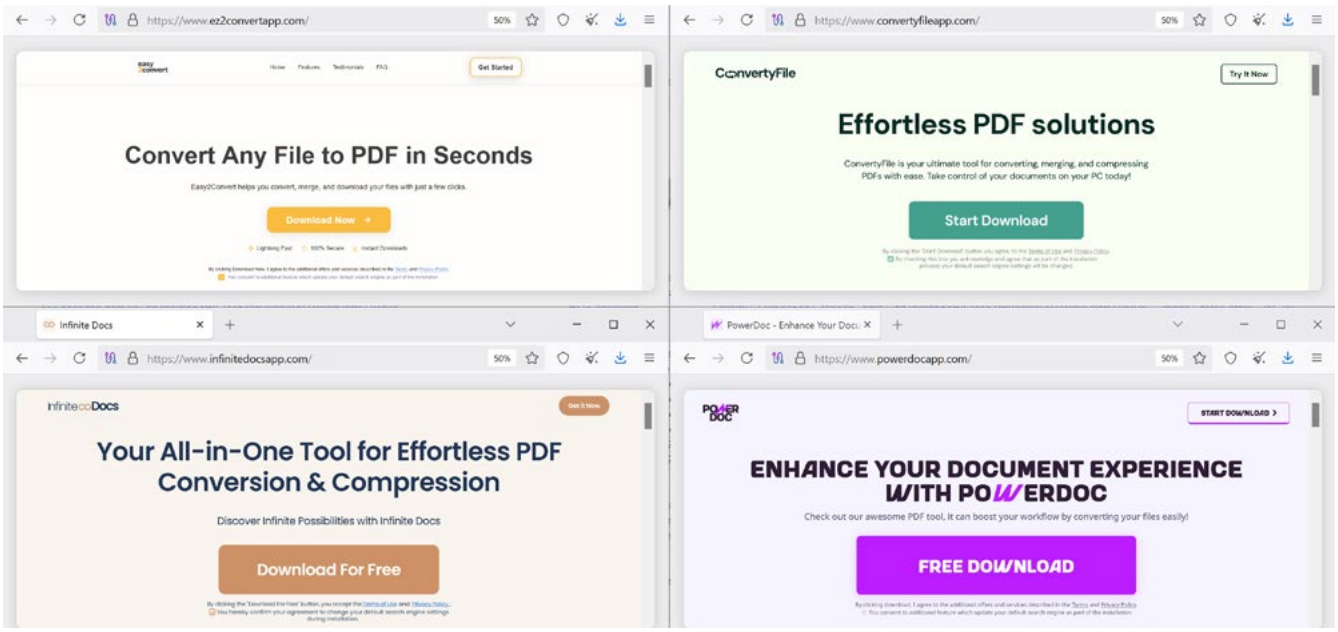


Abbildung 4 – Converter Themed RAT Download-Websites

Auffällig war in mehreren Fällen eine ausbleibende oder verspätete Initialerkennung durch gängige Endpoint-Sicherheitslösungen. In der Praxis deutete das weniger auf fehlende Sensorik hin, sondern darauf, dass vorhandene Möglichkeiten nicht ausgeschöpft wurden. Vielen IT-Verantwortlichen ist nicht bewusst, dass sich beispielsweise auch auf Endpoint-Ebene eigene Detektionslogiken ähnlich wie bei einem SIEM abbilden lassen, häufig sogar ohne Zusatzmodule.

Lessons Learned – Malvertising ist ein operatives Risiko, kein Randphänomen (Prävention)

Werbeanzeigen in Suchmaschinen sind ein stabiler Verteilkanal für vermeintliche Alltagssoftware und treffen Nutzer in Routineentscheidungen. Wirksamer Schutz beginnt vor dem Endpoint durch konsequente Webkontrolle, etwa über Webproxy und Webfilter mit klaren Richtlinien für Kategorien, Risikodomains und Download Verhalten.

Ergänzend sind definierte Bezugsquellen und ein belastbarer Freigabeprozess notwendig, um Installationen aus Werbeanzeigen heraus strukturell zu verhindern. Werden risikoreiche Dateitypen konsequent eingeschränkt, sinkt die Erfolgsquote deutlich, auch ohne jeden Einzelfall vorab kennen zu müssen.

Bei den Managed-Detection-and-Response-Kunden der r-tec zeigte sich entsprechend ein anderes Bild. Dort wurden die Konverter-Infektionen durch einen bereits etablierten kuratierten Regelsatz durchgehend detektiert. Dazu gehörten auch schon vor dieser Kampagne vorhandene Erkennungsregeln, beispielsweise zur Erstellung von Scheduled Tasks aus verdächtigen Verzeichnissen wie %LOCALAPPDATA%. Einem Persistenzmechanismus der bei den genannten Malware-Infektionen nahezu durchgängig zum Einsatz kam und zu Beginn von den meisten Endpoint-Sicherheitslösungen nicht erkannt wurden.

Im vorliegenden Fall wurde r-tec nach einer SentinelOne-Detektion bei einem betroffenen Kunden hinzugezogen. Der Ursprung ließ sich forensisch schnell auf den Download und die Ausführung der vermeintlichen Konvertierungssoftware zurückführen. Infolgedessen wurde auf Empfehlung von r-tec das System isoliert und die Passwörter sämtlicher involvierter Identitäten rotiert. Darauf aufbauend erfolgte Threat Hunting unter Verwendung der extrahierten IOCs sowie zusätzlicher Indikatoren aus Threat-Intelligence-Aktivitäten und aus vergleichbaren Vorfällen. Auf diese Weise wurden weitere infizierte Systeme identifiziert, bei denen bis dahin keine produktseitige Erkennung ausgelöst hatte.

Lessons Learned – Detektion wird durch eigene Regeln und schnellen Erkenntnistransfer stark (Detektion & Reaktion)

Standardsignaturen reichen gegen viele Infektionsvarianten oft nicht aus, weil Funktionalität und Tarnung bewusst ineinandergreifen. Entscheidend sind verhaltensbasierte Regeln, die typische Persistenzmechanismen, verdächtige Pfade und ungewöhnliche Task Erstellung abdecken. Erkenntnisse aus einem Vorfall müssen zügig in Detektionslogiken und Suchmuster überführt werden, damit Folgeinfektionen früh erkannt werden. Threat Hunting schließt dabei die Lücke zwischen Erstsignal und sicherer Scope Bestimmung.

Kündigung nicht akzeptiert: Wie ein IT-Dienstleister den Global Admin mit ins Grab nahm

Bedrohungsakteur	Insider, Deutschland
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	30h

Nicht jeder Sicherheitsvorfall beginnt mit Phishing oder Malware. 2025 traten wiederholt Fälle auf, in denen die Ursache im Umfeld von Mitarbeitenden, Geschäftspartnern oder IT-Dienstleistern lag. Gerade Dienstleister verfügen häufig über weitreichende Berechtigungen und tiefes Umgebungswissen. Wenn Offboarding, Rollenmodell und Kontrolle privilegierter Zugänge nicht sauber umgesetzt sind, entsteht daraus ein eigenständiges Risikoprofil.

Im vorliegenden Fall kam eine zusätzliche Kontextinformation hinzu: Der Vertrag mit einem IT-Dienstleister war kürzlich in einem konfliktbehafteten Verlauf gekündigt worden. Am Folgetag fiel der Organisation auf, dass ihr Microsoft-Entra-Tenant auffällige Veränderungen zeigte. Der Tenant wirkte „leer“, produktive Benutzer- und Betriebsdaten fehlten, gleichzeitig war die Umgebung mit rund 50.000 Gastbenutzern geflutet. r-tec wurde auf Wunsch der beauftragten Cyberversicherung des betroffenen Unternehmens hinzugezogen.

Lessons Learned – Privilegierte Zugänge externer Parteien brauchen ein kontrolliertes Lebenszyklusmodell (Prävention)

Dienstleisterkonten sind Hochrisiko-Identitäten und müssen, wie eigene Assets behandelt werden. Least Privilege, getrennte Admin Konten, klare Owner und regelmäßige Reviews reduzieren die Abhängigkeit von Vertrauen. Offboarding muss technisch durchgesetzt werden und darf nicht von Tickets oder Goodwill abhängen. Vertrags und Prozessdesign sind Teil der Sicherheitsarchitektur, nicht nur Einkaufsthema.

Die Cloud-Forensik zeigte einen klaren Ablauf. Zunächst erfolgte ein Login über ein Konto aus dem Dienstleisterkontext, wobei die Nutzung von VPN-IP-Adressen auffällig war. Anschließend wurden eine Enterprise Application registriert und ein weiterer Global-Admin angelegt. Danach folgten Löschungen von Benutzern und Postfächern. Im Anschluss setzte eine automatisierte Erzeugung zufällig benannter Gastkonten ein, die im Zusammenhang mit der zuvor angelegten Enterprise Application stand.

