SOPHOS

# Active Adversary Playbook 2022

## Verhaltensweisen, Taktiken und Tools von Cyberangreifern, die 2021 in der Incident-Response-Praxis beobachtet wurden

Autor: **John Shier**, Senior Security Advisor, CTO Office

*Sophos-Whitepaper Juni 2022*

# Einleitung

Unternehmen und Einrichtungen vor immer neuen, zunehmend komplexen Cyberbedrohungen zu schützen, kann eine echte Herausforderung sein. Denn Angreifer passen ihr Verhalten und ihre Tools ständig an aktuelle Gegebenheiten an und entwickeln sie weiter. Außerdem nutzen sie sofort neue Schwachstellen aus und zweckentfremden gewöhnliche IT-Tools, um unerkannt zu bleiben und Sicherheitsteams stets einen Schritt voraus zu sein.

Daher ist es für IT- und Sicherheitsexperten keine leichte Aufgabe, mit der Geschwindigkeit dieser modernen Angreifer mitzuhalten. Insbesondere wenn sie mit gezielten, aktiven Angriffen konfrontiert werden, an denen mehr als ein Täter beteiligt ist: zum Beispiel ein Initial Access Broker (IAB), der in ein Zielsystem eindringt und seinen Zugang anschließend an eine Ransomware-Gang verkauft, die diesen wiederum für ihren eigenen Angriff nutzt.

Das Active Adversary Playbook 2022 beschreibt die wichtigsten Angreifer, Tools und Vorgehensweisen, die 2021 von Sophos-Experten in der Praxis beobachtet wurden. Es knüpft an das Active Adversary Playbook 2021 an und zeigt, wie sich die Angriffslandschaft weiterentwickelt hat.

Ziel des neuen Almanachs ist es, Sicherheitsteams dabei zu unterstützen, Angriffstaktiken besser zu verstehen sowie schädliche Aktivitäten in Netzwerken effektiver zu erkennen und abzuwehren.

Die Ergebnisse basieren auf Daten von Vorfällen, die vom Sophos Rapid-Response-Team im Jahr 2021 untersucht wurden. Diese werden, insofern möglich, mit den Incident-Response-Erkenntnissen aus dem Active Adversary Playbook 2021 verglichen.

# Incident-Response-Daten 2021

Der Report basiert auf 144 Vorfällen, die sich in Unternehmen und Einrichtungen verschiedenster Größe in einer Vielzahl von Branchen und Ländern ereignet haben. So gehörten Organisationen aus den USA, Kanada, Großbritannien, Deutschland, Italien, Spanien, Frankreich, Schweiz, Belgien, den Niederlanden, Österreich, den Vereinigten Arabischen Emiraten, Saudi-Arabien, den Philippinen, den Bahamas, Angola und Japan zu den Opfern.

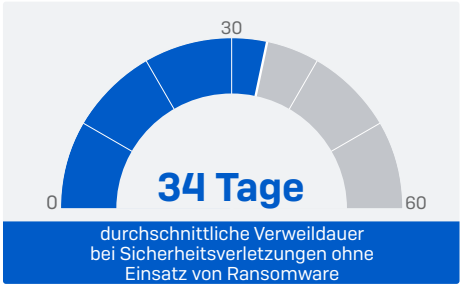
Die am stärksten betroffenen Bereiche waren Fertigung und Produktion (17 % der Incident-Response-Fälle), gefolgt vom Einzelhandel (14 %), Gesundheitswesen (13 %), IT-Sektor (9 %), Bauwesen (8 %) und Bildungswesen (6 %). Zusätzliche Informationen finden Sie in den Datentabellen am Ende dieses Reports.

# Dashboard: Anatomie aktiver Angriffe im Jahr 2021

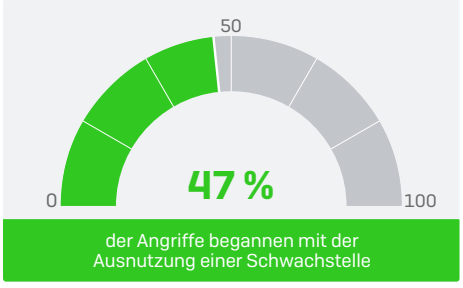
Im März und August 2021 wurde vor den Sicherheitslücken ProxyLogon und ProxyShell auf Microsoft-Exchange-Servern gewarnt, deren Schwachstellen sich als besonders folgenschwer erwiesen haben. Wie kürzlich von der CISA und anderen staatlichen Sicherheitsbehörden gemeldet, wurden die ProxyLogon/ProxyShell Bugs extensiv von Angreifern ausgenutzt. Es überrascht daher nicht, dass diese Schwachstellen auch der Grund für eine beträchtliche Anzahl der von Sophos 2021 untersuchten Vorfälle waren.

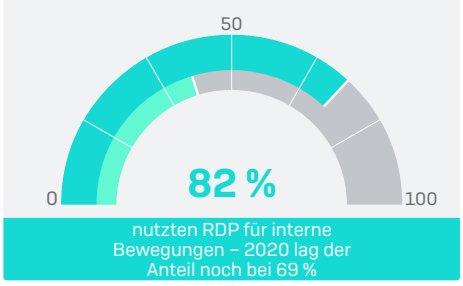
## Dashboard: Anatomie aktiver Angriffe im Jahr 2021

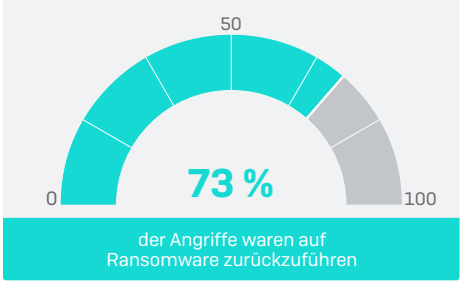
Wichtigste Erkenntnisse aus den Incident-Response-Analysen

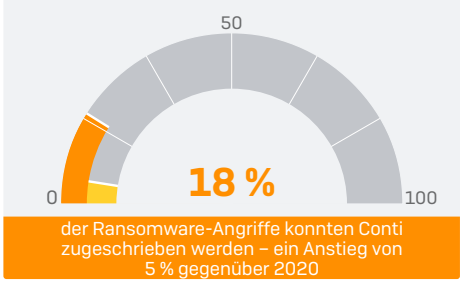



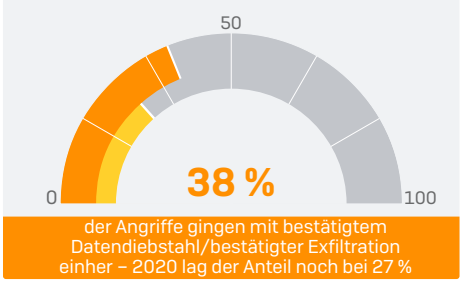




Vermutlich gibt es viele weitere, bislang noch unbekannte ProxyLogon/ProxyShell-Sicherheitsverstöße, bei denen Web-Shells und Backdoors für den dauerhaften Zugang zu Opfersystemen implantiert wurden und jetzt still darauf warten, dass dieser Zugang verwendet oder verkauft wird.

