

# StegoMalware – Scores from MITRE

Aus dem Projekt ATTRIBUT (<https://attribut.cs.uni-magdeburg.de/>)

## Attribution von verdeckten (Informations-)Kanälen im Bereich kritischer Infrastrukturen und Potentiale für Prävention und Reaktion

### Herausforderung:

Verdeckte Informationskanäle spielen eine Rolle bei komplexen Angriffen und erlauben den Angreifern Persistenz in Zielsystemen und damit langfristige Bedrohung.

Aktuelles Beispiel: **Volt Typhoon** (Siehe Darstellung auf der rechten Seite)

### Ansatz dieser Arbeit:

Aufbereitung des MITRE ATT&CK® Frameworks zur Identifikation konkreter Umsetzungen verdeckter Informationskanäle als Grundlage für Identifikation und Attribution.

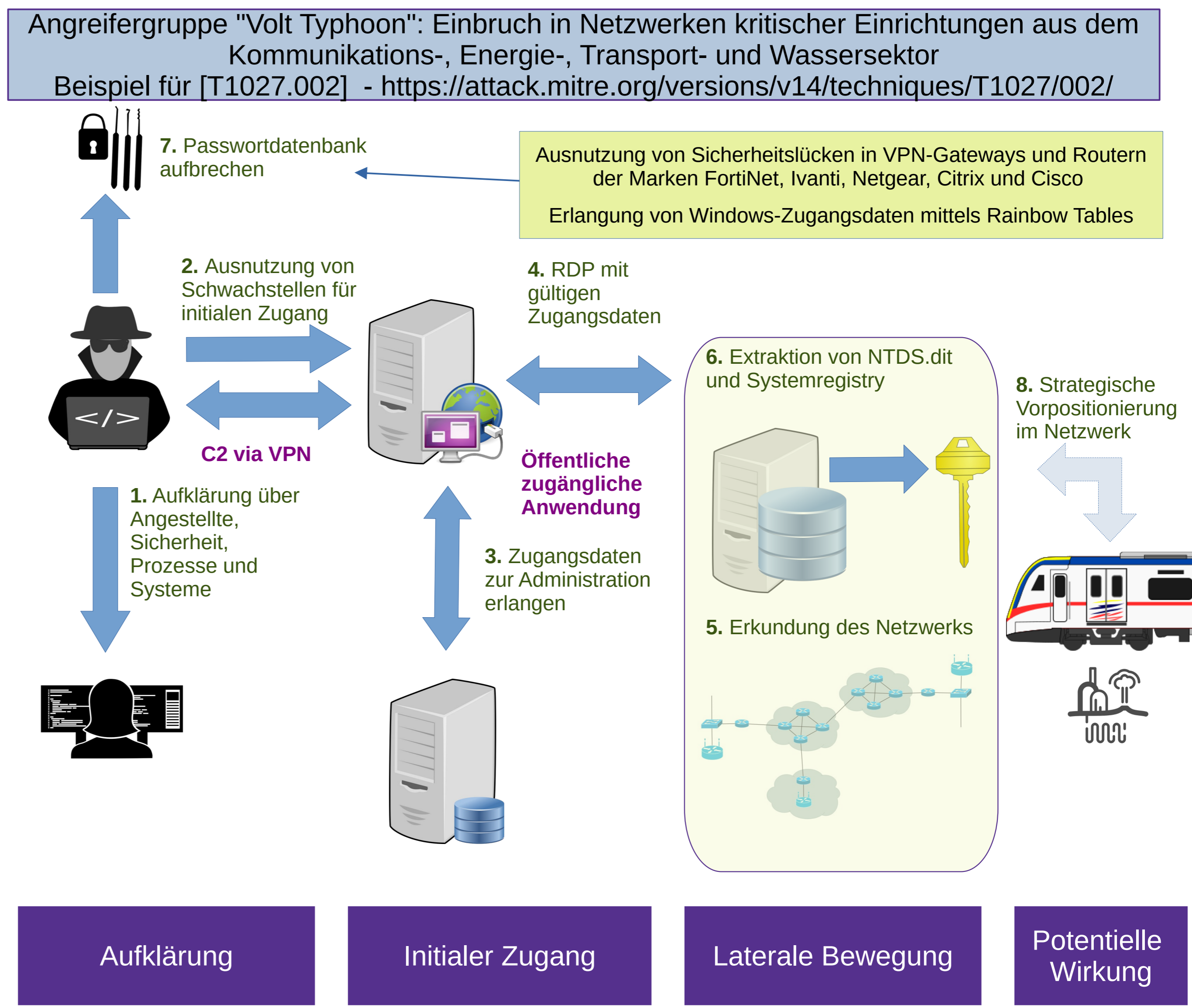
Verwendung der Techniken **T1001.002 Data Obfuscation: Steganography** und **T1027.003 Obfuscated Files or Information: Steganography**, aufbereitet aus dem MITRE ATT&CK® Framework <https://attack.mitre.org/>

### Ergebnis:

Vergleichstabelle über Beispiele in denen die Techniken T1001.002 und T1027.003 sowie deren Sub-Techniken zum Einsatz kommen. Dabei werden unterschiedliche Covertypen (Bild, Text/PDF, Audio) betrachtet.