ActivityDateTime	Activity	OperationType	Status	Country Name	OrgName	Target1ModifiedProperty1NewValue
2025-05-14 18:40:30.000	Add group	Add	success			noreply13
2025-05-14 18:40:29.000	Add group	Add	success			noreply11
2025-05-14 18:40:28.000	Add group	Add	success			noreply10
2025-05-14 18:40:27.000	Add group	Add	success			noreply8
2025-05-14 18:40:27.000	Add group	Add	success			noreply9
2025-05-14 18:40:26.000	Add group	Add	success			noreply7
2025-05-14 18:40:25.000	Add group	Add	success			noreply6
2025-05-14 18:40:24.000	Add group	Add	success			noreply5
2025-05-14 18:40:23.000	Add group	Add	success			noreply3
2025-05-14 18:40:23.000	Add group	Add	success			noreply4
2025-05-14 18:40:22.000	Add group	Add	success			noreply2
2025-05-14 18:40:21.000	Add group	Add	success			noreply1
2025-05-14 18:32:42.000	Add service principal	Add	success			true
2025-05-14 18:29:28.000	Add member to role	Assign	success	United States	RouterHosting LLC	
2025-05-14 18:29:27.000	Update service principal	Update	success	United States	RouterHosting LLC	
2025-05-14 18:29:27.000	Add service principal	Add	success	United States	RouterHosting LLC	true
2025-05-14 18:29:27.000	Update application	Update	success	United States	RouterHosting LLC	
2025-05-14 18:29:27.000	Update application – Certificates and secrets manage	Update	success	United States	RouterHosting LLC	KeyIdentifier= KeyType=Password,KeyUsage=Verify,DisplayName=MySecret
2025-05-14 18:29:26.000	Add application	Add	success	United States	RouterHosting LLC	
2025-05-14 18:29:18.000	Add delegated permission grant	Assign	success	France	Microsoft Corporation	Application.ReadWrite.All Directory.ReadWrite.All RoleManagement.ReadWrite.Directory openid profile offline_access
2025-05-14 18:29:18.000	Add service principal	Add	success	France	Microsoft Corporation	true
2025-05-14 18:29:18.000	Add app role assignment grant to user	Assign	success	France	Microsoft Corporation	00000000-0000-0000-0000-000000000000
2025-05-14 18:29:18.000	Consent to application	Assign	success	France	Microsoft Corporation	True
2025-05-14 17:22:31.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:31.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:31.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True
2025-05-14 17:22:30.000	Hard Delete user	Delete	success	Bangladesh	Link3 Technologies Ltd.	True

Abbildung 5 – Verdächtige Registrierung einer Entra Anwendung

Die aktivierten Entra- und M365-Logging-Einstellungen ermöglichten eine weitgehend lückenlose Rekonstruktion. Eine eindeutige Attribution blieb dennoch offen. Die Protokolle zeigten erfolgreiche MFA-Nutzung sowie den Zugriff über ein registriertes Gerät, was einen

Zugriff aus dem Dienstleisterumfeld plausibel macht, eine Kompromittierung des Kontos jedoch nicht ausschließt. Unabhängig von der finalen Täterschaft verdeutlicht der Fall, wie schnell privilegierte Cloud-Berechtigungen zu einem vollständigen Kontrollverlust führen können, wenn Governance- und Offboarding-Prozesse nicht belastbar sind.

Lessons Learned – Cloud Kontrollverlust entsteht durch wenige Aktionen, deshalb müssen genau diese überwacht werden (Detektion & Reaktion)

Kritische Schritte wie App Registrierung, Rollenvergabe, Massenlöschungen und Gastnutzeranlage müssen als Hochrisiko Ereignisse alarmiert werden. Das setzt vollständige Audit Logs, ausreichende Retention und klare Reaktionspfade voraus, damit nicht nur rekonstruiert, sondern gestoppt werden kann. MFA-Erfolg ist kein Entwarnungssignal, sondern kann auch Missbrauch eines legitimen Pfads bedeuten. Wirksam wird Monitoring erst, wenn es mit getesteten Playbooks und eskalationsfähiger Bereitschaft verbunden ist.

Lagebericht 2025

ClickFix, FileFix, CrashFix – Spoiler: Nichts davon fixt irgendwas

Bedrohungsakteur	mutmaßlich APT28, Russland
r-tec Service-Kunde	Ja
Bearbeitungsdauer CERT	8h

Angreifer waren auch 2025 in der Verteilung von Malware auffällig kreativ. Ein besonders wirksames Muster waren sogenannte ClickFix-Angriffe, über die 2024 erstmals in der Öffentlichkeit berichtet wurde. Anders als bei klassischen Download- oder E-Mail-Anhang-Ketten wird hier die Benutzerinteraktion selbst zur Ausführungskomponente. Betroffene werden über Spearphishing, Malvertising oder kompromittierte Websites auf eine maliziöse Landingpage geführt, die als „Human Verification“ oder Fehlerbehebung getarnt ist. Dort erhalten sie Schritt-für-Schritt-Anweisungen, die letztlich dazu führen, dass ein bereits in die Zwischenablage kopierter Befehl in die Befehlsausführung eingefügt und ausgeführt wird.

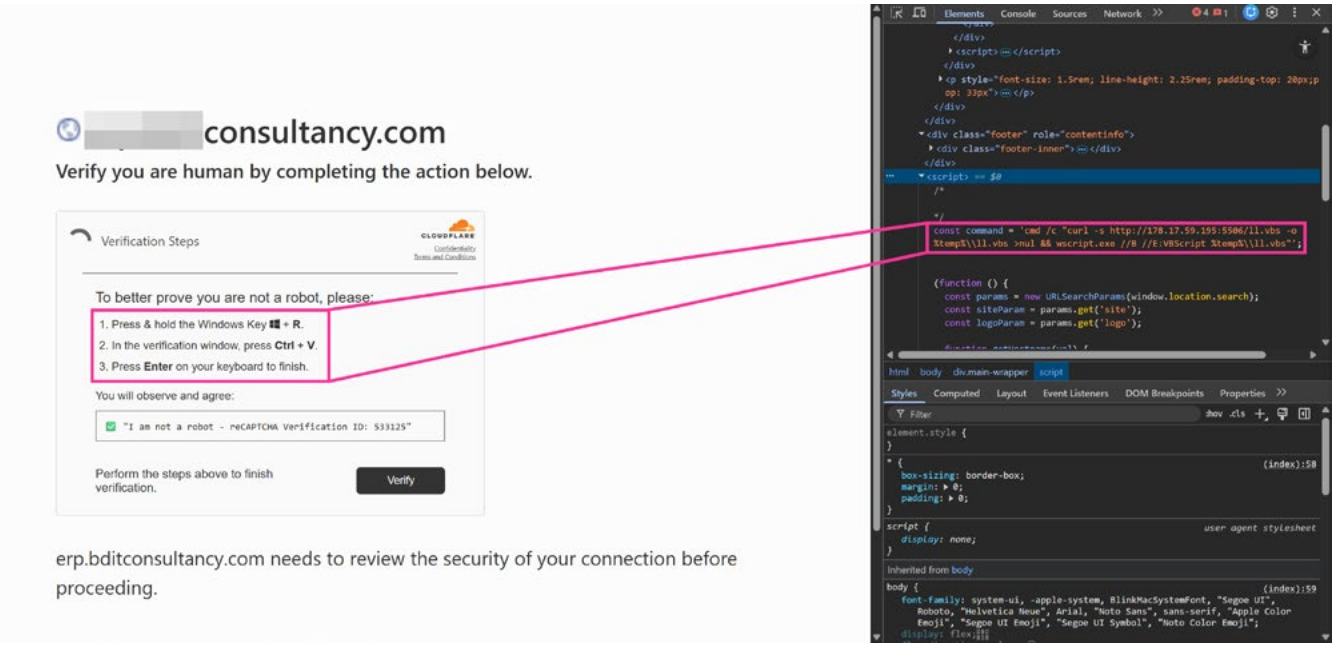


Abbildung 6 – Klassisches ClickFix Payload Delivery Beispiel

Die Technik funktioniert gerade deshalb, weil sie psychologisch ausgefeilt aufgebaut ist. Der Nutzer glaubt, eine Sicherheitsprüfung abzuschließen oder ein Anzeigeproblem zu beheben, und führt dabei tatsächlich einen initialen Loader aus. Häufig gibt es dabei auch keinen „klassischen“ Malware-Download, sondern eine Befehlskette, die direkt über Living-off-the-Land-Binaries startet, typischerweise über powershell.exe, mshta.exe oder msiexec.exe. Wenn doch Dateisysteminteraktion entsteht, dann oft über Script-Hosts wie wscript.exe oder cscript.exe oder HTML-/Script-Container. Dass diese Mechanik längst nicht nur von Cybercrime genutzt wird, sondern auch staatlich gesteuerte Akteure ClickFix/Fake-CAPTCHA-Ketten einsetzen, zeigt der hier beschriebe Fall.