Hierbei kommt eine weitere wichtige Entwicklung zum Tragen, von der die Cyberbedrohungs-Landschaft 2021 geprägt war: dem wachsenden Einfluss und der zunehmenden Macht von Initial Access Brokern (IABs).

Das Geschäftsmodell von IABs besteht darin, neu geschaffene Zugänge zu Opfersystemen zu verkaufen. Somit hängt ihr Erfolg davon ab, ob es ihnen gelingt, als erstes die Abwehr eines anfälligen Ziels zu durchbrechen. Demzufolge werden IABs häufig am Schauplatz neu gemeldeter Bugs beobachtet, wo sie versuchen, noch ungepatchte Ziele zu kompromittieren. Ihr Ziel ist es, auf einem Opfersystem Fuß zu fassen und möglicherweise erste Erkundungsschritte vorzunehmen, um den Wert des verschafften Zugangs zu bemessen. Diesen Zugang verkaufen die IABs anschließend an andere Angreifer (z. B. Ransomware-Betreiber), die manchmal erst Monate nach der ersten Kompromittierung weitere Angriffe auf das Ziel starten.

Wie im Sophos 2022 Threat Report beschrieben, spiegelt die wachsende Verbreitung von IABs die zunehmende „Professionalisierung" von Angriffen in einem Cyberbedrohungs-Markt wider, in dem immer mehr spezialisierte Dienstleister agieren. Ein weiteres Beispiel für diesen Trend ist das florierende RaaS-Geschäft („Ransomware as a Service").

Nicht zuletzt haben forensische Beweise im Rahmen von Incident-Response-Analysen 2021 gezeigt, dass in einigen Fällen mehrere Angreifer, darunter IABs, Ransomware-Gangs, Cryptominer und gelegentlich sogar mehrere Ransomware-Akteure, gleichzeitig auf dieselbe Organisation abzielten. Diese Entwicklung wird die Cyberbedrohungs-Landschaft auch 2022 und in den kommenden Jahren prägen.

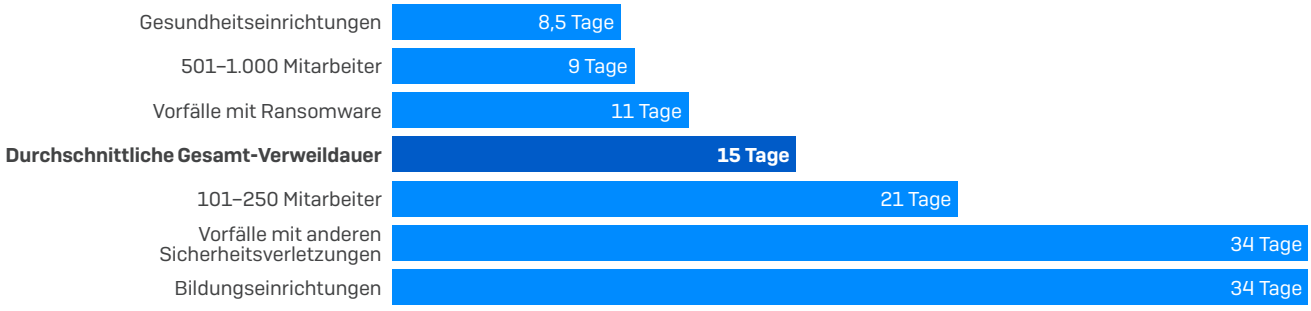
Mittlerweile verweilen die Eindringlinge länger in den Netzwerken ihrer Opfer. Dies ist aller Wahrscheinlichkeit nach auf die oben beschriebenen Angriffe mit mehreren Akteuren zurückzuführen. Weitere Angreifer, die sich über einen längeren Zeitraum und manchmal gleichzeitig in Opfernetzwerken aufhalten, sind Botnet Builder und Malware-Delivery-Plattformen oder Dropper.

Auf diese Entwicklungen gehen wir im Folgenden näher ein.

# Unsichtbare Eindringlinge

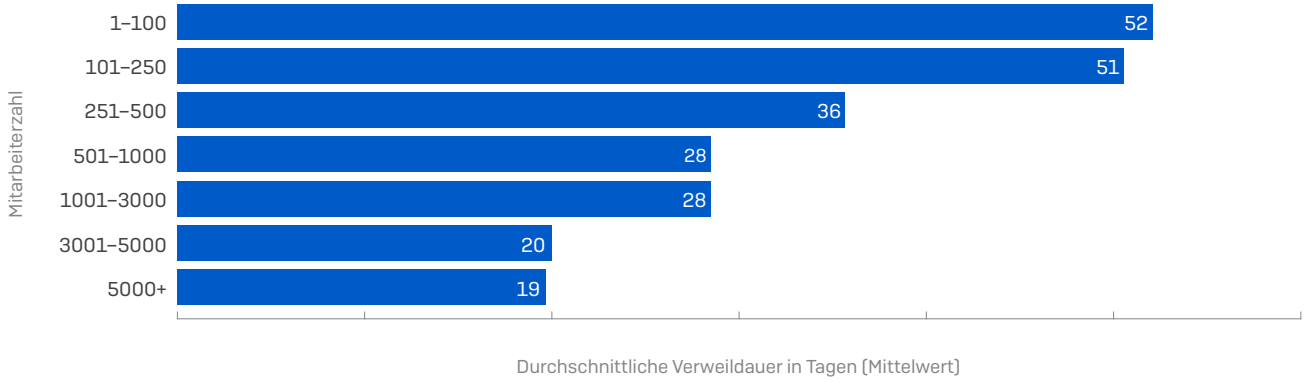
Daten zu Sicherheitsverletzungen zeigen, dass die durchschnittliche Verweildauer (Median) zwischen 2020 und 2021 um etwa ein Drittel, d. h. von 11 Tagen auf 15 Tage, gestiegen ist. Dabei gab es erhebliche Unterschiede hinsichtlich der Verweildauer: Angreifer, die Ransomware verbreiten wollten, verweilten durchschnittlich 11 Tage (2020 waren es noch 18 Tage), während die durchschnittliche Verweildauer (Median) bei anderen Sicherheitsverletzungen mit 34 Tagen deutlich länger ausfiel.

### Unterschiede bei der durchschnittlichen Verweildauer von Eindringlingen (Median)



Wie zuvor erwähnt, könnten die längeren Verweilzeiten auf IABs zurückzuführen sein. Bei kleineren Unternehmen oder Bereichen wie dem Bildungswesen (durchschnittliche Verweildauer von Eindringlingen: 34 Tage) sind die längeren Verweilzeiten auch ein Zeichen dafür, wie schwierig es für interne IT-Sicherheitsmitarbeiter ist, verdächtige Warnmeldungen und potenzielle Bedrohungen proaktiv aufzuspüren, zu analysieren und darauf zu reagieren.

