Trellix | ABC Co.

ADVANCED THREAT RESEARCH-REPORT

JAN. 2022

Dieser Advanced Threat Research-Report wird Ihnen mit freundlicher Unterstützung unseres Partners zur Verfügung gestellt.

BERICHT

Trellix

ADVANCED THREAT RESEARCH-REPORT

JAN. 2022

BERICHT

INHALT

03 BRIEF UNSERES CHIEF SCIENTIST

04 LOG4J

04 Log4j: Der allwissende Speicher
04 Log4j-Zeitleiste
05 Log4j-Angriff
05 ATR-Schutzmaßnahmen von Trellix für Log4j

06 RANSOMWARE

07 Staatliche Maßnahmen gegen Ransomware-Bedrohungen
07 Erkennungen von Ransomware-Familien

08 ANGRIFFSMUSTER/TECHNIK (APT)

08 APT-Bedrohungsakteure
09 APT-Tools

10 ADVANCED THREAT RESEARCH

10 ATR-Toolbedrohungen

11 BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

11 Länder und Kontinente: 3. Quartal 2021
11 Angegriffene Branchen: 3. Quartal 2021
11 Angriffsvektoren: 3. Quartal 2021

12 LIVING OFF THE LAND: 3. QUARTAL 2021

12 Native Binärdateien der Betriebssysteme
13 Verwaltungs-Tools

13 BUG-REPORT

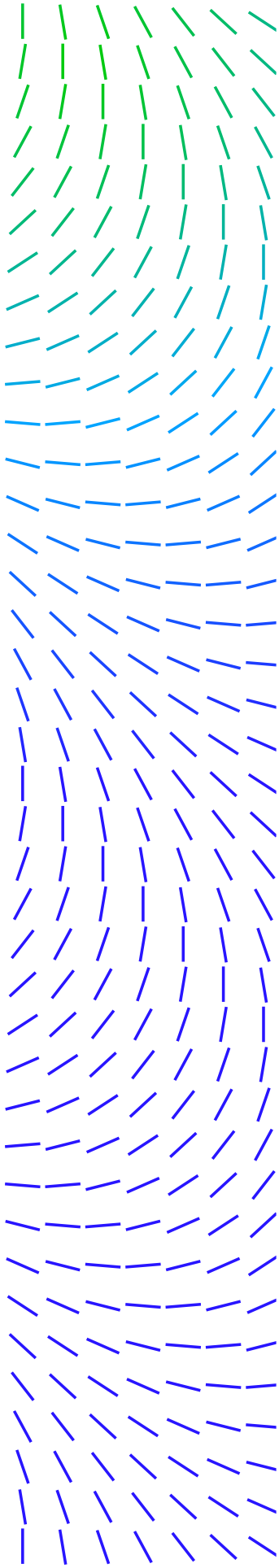
13 Ungeziefer auf der Windschutzscheibe
14 Eine kurze Reflexion
14 Termiten

15 FORSCHUNG ZU WEITEREN DATEN UND FORSCHUNG AUS DEM 3. QUARTAL 2021

15 Ransomware: Kundensektoren, Kundenländer und MITRE ATT&CK-Techniken
16 Angriffsmuster/Techniken (APT): Kundensektoren, Kundenländer und MITRE ATT&CK-Techniken
18 Advanced Threat Research (ATR): Kundensektoren, Kundenländer und MITRE ATT&CK-Techniken

20 RESSOURCEN

20 Twitter



Im ersten Threats-Report unseres neuen Unternehmens geht es um das Log4j-Problem, das nicht nur die Schlagzeilen beherrschte, sondern auch die Entwickler von Verteidigungsstrategien und die Sicherheitsteams in Unternehmen vorrangig beschäftigte.

BRIEF UNSERES CHIEF SCIENTIST

Willkommen zu unserem neuen Threats-Report und unserem neuen Unternehmen.