Mit der Zeit wurde das Grundprinzip weiterentwickelt. Eine verbreitete Ausprägung ist die „OSUpdate“-artige Variante: Statt CAPTCHA wird ein täuschend echter Windows-Update-Bildschirm angezeigt, um zusätzlichen Handlungsdruck zu erzeugen. Die Variante „FileFix“ hingegen verschiebt den Ausführungspunkt von „Ausführen“ in den File-Explorer. Die Opfer werden aufgefordert eine vermeintliche Pfadangabe in die Explorer-Adresszeile einfügen, die dann einen PowerShell-Aufruf zur Folge.

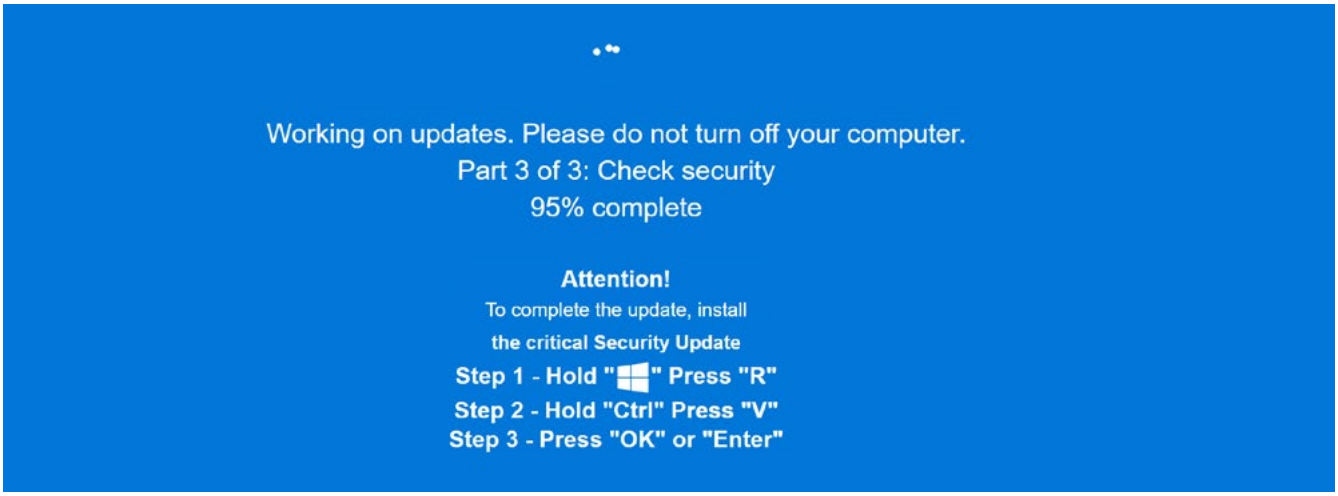


Abbildung 7 – OSUpdate ClickFix Variante

Die bislang jüngste öffentlich dokumentierte Variante ist „CrashFix“. Hier wird nicht nur ein Problem behauptet, sondern tatsächlich erzeugt. Eine zunächst installierte schädliche Browser-Erweiterung bringt den Browser gezielt zum Absturz und präsentiert danach eine „Fix“-Anleitung, die erneut auf Copy-Paste-Ausführung hinausläuft.

Im vorliegenden Fall führte eine ClickFix Infektion zur Alarmierung des r-tec SOC und anschließend zur Eskalation an das CERT. Die forensische Einordnung zeigte als Ursprung einen Website-Besuch einer legitimen Website, gefolgt von einer Weiterleitung über eine Werbeeinblendung zum maliziösen CAPTCHA und der anschließenden Ausführung einer Befehlskette. Nach initialer PowerShell-Aktivität wurde mshta.exe ausgeführt, wodurch remote Inhalte ausgeführt wurden. Auffällig war dabei eine vermeintliche .m4a-Datei, die sich tatsächlich als stark obfuskierte HTA-Stufe erwies. Es folgten weitere, jeweils stark verschleierte Malware-Stufen bis zur finalen RAT-Ausführung. Durch vorhandene Detektionsregeln zur Erkennung von Script-Host-Executables, insbesondere in Kombination mit

Internetaktivitäten, und die Anbindung an automatisierte Reaktionspfade konnte das betroffene System jedoch frühzeitig isoliert werden, noch bevor der finale Payload zur Ausführung kam.

Lessons Learned – ClickFix-Abwehr: LoLBin-Sichtbarkeit und stufenweise Härtung (Prävention & Detektion)

ClickFix-Ketten lassen sich in der Praxis zuverlässig über auffällige Prozessbeziehungen und das Verhalten typischer Living-off-the-Land-Binaries erkennen (z. B. Browser/Office → powershell/mshta/wscript/cscript) sowie über korrelierte Netzwerkaktivitäten dieser Prozesse nach einem initialen Baselining. Langfristig ist Application Control für selten benötigte Script- und HTA-Ausführer der wirksamste Hebel. Sinnvoll ist ein stufenweises Vorgehen, bei dem zunächst Monitoring und Inventarisierung die realen Softwareanforderungen aufdeckt, gefolgt von sukzessiven Einschränkungen und Blockierungen und klaren Ausnahmeprozessen. Ergänzend reduzieren Webfilter, restriktive Extension-Policies und SIEM- und Endpoint-Regelsätze die Erfolgsquote deutlich, weil diese Infektionsketten auf wiederkehrenden Ausführungsmustern aufbauen.

Sehr geehrte Damen und Herren, anbei meine Bewerbung.exe

Bedrohungsakteur	unklar, mutmaßlich Russland oder Nord-Korea
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	46h

Auch HR-Abteilungen sind ein attraktives Ziel, weil sie regelmäßig Dateien von externen Absendern erhalten und öffnen müssen. Lebensläufe kommen nicht nur als PDF, sondern auch als DOCX, Bild, Archiv, teils verschlüsselt, und im schlechtesten Fall als Bewerbung.exe. Zwar sind technische Kontrollen zur Einschränkung von Downloads und Ausführungen unabdingbar, sie bleiben in der Praxis jedoch oftmals umgehbar. In solchen Prozessketten ist der Mensch häufig zugleich erste und letzte Verteidigungslinie.

Die Relevanz dieses Angriffsvektors zeigt sich auch in öffentlich beschriebenen Kampagnen nordkoreanischer Akteure, die über Recruitment- und Bewerbungsnarrative arbeiten, teils mit gefälschten Identitäten, „Bewerberprofilen“ und dem Ziel, Zugriff auf Unternehmensumgebungen zu erlangen oder Schadsoftware nachzuladen. In diesem Kontext wird unter anderem Famous Chollima als Akteur genannt, der Job- und Bewerbungsprozesse gezielt ausnutzt.[02]

Lessons Learned – HR-Prozesse brauchen ein sicheres Einreichungs- und Öffnungskonzept (Prävention & Reaktion)

Bewerbungen sind ein regelmäßiger externer Dateieingang und müssen als eigener Initial Access Pfad modelliert werden. Sichere Kanäle wie Portale, kontrollierte Viewer und isolierte Öffnungsumgebungen reduzieren den Zwang, Anhänge direkt auszuführen oder lokal zu speichern. Dateityp Policies müssen strikt gestaltet sein und dürfen nicht durch Einzelfall Ausnahmen ausgehöhlt werden. Schulung hilft, ersetzt aber keine technische Prozessführung.

02 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/

Der vorliegende Fall begann wie mehrere andere Vorfälle 2025 nicht mit einem internen Alarm, sondern mit einem externen Hinweis einer Ermittlungsbehörde. Die betroffene Organisation erhielt einen Hinweis von der Polizei mit dem Hinweis auf eine mögliche Kompromittierung mindestens eines Systems. Ein Blick in die eingesetzte Sophos-Endpoint-Sicherheitslösung zeigte, dass auf dem betroffenen System bereits Alarme vorlagen. Eine Reaktion war jedoch ausgeblieben. Der Vorfall wurde erst rund zwei Wochen später durch den polizeilichen Hinweis aktiv bearbeitet. Das unterstreicht erneut, dass Sicherheitslösungen nur dann wirksam sind, wenn Alarme kontinuierlich gesichtet und in klare Reaktionsprozesse überführt werden.

Die Analysen ergaben folgenden Ablauf: Eine Recruiterin erhielt zunächst den Lebenslauf LEBENSLAUF NAME.pdf. Beim Öffnen trat ein bewusst herbeigeführter Fehler auf. In einem anschließenden Telefonat mit dem vermeintlichen Bewerber wurde eine zweite Datei übermittelt, diesmal LEBENSLAUF NAME.exe. Nach Ausführung der Datei wurde eine Command-and-Control-Verbindung aufgebaut. In der Folge nutzte der Angreifer primär den C2-Beacon und Systemwerkzeuge zur Auskundschaftung, ohne auffällige zusätzliche Tools nachzuladen. Der Beacon wurde in ping.exe injiziert, anschließend waren typische Discovery-Kommandos nachvollziehbar (u. a. net, netstat, nslookup, tasklist). Zudem wurde RDP eingesetzt, erkennbar getunnelt über den C2-Beacon und einen Proxy.