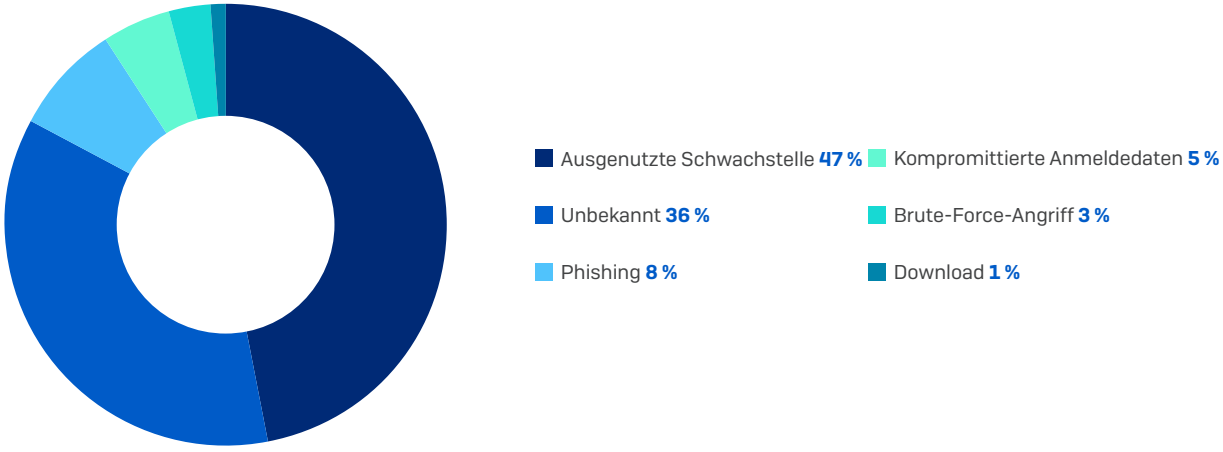
### Verweildauer von Eindringlingen nach Unternehmensgröße (Mittelwert)




## Ursachen von Angriffen

Es ist nicht immer möglich oder einfach, der Ursache eines Angriffs auf den Grund zu gehen. Manchmal haben die Angreifer absichtlich Beweise ihrer Aktivitäten vernichtet und in einigen Fällen hat das IT-Sicherheitsteam kompromittierte Computer bereits bereinigt oder neue Images aufgespielt, wenn die Response-Experten sich an die Arbeit machen. Dessen ungeachtet konnte Sophos bei fast der Hälfte (47 %) der 2021 analysierten Cybervorfälle die Ausnutzung ungepatchter Schwachstellen – wie ProxyLogon oder ProxyShell – als Ursache nachweisen.

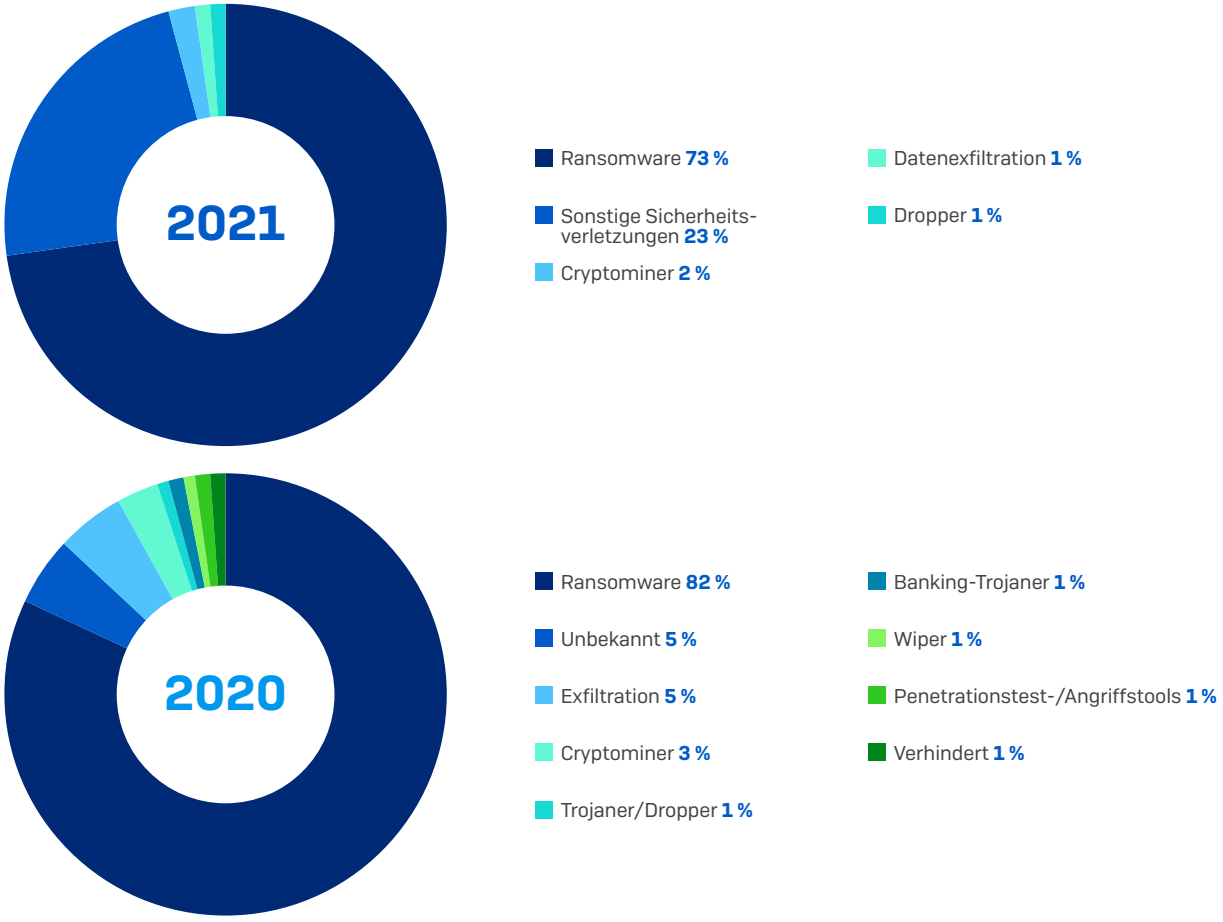
### Ursachen von Angriffen



# Häufigste Angriffstypen

Häufig bemerken IT-Sicherheitsteams einen Ransomware-Angriff erst, wenn die Schadsoftware bereits in Umlauf gebracht wurde. Es verwundert daher kaum, dass bei 73 % der Vorfälle, auf die Sophos im Jahr 2021 reagierte, Ransomware im Spiel war. Ransomware war auch im Jahr 2020 der häufigste Angriffstyp, damals mit 82 % (die höhere Zahl liegt vermutlich an der kleineren Datenbasis). Im Falle von Datenexfiltrationen, die für 1 % der Vorfälle verantwortlich waren, gehen die Response-Experten davon aus, dass sich diese vermutlich zu Ransomware-Angriffen entwickelt hätten, jedoch rechtzeitig erkannt und beseitigt wurden.