Beispiele für T1001.002 und Subtypen: 48  
 Beispiele für T1027.003 und Subtypen: 593  
 Gemeinsame Vorkommen: 39

	T1001	T1001.001	T1001.002	T1001.003
T1001	7	1	1	0
T1001.001	1	15	1	2
T1001.002	1	1	11	1
T1001.003	0	2	1	15



Basisabbildung aus [1] [https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure\\_1.pdf](https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf)  
 [2] <https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques> - 15.2.2024

### Gemeinsames Vorkommen von T1001 und Sub-Techniken

	T1027	T1027.001	T1027.002	T1027.003	T1027.004	T1027.005	T1027.006	T1027.007	T1027.008	T1027.009	T1027.010	T1027.011	T1027.012
T1027	308	25	58	12	6	11	2	4	0	4	21	21	0
T1027.001	25	36	10	2	1	2	2	0	0	0	6	4	0
T1027.002	58	10	88	4	1	5	2	1	0	2	7	5	0
T1027.003	12	2	4	28	1	0	0	0	0	1	2	2	0
T1027.004	6	1	1	1	7	0	0	0	0	0	3	1	0
T1027.005	11	2	5	0	0	17	1	0	0	0	5	2	0
T1027.006	2	2	2	0	0	1	3	0	0	0	1	1	0
T1027.007	4	0	1	0	0	0	0	5	0	0	0	0	0
T1027.008	0	0	0	0	0	0	0	1	1	0	0	0	0
T1027.009	4	0	2	1	0	0	0	1	11	5	2	0	0
T1027.010	21	6	7	2	3	5	1	0	0	5	59	8	0
T1027.011	21	4	5	2	1	2	1	0	0	2	8	29	0
T1027.012	0	0	0	0	0	0	0	0	0	0	0	0	0

### Gemeinsames Vorkommen von T1027 und Sub-Techniken

T1027.003	C0023	Operation Ghost	During Operation Ghost, APT29 used steganography to hide the communications between the implants and their C&C servers.	Bild	T1001.002
T1027.003	C0005	Operation Spalax	For Operation Spalax, the threat actors used packers that read pixel data from images contained in PE files' resource sections and build the next layer of execution from the data.	Bild/PE	
T1027.003	S0518	PolyglotDuke	PolyglotDuke can use steganography to hide C2 information in images.	Bild	
T1027.003	S0139	PowerDuke	PowerDuke uses steganography to hide backdoors in PNG files, which are also encrypted using the Tiny Encryption Algorithm (TEA).	Bild/PNG Bild/JPG Bild/BMP	
T1027.003	S0654	ProLock	ProLock can use .jpg and .bmp files to store its payload.		
T1027.003	S0565	Raindrop	Raindrop used steganography to locate the start of its encoded payload within legitimate 7-Zip code.		
T1027.003	S0458	Ramsay	Ramsay has PE data embedded within JPEG files contained within Word documents.	Bild/JPEG	
T1027.003	S0495	RDAT	RDAT can process steganographic images attached to email messages to send and receive C2 commands. RDAT can also embed additional messages within BMP images to communicate with the RDAT operator.	Bild/BMP	T1001.002
T1027.003	S0511	RegDuke	RegDuke can hide data in images, including use of the Least Significant Bit (LSB).	Bild	
T1027.003	G0127	TA551	TA551 has hidden encoded data for malware DLLs in a PNG.	Bild/PNG	
T1027.003	G0081	Tropic Trooper	Tropic Trooper has used JPG files with encrypted payloads to mask their backdoor routines and evade detection.	Bild/JPG	

### Detailansicht: Vorkommen von T1027 und Sub-Techniken

#### Fazit:

Beobachtete Beispiele für spezifische Angriffe oder Schadsoftware setzen häufig mehr als nur eine Technik oder Sub-Technik zur Verwendung verdeckter Informationskanäle ein. Dabei kommt eine große Bandbreite von Techniken oder Sub-Techniken zum Einsatz.

Das hat Implikationen auf das Bedrohungsbild und führt dazu, dass eine Verteidigung bis in die Tiefe des Netzwerkes und nachgeordneter Systeme angebracht ist um zu verhindern dass Schadwirkungen gegen nachgeordnete cyber-physikalische Systeme angewendet werden können.

### Anstehende Veröffentlichung:

**BSI Sicherheitskongress 2024** -- Dr.-Ing. Robert Altschaffel, Dr.-Ing. Stefan Kiltz, Kevin Lamshöft, Prof. Dr.-Ing. Jana Dittmann: Paper SYNTHESIS und ATTRIBUT Projektbeiträge angenommen: ICS/OT-Sicherheit: Evaluation und Validierung der Erkennungsleistung von Stego-Malware in industriellen Steuernetzwerken mittels Synthese und Simulation,

**GI Sicherheit 2024 Practitioners Track** -- Jana Dittmann, Christian Krätzer, Stefan Kiltz, and Robert Altschaffel (Otto-von-Guericke Universität); Claus Vielhauer (TH Brandenburg); Steffen Wendzel (HS Worms); Sandro Wefel (MLU Halle); Holger Nitsch (HFOED Bayern) Attribution von verdeckten (Informations-)Kanälen im Bereich kritischer Infrastrukturen und Potentiale für Prävention und Reaktion (ATTRIBUT):



Diese Studie/Forschungsarbeit wurde durch die Agentur für Innovation in der Cybersicherheit GmbH im Rahmen des Vorhabens Forschung zu „Existenzbedrohenden Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien“ beauftragt und finanziert. Eine Einflussnahme der Agentur für Innovation in der Cybersicherheit GmbH auf die Ergebnisse fand nicht statt.