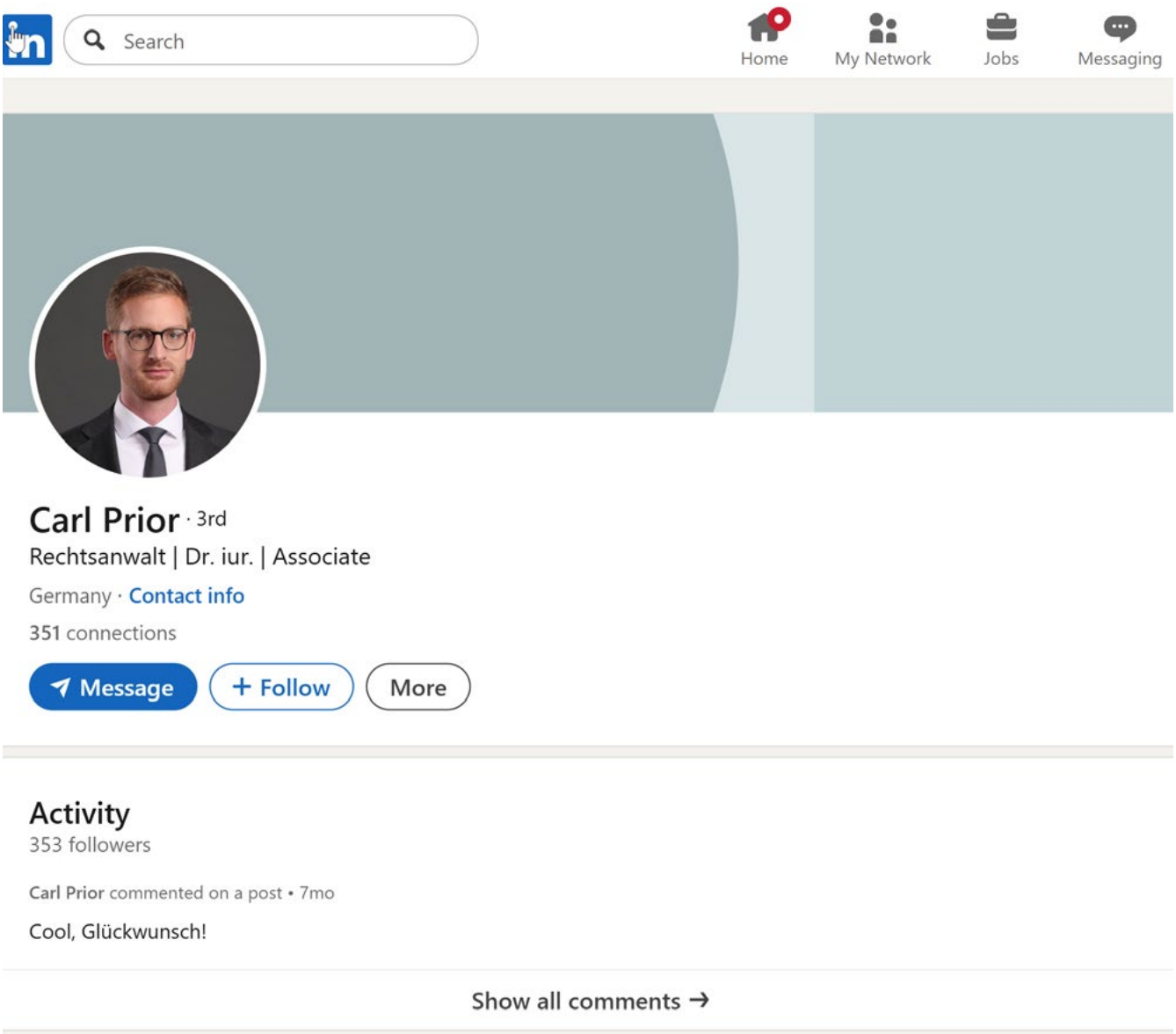
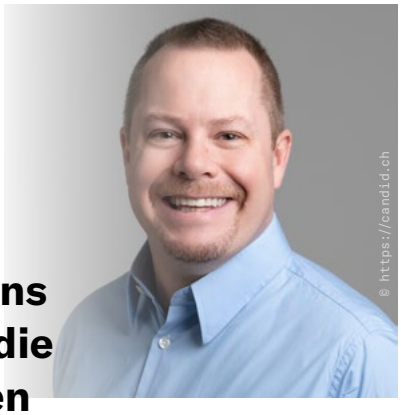


Abbildung 8 – Gefälschtes LinkedIn Bewerberprofil

Im weiteren Verlauf griff der Angreifer auf mehrere Terminalserver zu. Von dort aus erfolgten umfangreiche SMB-Zugriffe auf Netzlaufwerke. Es folgte die Erzeugung diverser Datei-Archive, welche anschließend an die C2-Infrastruktur der Angreifer übertragen wurde. Der Fall ist insbesondere deshalb relevant, weil Terminalserver als „Sprungbrett“ ein hohes Eskalationspotenzial haben, wenn Segmentierung, Tiering und Privilegienmanagement nicht konsequent umgesetzt sind. Eine weitergehende Eskalation konnte im vorliegenden Fall nicht belastbar nachgewiesen werden, das Risikoprofil war jedoch klar erkennbar.

Lessons Learned – Terminalserver und Shares müssen so gestaltet sein, dass ein einzelnes Postfach nicht zum Datendiebstahl führt (Detektion & Prävention)

Wenn Angreifer von einem kompromittierten Client auf Terminalserver springen, entsteht schnell ein Multiplikator für laterale Bewegung. Segmentierung, Tiering und restriktive Berechtigungen auf Shares begrenzen den Impact und erschweren Massensammlung. Zusätzlich sollten RDP-Nutzung, Discovery Befehle und ungewöhnliche Archivierungsvorgänge eng überwacht werden. Der Schutz liegt damit im Design der Umgebung, nicht nur im Erkennen der ersten Datei.



»Jeder Fall enthält konkrete, herstellerunabhängige Lessons Learned sowie Maßnahmen, die Unternehmen direkt umsetzen können – kurz, prägnant und praxisnah. In den vielen Diskussionen über zukünftige Angriffsmuster wie z. B. AI Prompt Injection vergessen wir leicht, dass Cyberkriminelle bereits heute mit anderen Methoden sehr erfolgreich sind. Sichere Konfiguration und Grundschutz sind nach wie vor essenziell.«

Candid Wüest
Principal Threat Researcher, xorlab

Jurassic Malware – Wenn USB-Sticks aus der Steinzeit Ihre Produktion lahmlegen

Bedrohungsakteur	Nord-Korea
r-tec Service-Kunde	Ja
Bearbeitungsdauer CERT	38h

© googledeepmind | pexels

Der Vorfall begann zunächst unspektakulär. In einer Produktionsumgebung des betroffenen Unternehmens traten wiederholt Windows Blue Screens auf. Betroffen waren ausschließlich Legacy-Systeme (Windows XP, Vista, Windows Server 2003 und Windows Server 2008), die in OT-nahen Segmenten weiterhin betrieben wurden. Die Ursache war zunächst schwer einzugrenzen, weil das Segment über keine Internet-Anbindung verfügte und damit nur eingeschränkt von klassischer Telemetrie abgedeckt war. Erste Crashdump-Stichproben deuteten auf Netzwerk-/Treiberbezug hin, insbesondere Netzwerkstack- und SMB-nahe Treiberpfade. Erst die Ausweitung der Analyse brachte den entscheidenden Pivot. Auf mehreren Hosts fanden sich WannaCry-Artefakte, Spuren in Service-Registrierungen, Registry-Pfaden und im Dateisystem, konsistent mit bekannten Installations- und Persistenzmustern.

Lessons Learned – Legacy Systeme benötigen eigene Sicherheitsregeln und klare Eintrittskontrollen (Prävention)

OT und Legacy Umgebungen sind oft nicht patchbar und nicht agentfähig, daher muss Schutz über Architektur erfolgen. Segmentierung, kontrollierte SMB-Nutzung und strikte Regeln für Wechseldatenträger sind hier die wirksamsten Hebel. Besonders wichtig ist ein Reaktivierungsprozess, der Systeme vor Wiederaufnahme auf eine Infektion untersucht, quarantänisiert und freigibt. Ohne solche Regeln bleibt Abschottung ohne Internet ein trügerisches Sicherheitsargument.