### Angriffstypen




23 % der Vorfälle fielen unter die allgemeine Kategorie „sonstige Sicherheitsverletzungen". Im Rahmen dieses Reports wurden dieser Kategorie Sicherheitsverletzungen zugeordnet, die nicht zu Ransomware oder einem anderen nachverfolgten Angriffstyp geführt haben.

Sicherheitsverletzungen sind oft auf die Ausnutzung ungepatchter Schwachstellen wie ProxyLogon oder ProxyShell zurückzuführen, oder aber auch auf die missbräuchliche Nutzung von RAS-Diensten oder unsicheren VPNs. Aber auch gestohlene Konto-Anmeldeinformationen oder Sicherheitsfehler (z. B. über das Internet öffentlich zugängliche Eintrittspunkte) können die Ursache sein.

Der entscheidende Punkt ist, dass die Sicherheitsverletzungen erkannt und beseitigt wurden, bevor ein umfangreicher Payload auf das Zielsystem eingeschleust werden konnte. Aller Wahrscheinlichkeit nach handelte es sich bei einigen oder sogar den meisten dieser Sicherheitsverletzungen um „Überbestände" von IABs: also „ergaunerte" Zugänge, die noch nicht an einen anderen Angreifer verkauft wurden. Wären die Sicherheitsverletzungen unentdeckt geblieben, hätte sich vermutlich ein beträchtlicher Teil zu Ransomware-Angriffen entwickelt.

Cryptominer waren bei 2 % der untersuchten Vorfälle der Hauptangriffstyp. Schädliche Cryptominer werden häufig durch ihre Beeinträchtigung der Systemleistung erkannt, da das illegale Coin Mining Rechenleistung von Computern abzieht. Es kann verlockend sein, Cryptominer als lästige Bedrohung von geringer Bedeutung abzutun. Ihre Präsenz im Netzwerk beweist jedoch, dass es irgendwo einen anfälligen Eintrittspunkt gibt. Cryptominer können daher ein Vorbote für ernstere Bedrohungen sein.

Gleiches gilt allgemein für Dropper und Malware-Delivery-Systeme, die für die Bereitstellung, das Laden oder die Installation anderer schädlicher Payloads auf Zielsystemen konzipiert sind. Sie machen die Ausbreitung eines Angriffs überhaupt erst möglich und bieten eine Plattform für zusätzliche schädliche Module wie Backdoors und Ransomware. Analysten müssen daher die Präsenz von Droppern und Malware-Delivery-Systemen wie Trickbot und Emotet genauso ernst nehmen wie eine große Ransomware-Gruppe, da sie nicht selten die Vorboten größerer Angriffe sind.

## Eine überfüllte Kampfarena

Angriffstypen schließen sich nicht gegenseitig aus. Wie bereits erwähnt, können mehrere Angreifer, darunter IABs, Ransomware-Gangs und Cryptominer, gleichzeitig in einem einzigen Zielnetzwerk präsent sein.

Cryptominer waren beispielsweise in nur 2 % der Incident-Response-Fälle der Hauptangriffstyp, jedoch auch in 7 % der Ransomware-Fälle vorhanden. Cryptominer suchen in infizierten Netzwerken oft nach anderen Minern und entfernen diese, können aber auch problemlos mit weiteren Bedrohungen wie Ransomware koexistieren.

Zu den von Sophos im Jahr 2021 gemeldeten gleichzeitigen Angriffsereignissen gehörten Atom-Silo-Ransomware und zwei Cryptominer sowie ein Ransomware-Doppelangriff mit Netwalker und REvil. Dieser Trend setzt sich auch im Jahr 2022 fort.

# Der Werkzeugkoffer von Angreifern

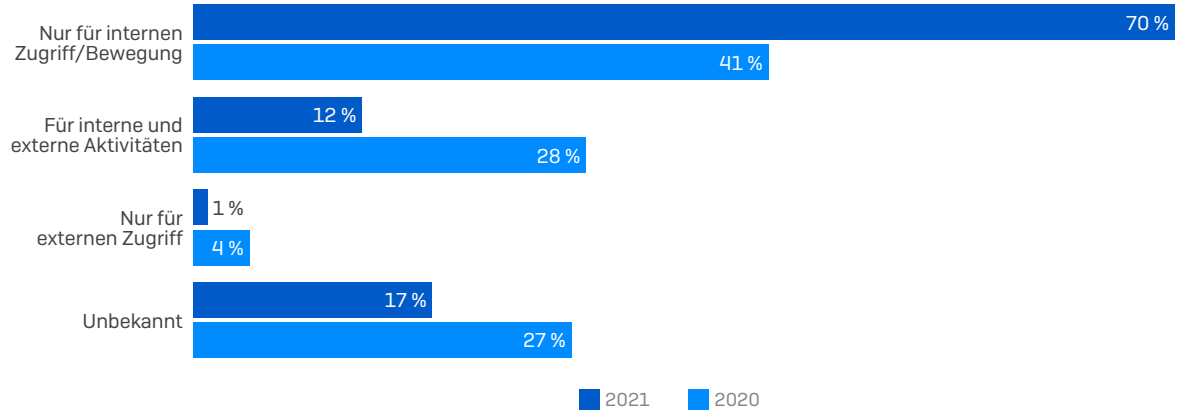
## Remote Desktop Services sind eine große interne Bedrohung

Im Jahr 2021 spielte RDP bei mindestens 83 % der Angriffe eine Rolle, ein Anstieg von 10 % gegenüber dem Vorjahr. In 82 % der Fälle wurde eine interne Verwendung festgestellt, in 13 % der Fälle eine externe Verwendung. Im Jahr 2020 lag die interne Verwendung bei 69 %, die externe Verwendung bei 32 %.

Hierbei sollte allerdings die Art und Weise, wie Angreifer RDP verwendeten, berücksichtigt werden: Bei fast 70 % der Vorfälle, in denen RDP involviert war, wurde das Tool *nur* für den internen Zugriff und zur lateralen Bewegung genutzt – ein deutlicher Anstieg gegenüber 2020, als dieser Anteil noch bei 41 % lag.

RDP wurde in nur *1 %* der Fälle für den externen Zugriff verwendet, im Vergleich zu 4 % im Jahr 2020; und bei nur 12 % der Angriffe nutzten die Angreifer RDP sowohl für den externen Zugriff als auch für interne Bewegungen. Dieser Anteil hat sich gegenüber 2020 mehr als halbiert (damals waren es noch 28 %).