Zu Beginn dieses neuen Jahres müssen wir eine Bedrohungslandschaft konstatieren, die uns Ende 2021 noch einmal alles abverlangte. Im ersten Threats-Report unseres neuen Unternehmens geht es um das Log4j-Problem, das nicht nur die Schlagzeilen beherrschte, sondern auch die Entwickler von Verteidigungsstrategien und die Sicherheitsteams in Unternehmen vorrangig beschäftigte. Und wir blicken zurück auf das 3. und 4. Quartal 2021. Zuerst möchten wir jedoch unsere vielfältigen Ressourcen vorstellen, die Ihnen im Kampf gegen Log4j zur Verfügung stehen.

Je mehr Details zur Log4j-Bedrohung bekannt werden, desto wichtiger ist es, auf unsere Forschung und aktualisierten Hilferessourcen hinzuweisen. Neben dem Produktstatus überwachen wir ständig alle aktiven Kampagnen, die diese Schwachstelle nutzen, und informieren detailliert über den Umfang des Schutzes vor den neuen Schadensroutinen.

Als Details zur Log4j-Schwachstelle bekannt wurden, haben wir schnell mit netzwerkbasierten Signaturen und einem Bericht über die Schwachstelle reagiert. In der Folge haben wir zügig weitere Ressourcen bereitgestellt, die in diesem Report beschrieben werden.

Weitere Informationen zu aktuellen Log4j-Bedrohungsaktivitäten und anderen kursierenden Bedrohungen finden Sie in unserem wertvollen Threat-Dashboard.

In unseren Trellix Threat Labs-Blogs stellen wir Ihnen darüber hinaus unsere neuesten Bedrohungsinformationen, Videos und Links zum Sicherheitsbulletin zur Verfügung.

Natürlich ist Log4j nicht die einzige Bedrohung für die Sicherheit Ihres Unternehmens. Deshalb wirft dieser Report auch ein Schlaglicht auf das Gefahren- und Störpotenzial von Ransomware und anderen beobachteten Bedrohungen und Angriffen.

Viel Glück im neuen Jahr 2022 und herzlich willkommen bei unserem neuen Unternehmen.

– Raj Samani

Fellow und Chief Scientist

Twitter: @Raj_Samani

Autoren und Forscher

Alfred Alvarado
Christiaan Beek
John Fokker
Douglas McKee
Tim Polzer
Steve Povolny
Raj Samani
Leandro Velasco

LOG4J: DER ALLWISSENDE SPEICHER

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

Es ist leider schon fast Tradition und auch 2021 wurde mit Log4j pünktlich zu den Feiertagen eine neue Schwachstelle bekannt gegeben, die eine stark genutzte Log4j-Bibliothek betrifft. Sie wird in der Cyber-Sicherheit als schwerwiegendste Schwachstelle der letzten Jahrzehnte beschrieben und hat Trellix sowie die gesamte Cyber-Sicherheitsbranche im 4. Quartal 2021 auf den Plan gerufen. Die Log4j-Schwachstelle hat potenziell schwerste Auswirkungen auf alle Produkte, in deren Anwendungen und Websites die Log4j-Bibliothek integriert ist. Dazu gehören z. B. Produkte und Dienste des Apple iCloud-, Steam-, Samsung Cloud-Speichers u. v. m.

Unser Team hat Log4j seit ihrer Entdeckung aufmerksam verfolgt. Für Kunden, die die Network Security Platform (NSP) nutzen, haben wir die Netzwerksignatur KB95088 veröffentlicht. Die Signatur erkennt Versuche, CVE-2021-44228 über LDAP auszunutzen. Diese Signatur kann auf weitere Protokolle oder Dienste ausgedehnt werden und es können weitere Signaturen veröffentlicht werden, um den Schutzumfang zu verbessern.