WannaCry ist eine Ransomware-Wurm-Kombination aus 2017, deren Propagation insbeson-

dere über SMB-basierte Mechanismen erfolgte und insbesondere mit der Schwachstelle MS17-010 (EternalBlue/SMBv1) zusammenhängt. Im vorliegenden Fall wurde sichtbar, warum „alt“ nicht „harmlos“ bedeutet. Der Auslöser war ein betriebliches Muster, das in Produktionsnetzen häufig ist. Ein Patient-Zero-System war über Jahre nicht genutzt worden und wurde kürzlich wieder in das Netzwerk aufgenommen. Die automatische Wurmfunktionalität sorgte anschließend für fortgesetzte Infektionen weiterer Geräte im Segment. Dass die Umgebung kein Internet hatte, verhinderte zwar externe Folgeeffekte, änderte jedoch nichts am operativen Schaden innerhalb des Netzes. Laterale Bewegung und Instabilität in der Produktion sind auch ohne Internet hochkritisch. Verschärft wird der Umstand durch die Tatsache, dass viele OT-Umgebungen mit der IT verknüpft sind und somit potenziell die Ausbreitung in größere, kritische Netzsegmente nicht ausgeschlossen werden kann.

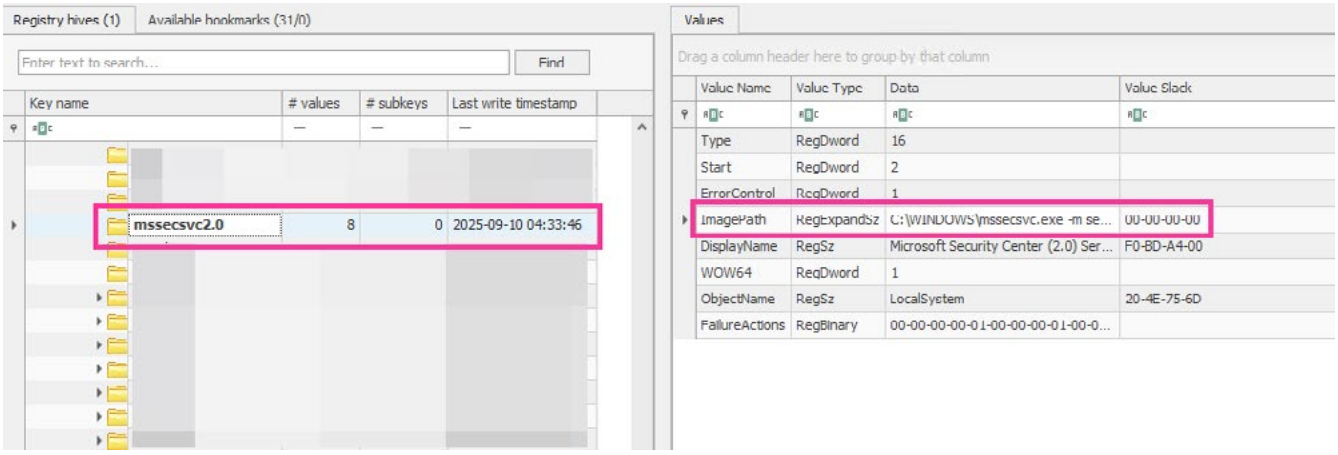


Abbildung 9 – WannaCry Wurmkomponente persistiert in der Windows Registry

Für den ursprünglichen Initialvektor ergab sich ein plausibles Bild, ohne dass eine nachträgliche Beweisführung möglich war. Da das System lange offline war, lag eine frühere Infektion nahe, etwa über Wechseldatenträger/USB im Rahmen von Wartung oder Datentransfers. Genau diese „Zwischenwelt“ zwischen IT-Hygiene und Produktionsrealität macht solche Vorfälle so hartnäckig. Patchen ist oft nicht möglich, EDR-Agenten sind nicht installierbar, und die Prozesse sind auf Verfügbarkeit optimiert, nicht auf schnelle Modernisierung.

Lessons Learned – Sichtbarkeit im OT-Segment ist Pflicht, auch ohne klassische EDR-Telemetrie (Detektion & Reaktion)

Wenn Agenten fehlen, muss Netzwerkmonitoring die Rolle der Frühwarnung übernehmen, etwa durch IDS und Protokollanalyse. Ereignisse wie ungewöhnliche SMB-Aktivitäten, wiederkehrende Abstürze und Service Artefakte müssen in ein klares Incident Vorgehen münden. Reaktion bedeutet hier oft Isolation, Bereinigung im Segment und kontrollierter Wiederanlauf statt klassischer Endpoint Maßnahmen. Entscheidend ist, dass diese Abläufe vorab definiert und mit Betrieb und Produktion abgestimmt sind.

To Docker or not to Docker – Das ist hier die Backdoor

Bedrohungsakteur	unbekannt, mutmaßlich Russland
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	20h

Malvertising zielt nicht nur auf die „breite Masse“, sondern zunehmend auch gezielt auf Entwickler und IT-Administratoren. Das ist besonders kritisch, weil diese Zielgruppe häufig mit erhöhten Rechten agiert und Software routinemäßig über Browsing-Aktivitäten bezieht. Für Betroffene ist die Erkennung zusätzlich erschwert, wenn Angreifer legitime Plattformen als „Zwischenstation“ missbrauchen. Wer bei der Suche nach „Docker Desktop“ oder „GitHub Desktop“ eine Anzeige anklickt und auf Docker Hub oder GitHub landet, bewertet den Link schnell als vertrauenswürdig, obwohl die schädliche Komponente erst im nächsten Schritt steckt.

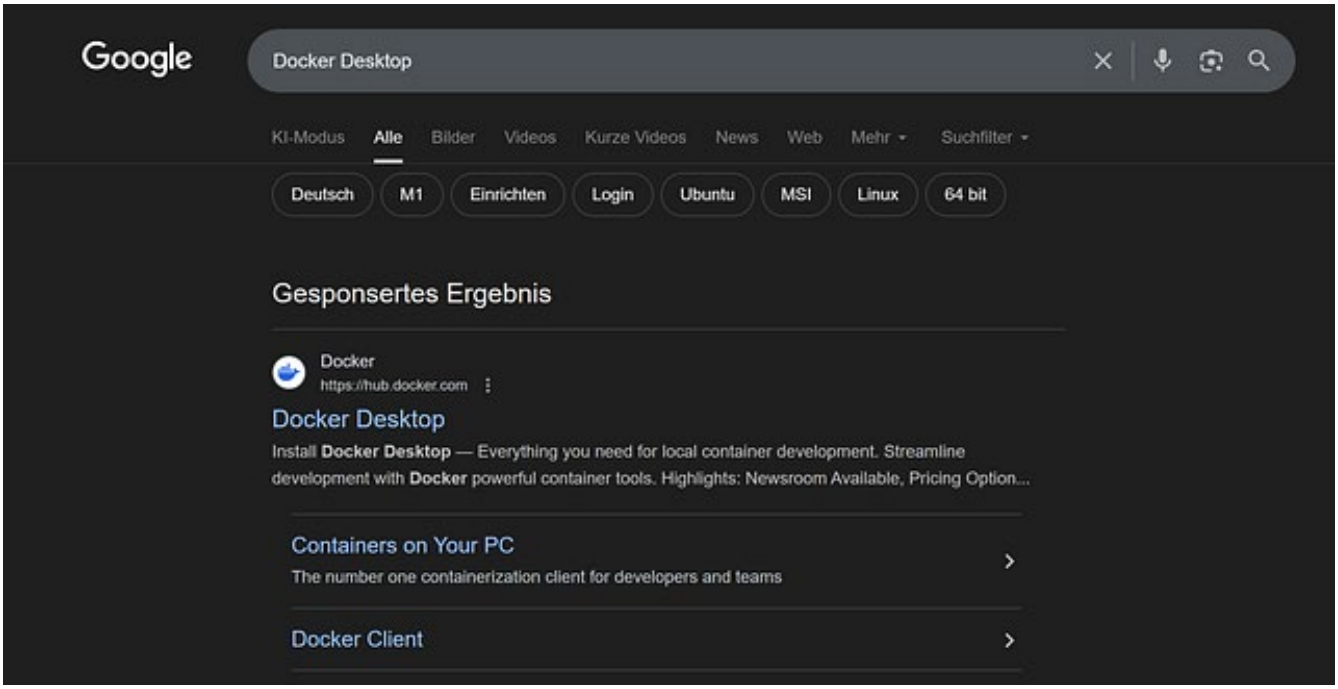


Abbildung 10 – Maliziöse Docker Desktop Werbeanzeige

Im November 2025 identifizierte r-tec im Rahmen von Threat-Intelligence-Aktivitäten eine Kampagne, bei der Suchanzeigen auf Docker-Hub-Repositories verwiesen, die optisch wie

offizielle Download-Seiten gestaltet waren. Solche Repositories waren teils bereits über Wochen aktiv und enthielten Beschreibungen, Banner und „Download Docker Desktop“-Buttons. Die sichtbaren Verlinkungen führten jedoch nicht zum legitimen Installer, sondern zu Angreifer-kontrollierter Infrastruktur, von der eine persistente Remote-Access-Malware nachgeladen wurde.