### Ausnutzung von Remote Desktop Protocol (RDP)



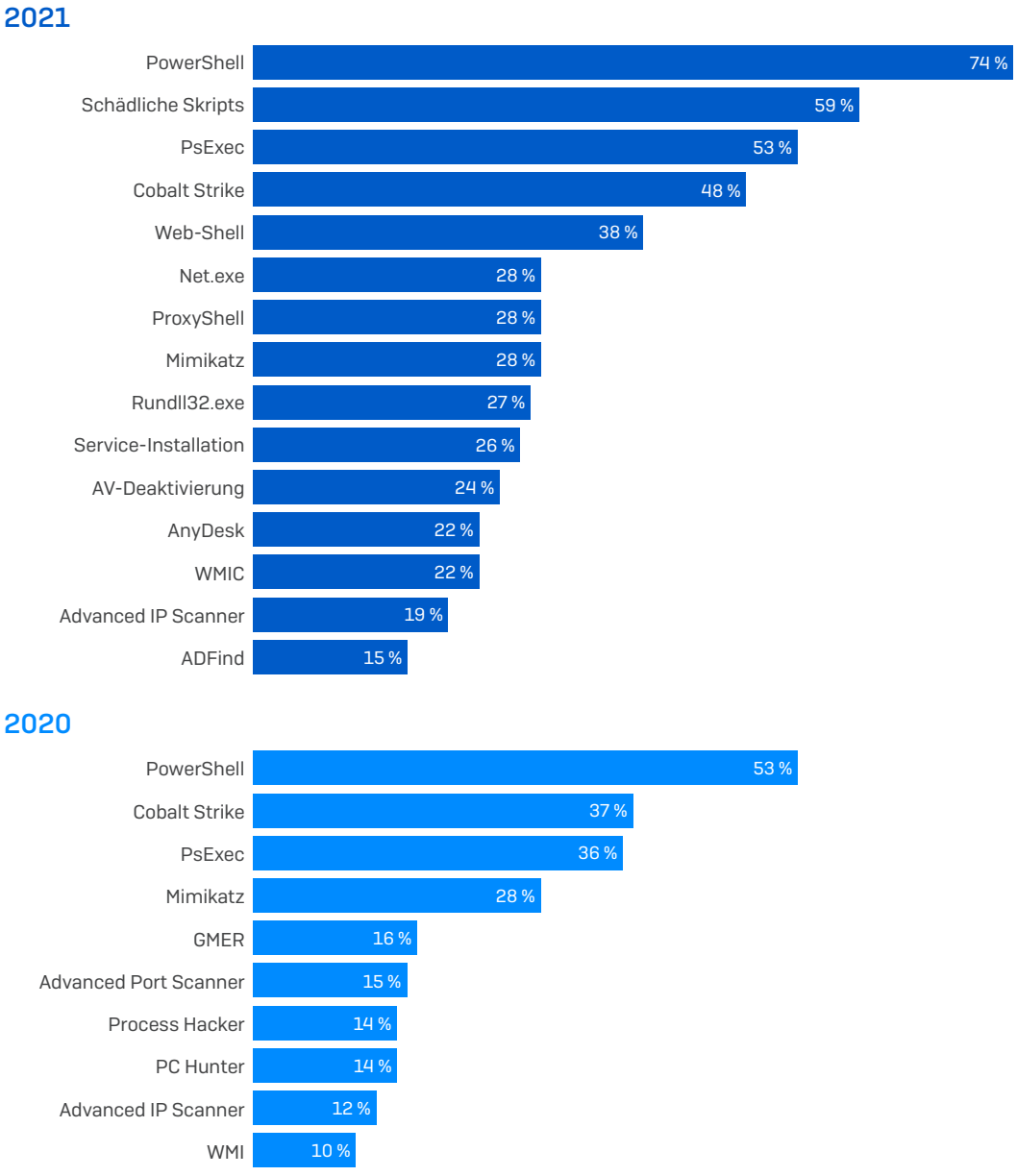

Die seltenere Ausnutzung von RDP für den externen Zugriff ist vermutlich auf bessere Sicherheitsmaßnahmen zurückzuführen (u. a. Deaktivierung dieses Service). RDP bleibt jedoch innerhalb der Netzwerkgrenzen weithin zugänglich und die Absicherung dieses Zugangs sollte ein Hauptaugenmerk für Sicherheitsteams sein.

## Die Angriffswerkzeuge im Jahr 2021

Das folgende Diagramm zeigt die beliebtesten „Artefakte“, einschließlich Tools, Techniken und Services, von Angreifern im Jahr 2021. Viele dieser Anwendungen können auch von IT-Experten für legitime Zwecke genutzt werden. Sie sind bei Angreifern beliebt, weil mit ihnen u. a. Aktivitäten wie Diebstahl von Anmeldeinformationen, Systemermittlung, laterale Bewegungen und Malware-Ausführung vorgenommen werden können, während gleichzeitig der Anschein erweckt wird, dass die Anwendung nur für harmlose IT-Zwecke genutzt wird.

Die Anzahl und Art der Artefakte verdeutlichen die Herausforderung, mit der sich Analysten bei der Unterscheidung zwischen schädlichen und legitimen Aktivitäten im Netzwerk konfrontiert sehen.

### Die häufigsten bei Angriffen genutzten Artefakte




Eine genauere Betrachtung der beliebtesten Angreifertools offenbart detaillierte Einblicke in die typischen Cyberangriffs-Strategien des Jahres 2021.

## Kategorien von Artefakten

Die bei Incident-Response-Analysen identifizierten Artefakte lassen sich in drei Kategorien unterteilen: Legitime und Hacking-Tools, Microsoft-Binärdateien und zusätzliche Artefakte (Skripts, Techniken, Dienste usw.).

Die Incident-Response-Analysen ergaben insgesamt 525 verschiedene Artefakte, gegenüber 132 im Jahr 2020 (allerdings war der Stichprobenumfang auch größer), darunter 209 legitime und Hacking-Tools, 107 Microsoft-Binärdateien und 209 zusätzliche Artefakte.

### Legitime und Hacking-Tools

In diese Kategorie fällt auch Software, die zur Unterstützung des Angriffsgeschehens zum Einsatz kam. Cobalt Strike (48 %) und Mimikatz (28 %) belegen wie schon 2020 die beiden ersten Plätze, gefolgt von AnyDesk (22 %), Advanced IP Scanner (19 %) und ADFind (15 %). Im Vergleich zu 2020 hat Cobalt Strike seinen Anteil erhöht (vormals 37 %), Mimikatz ist stabil geblieben (28 %) und drei neue Tools haben es in die Top 5 geschafft.