Lessons Learned – Softwarebezug ist ein Vertrauensanker und muss gesteuert werden (Prävention)

Für administrative Software darf Websuche kein Standardinstallationspfad sein. Definierte Bezugswege, Signatur und Hash Prüfungen sowie Freigabeprozesse senken das Risiko von Imitationen und Manipulation. Zusätzlich sollten Installationsrechte, Ausführungspfade und Persistenzmechanismen stärker kontrolliert werden, da diese Zielgruppen oft privilegiert arbeiten. Damit wird aus Beschaffung eine echte Sicherheitskontrolle.

Auffällig war, dass sich die Kampagne nicht auf ein einzelnes Repository beschränkte. Mittels Threat Intelligence konnten mehrere, thematisch ähnliche Repositories identifiziert werden. Zudem wurden Links in einzelnen Fällen zeitweise gegen legitime Downloads ausgetauscht, was die Sichtprüfung und nachträgliche Analyse erschwerte.

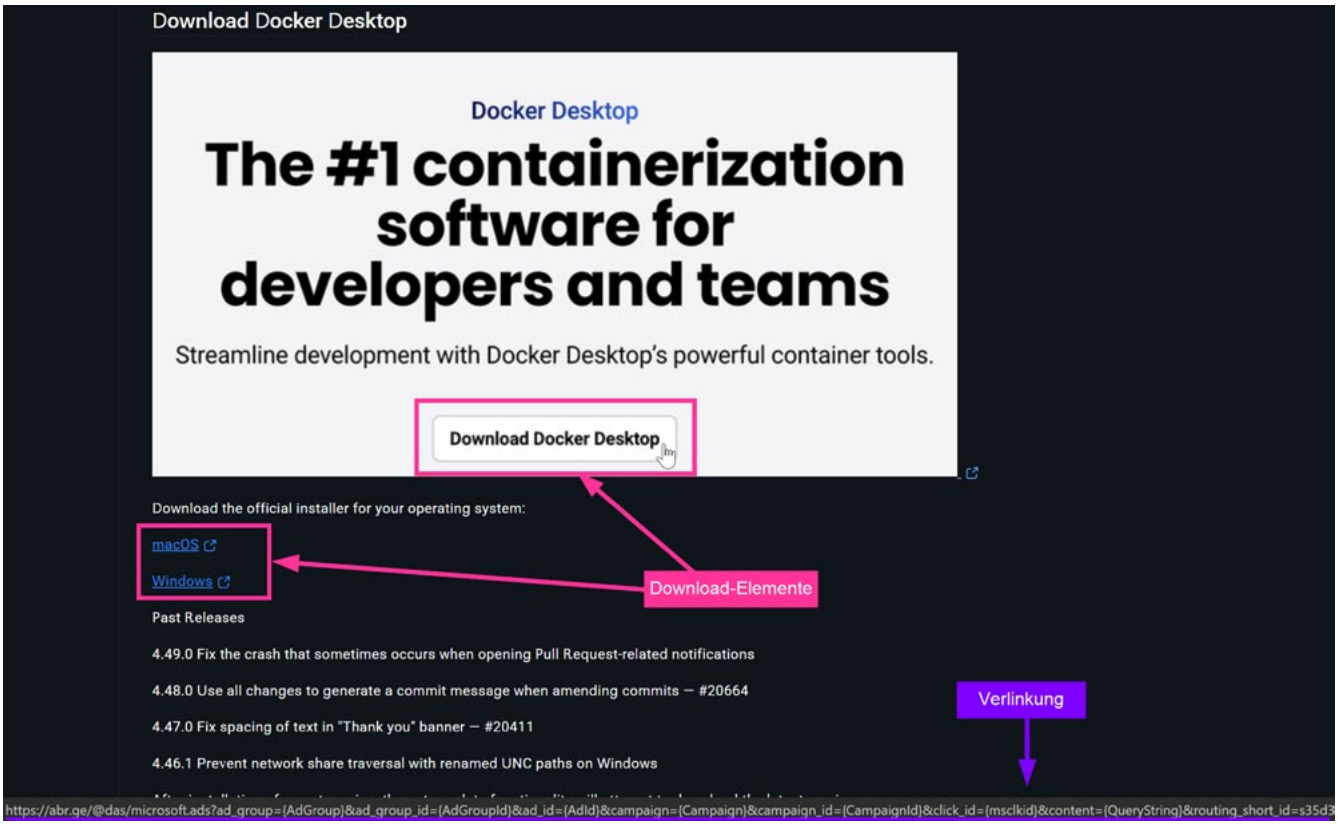


Abbildung 11 – Docker Desktop Docker Hub Repository

Technisch agierte der initiale Payload in einem der untersuchten Vorfälle als Dropper für eine nachgelagerte RAT-Infektion und setzte auf Analyse- und Sandbox-Evasion. Die Datei war mit rund 120 MB ungewöhnlich groß, obwohl die eigentliche Funktionalität deutlich kleiner war und durch Null-Padding künstlich aufgebläht wurde. Zusätzlich prüfte die Malware vor der Ausführung, ob das System über eine GPU verfügt, um typische Analyseumgebungen und Sandboxes auszuschließen.

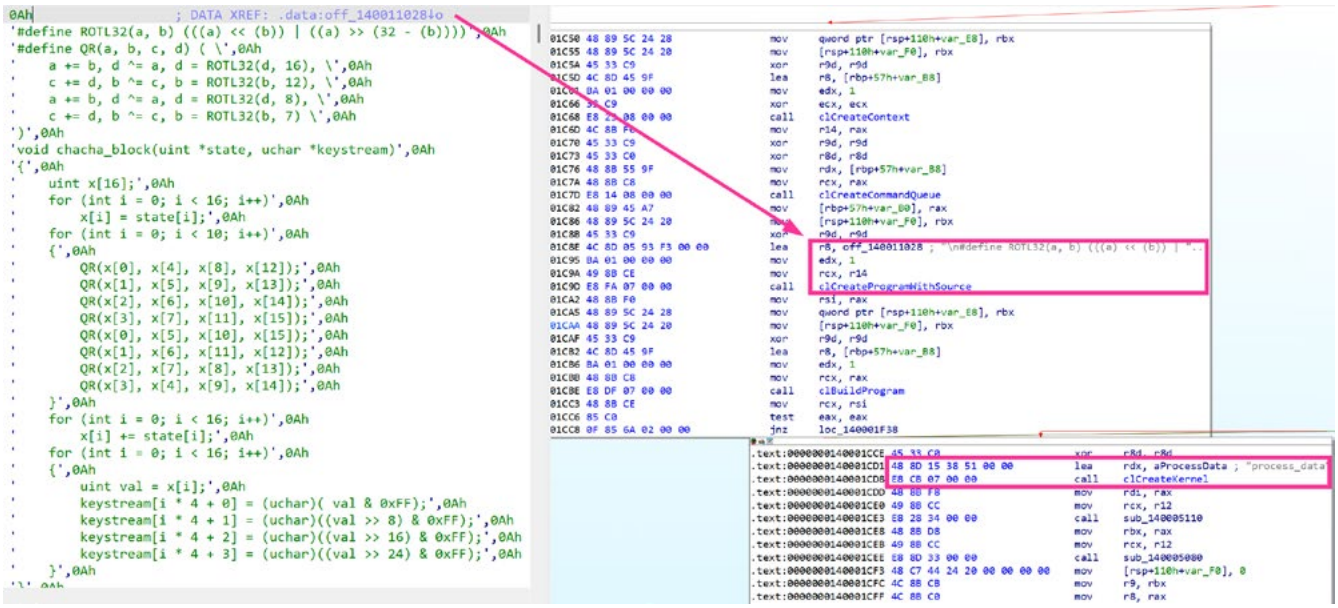


Abbildung 12 – ChaCha Entschlüsselungsfunktion als Kernel Objekt

Zur Laufzeit wurde die zweite Stufe mit ChaCha entschlüsselt und ausgeführt. Die benötigten Schlüsselparameter ließen sich durch Debugging und Analyse rekonstruieren, da das Schlüsselmaterial hardcodiert vorlag. Persistenz wurde über einen Scheduled Task etabliert, der die Ausführung bei Benutzer-Logon sicherstellte. Threat-Intelligence-Erkenntnisse deuteten zudem auf einen Ursprung in Russland hin. Wofür die RAT- und nachgelagerte Infostealer-Infektion im konkreten Fall genutzt werden sollte, ließ sich nicht belastbar bestimmen.

Lessons Learned – Brand Missbrauch ist ein messbarer Frühindikator, wenn man ihn aktiv beobachtet (Detektion & Prävention)

Sponsored Search und Repository Imitationen sind häufig über Wochen sichtbar, bevor sie breit eskalieren. Threat Intelligence sollte deshalb auch Markenbegriffe, Repositories und ungewöhnliche Download Weiterleitungen beobachten. Ergänzend helfen technische Kontrollen, etwa Blocklisten und sichere Allowlisten für offizielle Domains und Artefaktquellen. So wird aus einem reaktiven Incident ein proaktives Unterbrechen der Kampagne.

ToolShell – Der Patch war da, der Angreifer leider auch

Bedrohungsakteur	China
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	80h

Ab dem 18 Juli 2025 war eine breit angelegte Angriffswelle auf on premises SharePoint Server zu beobachten. Betroffen waren SharePoint Server Subscription Edition, SharePoint Server 2019 und SharePoint Server 2016. In vielen Umgebungen sind diese Systeme nicht nur Collaboration, sondern historisch gewachsene Applikationsplattformen, die extern erreichbar betrieben werden. Genau das machte die Lage operativ heikel. Aus einem einzelnen exponierten Server wird bei erfolgreicher Ausnutzung schnell ein Domino Stein für die gesamte interne Umgebung.

ToolShell wurde in Berichten als Sammelbegriff für eine Zero-Day Exploitkette geführt, die unter anderem mit CVE-2025-49706 als Authentication Bypass und CVE-2025-49704 als Remote Code Execution in Verbindung gebracht wurde. Später wurden Varianten wie CVE-2025-53770 diskutiert, die Deserialization Aspekte abdecken. Charakteristisch war die Möglichkeit, ohne vorherige Authentifizierung durch gezielte Requests in Richtung Dateiupload und Manipulation sicherheitsrelevanter Konfiguration zu gelangen. Damit konnten gültige Viewstate Tokens erzeugt und Codeausführung erreicht werden.

date	time	s-ip	cs-method	cs-uri-stem	s-port	c-ip	cs(User-Agent)
2025-07-18	17:43:00	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-18	18:08:08	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-18	17:32:25	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-18	18:08:36	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-19	07:03:20	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-19	07:26:27	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-19	06:52:27	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-19	07:26:46	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
2025-07-20	14:59:41	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	python-requests/2.31.0
2025-07-20	15:07:39	10.27.	GET	/_layouts/15/spinstall0.aspx	443	10.27.	python-requests/2.31.0

Abbildung 13 – ToolShell Exploitationsversuche

r tec sah mehrere Kunden betroffen, sowohl MDR- als auch nicht MDR-Kunden. MDR-Kunden profitierten unmittelbar von Threat Intelligence und Überwachung durch das SOC. Andere Kunden wurden über CERT Advisories informiert. In einem besonders relevanten Vorfall war die größte Hürde zunächst nicht die Forensik, sondern fehlende Transparenz. Es existierten mehrere SharePoint Server, aber kein belastbares Inventar, kein aktueller Netzwerkplan und kein klarer Überblick über Versionsstände. Wertvolle Zeit ging verloren, um

Scope und Prioritäten zu bestimmen. r-tec musste kurzfristig Discovery und Vulnerability Management Maßnahmen etablieren. Parallel wurde der Perimeter provisorisch weitreichend isoliert, um weitere Ausnutzung zu verhindern.

Lessons Learned – Inventar und Exposition entscheiden über Reaktionsgeschwindigkeit (Prävention, Reaktion, Detektion)

Wenn im Vorfall erst gesucht werden muss, welche Systeme existieren und wie sie erreichbar sind, ist der Zeitvorteil weg. Vollständige Asset Inventare, Versionsstände, Netzwerkpläne und klare Owner sind Voraussetzung für schnelle Priorisierung. Exposure Management muss Perimeter Systeme als Hochrisiko Bestand führen und regelmäßig validieren. Damit wird die Scope Bestimmung von Tagen auf Stunden oder Minuten verkürzt.

In der vertieften Analyse wurde mindestens ein System als erfolgreich kompromittiert eingestuft. Nach der RCE-Kette zeigten sich Artefakte, die auf TTPs mit dem Ziel der Extrahierung von Zugangsdaten hindeuteten, einschließlich Hinweisen auf LSASS Dumping. In hybriden Architekturen verschiebt das die Lage schnell in Richtung Identity. Ein kompromittierter SharePoint Server ist selten das Endziel, sondern ein Sprungbrett in privilegierte Kontexte. Entsprechend umfassten die Maßnahmen nicht nur Patchen und Bereinigung, sondern auch umfangreiche Passwort und Secret Rotationen in Entra sowie ergänzende Überwachungsmaßnahmen, um eine fortgesetzte Kompromittierung von Identitäten auszuschließen.

Der Fall stand nicht allein. r-tec bearbeitete 2025 weitere Szenarien rund um Supply-Chain und Abhängigkeiten, darunter Shai Hulud, NPM-Abhängigkeiten und React2Shell. In vielen Fällen lag am Ende keine Betroffenheit vor. Das Problem war dennoch real, weil Unklarheit über den eigenen Bestand und fehlende Übersicht häufig mehr Zeit und Risiko erzeugten als die eigentliche Ausnutzung. Besonders relevant war zudem, dass in mehreren Fällen Patches bereits eingespielt waren, Analysen jedoch dennoch Hinweise auf vorherige Kompromittierung aufdeckten. Die Tür war zu, aber der Angreifer war schon im Gebäude.

Lessons Learned – Bei aktiver Ausnutzung ist Patchen nur ein Zwischenschritt, nicht das Ende (Reaktion & Detektion)

Nach einem Patch muss eine Kompromittierungsprüfung folgen, die typische Artefakte, Webshell Hinweise, verdächtige Uploads und relevante IOCs abdeckt. In hybriden Umgebungen gehört dazu auch die Annahme, dass Zugangsdaten betroffen sein können, inklusive Rotation von Secrets und privilegierten Identitäten. Zusätzliche Überwachung und Hunting sind notwendig, um fortgesetzten Zugriff auszuschließen und Persistenz zu finden. Das Abschlusskriterium ist nicht ein installierter Patch, sondern dass die Umgebung eine vorangegangene Kompromittierung mit hinreichender Wahrscheinlichkeit ausgeschlossen werden kann.

Lagebericht 2025

Still mitgelesen, laut kassiert: Business-E-Mail Compromise über Monate – Der Patch war da, der Angreifer leider auch

Bedrohungsakteur	unbekannt
r-tec Service-Kunde	Nein
Bearbeitungsdauer CERT	140h

Der Vorfall begann nicht mit klassischer Malware, sondern mit einem Täuschungsmanöver, das in modernen M365-Umgebungen besonders wirksam ist: ein sauberer, „legitimer“ Login. Der Initialzugriff erfolgte bereits 2024 über eine geteilte SharePoint-Ressource, konkret eine OneNote-Datei, die als Köder diente. Der Benutzer wurde zur Eingabe von Zugangsdaten und zur MFA-Bestätigung verleitet; in der Rekonstruktion passte die Mechanik zu einem EvilGinx-ähnlichen Framework, das Proxy-basiert Anmeldedaten und Session-Informationen abgreift. Damit war der Angreifer nicht auf wiederholtes Phishing angewiesen, sondern verfügte anschließend über einen stabilen Zugriffspfad.

Lessons Learned – BEC ist ein Langzeitszenario und braucht Telemetrie mit ausreichender Tiefe

Low and slow Angriffe fallen nicht durch Lautstärke auf, sondern durch Abweichungen im Muster, die nur mit guter Retention sichtbar werden. Entra und M365 Logs müssen zentral gesammelt, normalisiert und korreliert werden, idealerweise im SIEM, damit große Zeiträume effizient analysierbar sind. Logniveau und Abdeckung sollten gezielt erweitert werden, etwa um Audit und Graph Aktivitäten, weil sonst relevante Spuren fehlen. Ohne diese Grundlage wird jeder Vorfall zur manuellen Datensammlung statt zur gezielten Untersuchung.

Im Anschluss etablierte der Bedrohungsakteur über Monate einen überwiegend lesenden Zugriff auf ein relevantes E-Mail-Postfach, unterstützt durch automatische E-Mail-Weiterleitungsregeln. Genau diese Zurückhaltung machte den Angriff so schwer greifbar: keine lauten MFA-Fehler, keine auffälligen Download-Spikes – stattdessen „still mitgelesen“. In den verfügbaren Entra-Logs waren seltene Anmeldungen über VPN-IP-Adressen erkenn-

bar, jedoch war ein tiefer Rückblick nur eingeschränkt möglich, weil die Log-Retention nicht ausreichte. Gleichzeitig war die Auswertung außergewöhnlich aufwändig, da kein SIEM angebunden war und Logdaten aus einem großen Tenant über einen langen Zeitraum manuell konsolidiert und korreliert werden mussten. Der Fall zeigte sehr deutlich: Entra- und M365-Telemetrie ist vorhanden, aber ohne zentrale Sammlung, Normalisierung und Korrelation bleibt sie im Ernstfall schwer nutzbar – insbesondere, wenn der Angreifer „low and slow" agiert.