**Cobalt Strike** ist eine kommerziell produzierte Exploitation Tool Suite, die Sicherheitsteams bei der Erstellung diverser Angriffsszenarien unterstützen soll. Angreifer versuchen, eine Cobalt Strike „Beacon" Backdoor auf einem infizierten Computer einzurichten. Beacons können so konfiguriert werden, dass sie Befehle ausführen, zusätzliche Software herunterladen und ausführen, Befehle an andere Beacons weiterleiten, die in einem Zielnetzwerk installiert sind, und zurück an den Cobalt-Strike-Server kommunizieren. Jede Erkennung von Cobalt Strike im Netzwerk sollte umgehend untersucht werden.

Das am zweithäufigsten beobachtete Tool **Mimikatz** wurde ursprünglich als Tool für offensive Sicherheitsmaßnahmen konzipiert und kann Passwörter und andere Konto-Anmeldeinformationen stehlen, um diese für Angriffe zu missbrauchen.

Mit legitimen Netzwerkscannern wie **Advanced Port Scanner** und **IP Scanner** lassen sich Listen von IP- und Gerätenamen generieren. So sind die Angreifer in der Lage, sich ein genaues Bild über die wichtigsten Systeme und Infrastrukturen in der Zielumgebung zu verschaffen.

Auch das legitime IT-Verwaltungstool **AnyDesk** wird immer häufiger zweckentfremdet, da es Angreifern die direkte Kontrolle über Zielcomputer verschafft, einschließlich der Kontrolle über die Maus/Tastatur und der Möglichkeit, den Bildschirm zu sehen. Legitime RAS-Dienste wie **TeamViewer**, **Screen Connect**, **Atera RMM** und **Splashtop** erfreuen sich seit 2021 ebenfalls zunehmender Beliebtheit.

**Process Hacker**, **PCHunter** und **GMER** sind alle legitime Tools, die Kernel-Treiber enthalten. Wenn ein Angreifer den richtigen Kernel-Treiber installiert, kann er häufig Sicherheitsprodukte deaktivieren.

### Microsoft-Binärdateien

Dass Microsoft-Tools bei diesen Untersuchungen überhaupt als separate Kategorie geführt werden, zeigt einmal mehr, wie häufig Angreifer für ihre Machenschaften auf systemeigene Programme zurückgreifen. Diese Tools sind alle von Microsoft digital signiert. **PowerShell** (74 %) führt die Liste erwartungsgemäß an, gefolgt von **PsExec** (53 %), „**net.ex**e" (28 %), „**rundll32.exe**" (27 %) und dem **WMI Command-line** (WMIC) Tool (22 %). Der Einsatz von PowerShell, PsExec und WMIC nahm im Jahr 2021 im Vergleich zum Vorjahr zu.

Das Tool „net.exe" wurde in vielen Angriffsphasen verwendet, am häufigsten als Ermittlungstool, während „rundll32.exe" extensiv zur Ausführung und Umgebung der Abwehr genutzt wurde.

Weitere Microsoft-Tools, die auf einen Angreifer im Netzwerk hindeuten könnten, sind „**whoami.exe**", der **Taskplaner** (zur Aufrechterhaltung der Persistenz) und „**schtasks.exe**" (zur Ausführung von schädlichem Code). Die Verwendung solcher Tools sollte deshalb genaustens überwacht werden.

### Zusätzliche Artefakte

Diese Kategorie umfasst sowohl Tools als auch Techniken, u. a. Versuche, den Schutz zu deaktivieren, Schwachstellen wie ProxyShell, den Einsatz von Cloud-Diensten wie **Mega.io**, das Auffinden zusätzlicher Malware, sekundäre Infektionen und verwendete Transportprotokolle.

**Schädliche Skripts** (mit Ausnahme von PowerShell) wurden in 59 % der untersuchten Vorfälle beobachtet. Schädliche Skripts sind Software-Code, der schädliche Aktivitäten ermöglicht. Beispiele für Skripts, die von Angreifern zweckentfremdet werden, sind DOS/CMD-Batch- und Befehlszeilen-Skripts, Python-Skripts (Sammlung von Befehlen in einer Datei, die wie ein Programm ausgeführt werden) und VBScripts (Visual-Basic-Skripts, die in Windows oder Windows Explorer ausgeführt werden können).

Web-Shells waren die zweithäufigste Bedrohungsart (bei 38 % der Vorfälle), ProxyShell (28 %) und ProxyLogon (11 %) stachen bei den Untersuchungen ebenfalls hervor. Service-Installationen, Schutz-Deaktivierungen, LSASS-Auslesungen, Einrichtungen nicht autorisierter Konten, Manipulationen der Registry und Löschungen von Protokollen runden die Top 10 ab.

## Datenexfiltration

2021 nahm **Rclone** Einzug in die Liste der wichtigsten zur Exfiltration genutzten Artefakte. Rclone ist ein Befehlszeilentool, das mit einer Vielzahl von Cloud-Speicheranbietern wie Mega verknüpft werden kann. Es war 2021 das am häufigsten verwendete Tool zur Datenexfiltration. Andere in den diesjährigen Daten vertretene Cloud-Speicheranbieter sind **Dropbox** , **DropMeFiles**, **M247**, **pCloud** und **Sendspace**.

Neben Rclone wurden bei Vorfallsanalysen zur Exfiltration von Daten auch die Tools **MEGAsync**, **FileZilla**, **Handy Backup**, **StealBit**, **WinSCP** und **Ngrok** beobachtet.

Dass Exfiltrationstools 2021 in der Top-Liste vertreten waren, verwundert kaum, wenn man bedenkt, dass bei 38 % aller untersuchten Vorfälle Daten exfiltriert wurden (2020 waren es noch 27 %). Bei einer Reihe weiterer Vorfälle (insgesamt 8 %) wurden Anzeichen dafür gefunden, dass Daten erfasst und auf eine mögliche Abschöpfung vorbereitet wurden. In Fällen erfolgreicher Datenexfiltrationen deuteten Indizien darauf hin, dass die gestohlenen Informationen in 46 % der Vorfälle anschließend offengelegt wurden.

Angreifer schöpfen Daten in der Regel in der letzten Angriffsphase ab, bevor sie die Ransomware installieren. Die Ereignisanalyse von Sophos zeigt, dass die mittlere Zeitspanne von der Datenexfiltration bis zur Bereitstellung von Ransomware 2021 rund 44 Stunden betrug. Die durchschnittliche Zeitspanne (Mittelwert) betrug etwas mehr als vier Tage (4,28 Tage), die mittlere Zeitspanne (Median) lag bei unter zwei Tagen (1,84 Tage).

Unabhängig davon, welcher Wert bei der Zeitspanne angewendet wird: Die wichtige Botschaft lautet hier, dass sich Analysten nach der Exfiltration ein potenzielles Zeitfenster bietet, in dem sie noch verhindern können, dass der Angriff in die letzte und schädlichste Phase übergeht. Jede Erkennung von Tools, die bekanntermaßen zur Datenexfiltration genutzt werden, sollte daher mit hoher Priorität untersucht werden.

## Tool-Kombinationen

Die Untersuchung von Vorfällen ergab ein Muster von Tool-Kombinationen in Opfernetzwerken, die IT-Sicherheitsteams als Warnung dienen sollten (Vergleichsdaten für 2020 lagen in einigen Fällen vor):

- 2021 wurden PowerShell und schädliche Nicht-PS-Skripts in 64 % der Fälle gemeinsam beobachtet
- PowerShell und Cobalt Strike wurden in 56 % der Fälle kombiniert, verglichen mit 58 % in 2020
- PowerShell und PsExec wurden in 51 % der Fälle identifiziert, verglichen mit 49 % in 2020
- PowerShell, schädliche Skripts und Cobalt Strike wurden in 42 % der Fälle beobachtet
- PowerShell, schädliche Skripts und PsExec wurden in 38 % der Fälle beobachtet
- PowerShell, Cobalt Strike und PsExec waren in 33 % der Fälle vertreten, ein Anstieg von 12 % ggü. 2020
- Cobalt Strike und Mimikatz wurden in 16 % der Fälle gemeinsam beobachtet

Solche Korrelationen bleiben auch in diesem Jahr so wichtig wie im vergangenen Jahr, da ihre Erkennung als Frühwarnung vor einem bevorstehenden Angriff dienen oder das Vorhandensein eines aktiven Angriffs bestätigen kann.

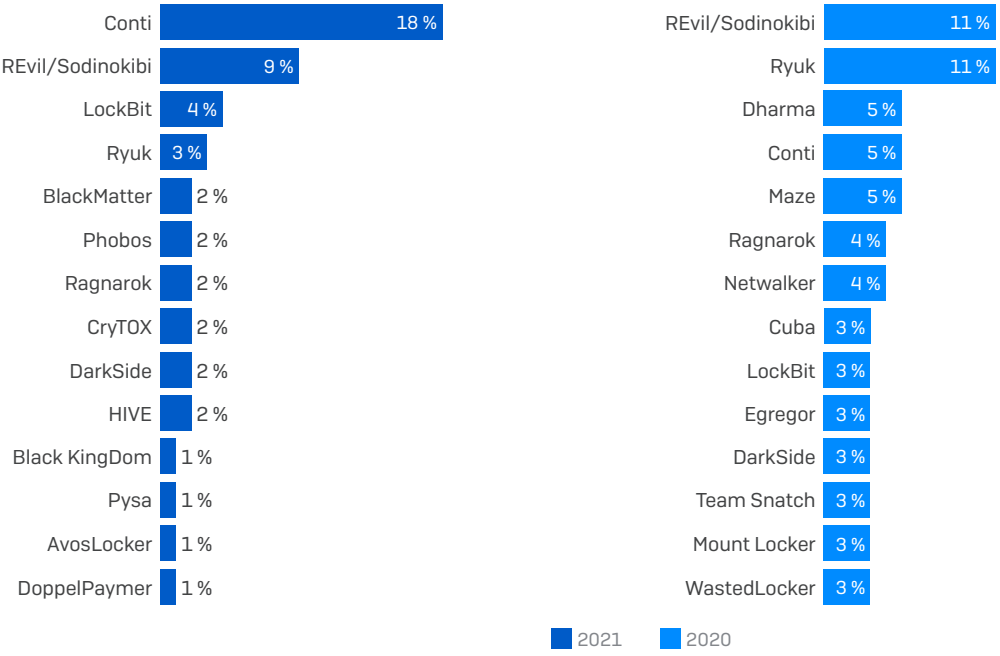
# Die aktivsten Ransomware-Angreifer im Jahr 2021

Für die 144 in der Analyse berücksichtigten Vorfälle konnten 41 verschiedene Ransomware-Angreifer identifiziert werden. Rund zwei Drittel (28) davon waren neue Gruppen, die erstmals im Jahr 2021 gemeldet wurden. Achtzehn Ransomware-Gruppen, die 2020 beobachtet wurden, waren 2021 von der Liste verschwunden – ein klarer Hinweis darauf, wie dynamisch und komplex die Cyberbedrohungs-Landschaft geworden ist und wie dies die Arbeit der Analysten erschweren kann.

In vielerlei Hinsicht war 2021 das Jahr für Conti, einen äußert produktiven RaaS-Anbieter, der bei fast einem von fünf (18 %) der von Sophos untersuchten Vorfälle seine Hände im Spiel hatte. Ebenfalls erwähnenswert ist jedoch, dass die Ransomware REvil für insgesamt einen von zehn Vorfällen verantwortlich war, trotz augenscheinlicher Einstellung der Aktivitäten im Juli 2021 (und erneut für kurze Zeit im September 2021 und 2022).

Andere weit verbreitete Ransomware-Familien waren im Jahr 2021 DarkSide, von der die RaaS stammte, die den berüchtigten Angriff auf Colonial Pipeline in den USA verursachte, und Black KingDom, eine der „neuen" Ransomware-Familien, die im März 2021 im Zuge der ProxyLogon-Schwachstelle auf der Bildfläche erschien.

### Am häufigsten beobachtete Ransomware




Rund ein Viertel (24 %) der Vorfälle im Jahr 2021 und 25 % der Vorfälle im Jahr 2020 wurden anderen Ransomware-Gruppen zugeschrieben. Alle übrigen Vorfälle konnten nicht eindeutig einer bekannten Gruppe zugeordnet werden.

Sophos hat bereits ausführlich über die Ransomware Conti berichtet. Eine umfassende Liste von Artikeln zu Conti und anderen weit verbreiteten Ransomware-Familien, darunter LockBit und Ryuk, finden Sie im Sophos Ransomware Threat Intelligence Center.

# Fazit

Jedes Unternehmen und jede Einrichtung ist ein mögliches Ziel für Angreifer, die irgendwo in den Weiten der Cyberwelt lauern – immer öfter sind es auch gleich mehrere Angreifer. Von Phishing und Finanzbetrug über Botnet Builder, Malware-Delivery-Plattformen, Cryptominer, IABs, Datendiebstahl, Unternehmensspionage, Ransomware und mehr – wenn es ein anfälliges Einfallstor in ein Netzwerk gibt, ist es sehr wahrscheinlich, dass Angreifer danach suchen, dieses schließlich finden und ausnutzen.

Bis aber der offene Eintrittspunkt geschlossen ist und alles vollständig beseitigt ist, was die Angreifer bereits vollbracht haben, um den Zugang zu schaffen und aufrechtzuerhalten, bleiben die Tore für alle folgenden Angreifer weit geöffnet. Und viele nehmen diese „Einladung" gerne an.