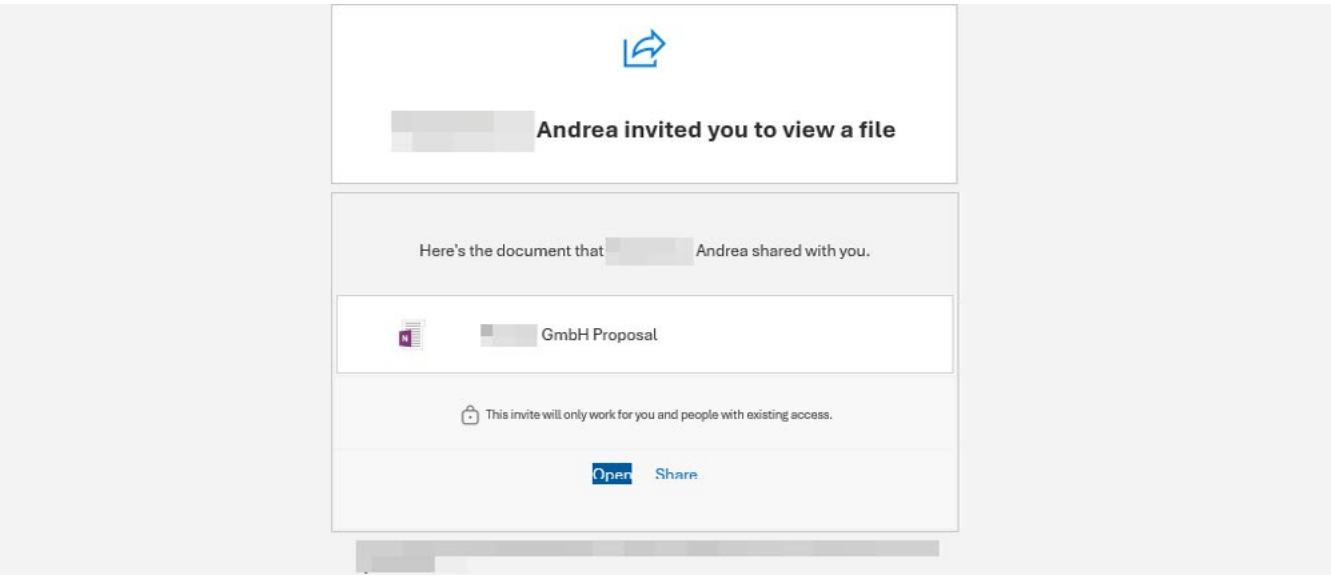


Abbildung 14 – SharePoint Business-E-Mail-Compromise Lure

Die Monetarisierung erfolgte, als eine reale Zahlungsabwicklung anstand. Der Angreifer kannte Zeitpunkt, Kommunikationspartner, Tonalität und Prozessdetails, weil er die Konversation lange beobachtet hatte. Im entscheidenden Moment wurden E-Mail-Inhalte und Dokumente (u. a. PDFs im Kontext der Rechnungs-/Zahlungsfreigabe) so manipuliert bzw. „abgefangen", dass eine Zahlung nicht an den vorgesehenen Empfänger, sondern in den Nahen Osten umgeleitet wurde. Aus einem klassischen BEC wurde damit ein Beinahe-Millionenbetrug. In diesem Fall konnte durch die Einschaltung von Ermittlungsbehörden eine Einfrierung der Gelder erreicht werden – der operative Schaden blieb dennoch erheblich, nicht zuletzt durch forensische Aufarbeitung, Krisenkommunikation und das vollständige Re-Hardening der betroffenen Identitäten und Prozesse.

Lessons Learned – Conditional Access als Sicherheitsgurt (Prävention & Detektion)

Conditional Access reduziert die Wahrscheinlichkeit stabiler Session Missbrauchspfade, wenn Compliant Devices, risikobasierte Policies und Continuous Access Evaluation konsequent genutzt werden. Zusätzlich müssen riskante Anmeldewege und alte Authentifizierungsverfahren restriktiv behandelt werden.

Ausblick 2026

Das Bedrohungsbild hat sich 2025 weniger durch völlig neue Methoden verändert, sondern vor allem durch mehr Geschwindigkeit, bessere Skalierbarkeit und steigenden operativen Druck. Drei Themen werden 2026 aus unserer Sicht besonders prägen:

KI wird operativ und verändert Tempo und Skalierung

2026 wird weniger durch neue Angriffsideen geprägt sein, sondern durch die weitere Operationalisierung von KI. Large Language Models erhöhen die Qualität von Social Engineering, verbessern Phishing und beschleunigen die Erstellung von Malware Bausteinen, Exploits und Hilfswerkzeugen. Der nächste Schritt ist die stärkere Nutzung agentischer Modelle, die Angriffsschritte teilautomatisiert ausführen und Workflows orchestrieren. Das erhöht nicht zwingend die Raffinesse jedes einzelnen Angriffs, aber die Schlagzahl und Anpassungsfähigkeit. Auf der Verteidigungsseite steigt der Druck, SecOps stärker zu automatisieren, Triage zu beschleunigen und Entscheidungen mit Kontextanreicherung zu unterstützen. Wer Signale nicht schnell priorisiert und konsistent reagiert, verliert gegen Tempo.

Identity und reale Angriffspfade rücken weiter in den Mittelpunkt

Bewährte Eintrittswege bleiben relevant. Phishing, Malvertising und Perimeter Schwachstellen in extern erreichbaren Systemen werden weiter genutzt. Gleichzeitig verschiebt sich der Schwerpunkt Richtung Identity. Tokens, Secrets und API Keys sind in modernen Umgebungen oft der schnellste Weg zu weitreichenden Berechtigungen, ohne klassische Schwachstellen auszunutzen. Supply Chain bleibt Normalbetrieb. Häufig ist nicht die Ausnutzung das Problem, sondern die fehlende Übersicht, welche Abhängigkeiten wo existieren. Das verschiebt die Praxis weg vom reinen CVE-Management hin zu Exposure Management entlang realer Angriffspfade. Entscheidend ist weniger, wie viele Schwachstellen existieren, sondern welche erreichbar sind und welche Wirkung sie im Kontext der eigenen Umgebung entfalten.

Layered Security wird zur Betriebsfrage und Sicherheitslösungen konsolidieren

2026 wird sich weiter durchsetzen, dass Einzellösungen zu viele blinde Flecken lassen. Belastbarer Schutz entsteht erst, wenn mehrere Ebenen zusammenspielen und Rückfallmechanismen greifen, etwa EDR, zentrale Auswertung im SIEM und kontinuierliches Threat Hunting. Gleichzeitig wird sich der Markt weiter konsolidieren, weg von vielen Spezialwerkzeugen hin zu Plattformansätzen, die Detection, Identity, Exposure und Response enger verzahnen. Das entlastet aber nur, wenn das Gesamtsystem betriebsfähig ist. Saubere Use Cases, klare Zuständigkeiten, getestete Playbooks und nachvollziehbare Response Ketten bleiben entscheidend.

Lagebericht 2025


© hx | Maurice Fielenbach

An mein Team

Dieser Bericht trägt eure Handschrift. Hinter jeder Zeile stehen echte Vorfälle, lange Nächte, Wochenenden im Einsatz und euer ruhiges, verlässliches Agieren im Chaos. Was ihr 2025 geleistet habt, war konstant stark, hochprofessionell – und in vielen Situationen weit mehr, als man erwarten darf. Ich Danke euch.

Maurice Fielenbach
Head of CERT der r-tec IT Security GmbH

r-tec cyber security
an accompio company

Als Cyber Security Provider mit mehr als 25 Jahren Erfahrung sehen wir Readiness als Kern unserer Leistung: Wir versetzen Unternehmen, Organisationen und Betreiber kritischer Infrastrukturen in die Bereitschaft, Cyberangriffe souverän abwehren zu können.

Dafür konzipieren wir Cyberabwehrstrategien, bieten maßgeschneiderte Cyber Security Services, empfehlen passende Herstellerprodukte und betreiben implementierte Lösungen. Schwerpunkte liegen auf der Vorbeugung, frühzeitigen Erkennung und Abwehr von Cyberangriffen in IT-, OT-, Cloud-, Big-Data- und IoT-Umgebungen.

Unsere Experten greifen dabei auf das Know-how und die Erfahrung aus hunderten Sicherheitsvorfällen pro Jahr zurück. Mit über 90 Mitarbeitern, unserem Security Operations und Cyber Defence Center bieten wir alle wichtigen Ressourcen, Technologien und Services, um unsere Kunden in die nötige Bereitschaft zu versetzen – ready to protect, ready to respond, ready to perform.

Als integraler Bestandteil der accompio Gruppe nimmt r-tec seit August 2024 die führende Rolle für Cyber Security innerhalb der Gruppe ein.

r-tec IT Security GmbH | Hatzfelder Str. 165–167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100