Sicherheitsteams können ihre Organisation schützen, indem sie verdächtige Aktivitäten überwachen und diese eingehend untersuchen. Der Unterschied zwischen unbedenklich und schädlich ist nicht immer leicht zu erkennen. Technologien können in jeder Umgebung – ganz gleich, ob virtuell oder physisch – viel leisten, reichen alleine jedoch nicht aus. Menschliche Erfahrung und Kenntnisse sowie die Fähigkeit, angemessen zu reagieren, sind wichtiger Bestandteil jeder Sicherheitslösung.

Die wichtigen Incident-Response-Lektionen des Jahres 2021 lassen sich wie folgt zusammenfassen: Angreifer nutzen anfällige, weit verbreitete Schwachstellen noch schneller und umfassender aus, was zu länger währenden Sicherheitsverletzungen führt, an denen oft mehrere Angreifer beteiligt sind. Dies wiederum bedeutet für Analysten, dass das Erkennen, Erforschen und Reagieren auf die Warnsignale bekannter Angriffswerkzeuge und -techniken wichtiger ist denn je.

# Sophos Rapid Response

Die Erkenntnisse dieses Reports basieren auf Daten zu Vorfällen, die von unserem Sophos Rapid-Response-Team untersucht wurden, das auf Incident Response und Beseitigung aktiver Bedrohungen spezialisiert ist. Sophos Rapid Response steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung.

Wenn bei Ihnen gerade ein Angriff stattfindet, kontaktieren Sie uns bitte auf Englisch über eine der beiden folgenden Optionen:

- per E-Mail an **RapidResponse@sophos.com**
- telefonisch über folgende Rufnummer:
  **+49 611 711 867 66** (D/AT/CH)

Die Rufnummern für alle anderen Regionen finden Sie unten.

Die KollegInnen sind 24x7 erreichbar. Falls gerade alle Experten im Gespräch sind, erreichen Sie nach 2 Min. die Voicebox. Bitte hinterlassen Sie Ihren Namen, Ihre Rufnummer und eine kurze Beschreibung des Vorfalls in englischer Sprache. Sie erhalten dann so schnell wie möglich einen Rückruf.

Rufnummern für andere Regionen:

**USA/weltweit:** +1 4087461064

**Frankreich:** +33 186539880

**UK:** +44 1235635329

**Australien:** +61 272084454

**Kanada:** +1 7785897255

# Zusätzliche Datentabellen

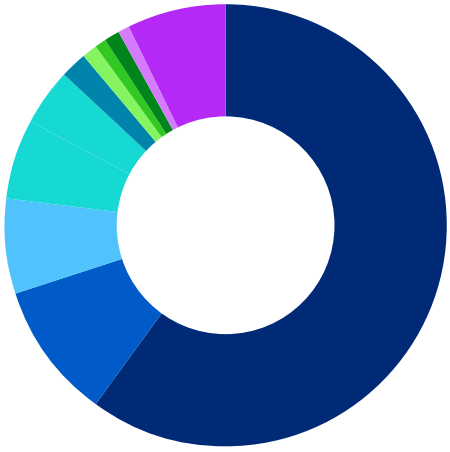
## Zuordnung von Vorfallsanalyse-Artefakten zur MITRE-Angriffskette

Die während der Vorfallsanalysen beobachteten Tools, Techniken und sonstigen Artefakte wurden dem MITRE ATT&CK Framework gegenübergestellt.

| Angriffsphasen nach MITRE | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
| **Artefakte** | | | | | | | | | | | |
| Remote Services | PowerShell | Cobalt Strike | Mimikatz | PowerShell | Mimikatz | Advanced IP Scanner | RDP | Netzwerk-Auskundschaftung | Cobalt Strike | Rclone | Datenverschlüsselung |
| Exploits | PsExec | AnyDesk | ProcDump | Rundll32.exe | ProcDump | Netscan | Cobalt Strike | Rclone | PowerShell | WinRAR | Netzwerk-Sicherheitsverletzung |

## Incident-Response-Daten 2021

### Incident-Response-Fälle nach Land

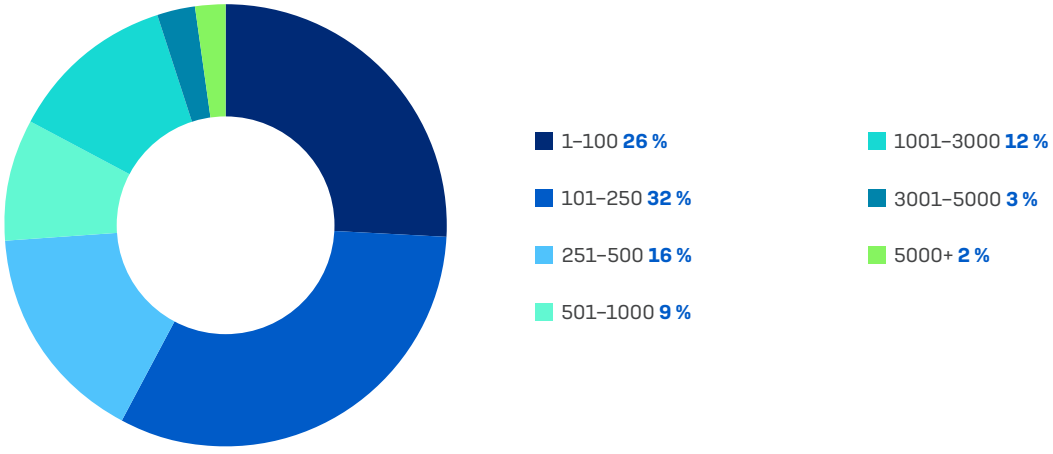


- USA **60 %**
- Deutschland **10 %**
- Großbritannien **7 %**
- Kanada **6 %**
- Italien **4 %**
- Spanien **2 %**
- Frankreich **1 %**
- Schweiz **1 %**
- Belgien **1 %**
- Philippinen **1 %**
- Sonstige **7 %** (Niederlande, Österreich, Vereinigte Arabische Emirate, Saudi-Arabien, Bahamas, Angola, Japan)

### Incident-Response-Fälle nach Branche

- Fertigung und Produktion **17 %**
- Einzelhandel **14 %**
- Gesundheitswesen **12 %**
- Informationstechnologie **9 %**
- Bauwesen **8 %**
- Bildungswesen **6 %**
- Lebensmittel **4 %**
- Logistik **4 %**
- Finanzwesen **4 %**
- Unterhaltung **3 %**
- Dienstleistungen **3 %**
- Medien **3 %**
- Sonstige **13 %** (Transportwesen, Arzneimittel, MSP/Hosting, gemeinnützige Organisationen, Behörden, Gastgewerbe, Rechtswesen, Landwirtschaft, Energie, Immobilien)

## Incident-Response-Fälle nach Größe des Unternehmens/der Einrichtung (Mitarbeiterzahl)



Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de



2022-05-25 DE (DD)

SOPHOS