Log4j-Zeitleiste

Hier eine kurze Zeitleiste zu Log4j und unserer Forschung:

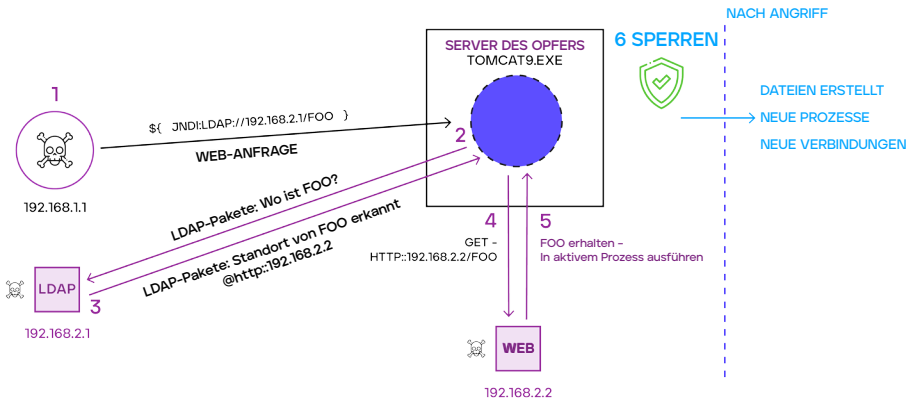
- **9. Dezember:** Die Log4j-Schwachstelle (CVE-2021-44228) wird auf Twitter und mit einem PoC auf Github für die Apache-Log4j-Protokollierungsbibliothek öffentlich gemacht. Apache wurde ursprünglich am 24. November über den Programmfehler informiert.
- **10. Dezember:** Steve Povolny und Douglas McKee posten einen Log4j-Blog mit einem Überblick über unsere ersten Erkenntnisse. Mit dem von uns reproduzierten und bestätigten PoC wollten wir zunächst bestimmen, wie einfach die Schwachstelle ausgenutzt werden kann. Dabei kamen der öffentliche Docker-Container, eine Client-Server-Architektur mit LDAP und RMI sowie marshalsec zum Einsatz, um die Log4j-Version 2.14.1 auszunutzen.
- **14. Dezember:** Die Anfälligkeit der Log4j-Version 1.2 für ähnliche Angriffe über die JMSAppender-Komponente wird bestätigt und CVE-2021-4104 veröffentlicht.
- **18. Dezember:** Die neue Denial of Service-(DOS-)Schwachstelle CVE-2021-45105 wird entdeckt. Sie betrifft die Log4j-Versionen 2.0-alpha1 bis 2.16.0.

Informationen über unsere neuesten Erkenntnisse zur Abwehr von Log4j-Angriffen erhalten Sie in unseren Trellix Threat Labs-Blogs und im Threats-Dashboard. Unser Team sammelt und analysiert Informationen aus mehreren offenen und geschlossenen Quellen, bevor es seine Berichte veröffentlicht.

Log4j-Angriff

Unser Team hat den Ablauf eines allgemeinen webbasierten Log4j-Angriffs schnell untersucht und beschrieben:

LOG4J-ANGRIFFSVERLAUF



- Schritt 1: Ein Angreifer sendet eine speziell programmierte Zeichenfolge an den Web-Server, der die anfällige Anwendung hostet. Diese Zeichenfolge kann nach unseren Erkenntnissen so verschleiert werden, dass sie netzwerkbasierte Signaturen umgeht.
- Schritt 2: Die Anwendung entschleiert diese Zeichenfolge, um sie in den Speicher zu laden. Ist dies geschehen, initiiert die Anwendung eine LDAP-Verbindung, um die Adresse für den Standort der schädlichen Klasse anzufordern.
- Schritt 3: Der vom Angreifer kontrollierte LDAP-Server sendet daraufhin die HTTP-URL-Adresse des entsprechenden Hosts als Standort der schädlichen Klassendatei.
- Schritt 4: Die anfällige Anwendung initiiert den Download der schädlichen Klassendatei.
- Schritt 5: Die anfällige Anwendung lädt die schädliche Klassendatei aus Schritt 4 und führt sie aus.

ATR-Schutzmaßnahmen von Trellix für Log4j

Für den Schutz einer Umgebung vor Angriffen wie Log4j können die Sicherheitsverantwortlichen zu einer mehrschichtigen Strategie aus Netzwerksicherheit in Kombination mit gezielten Endgerätespeicher-Scans greifen, um den Verlauf des Angriffs auf anfällige Systeme über Netzwerkvektoren effektiv zu erkennen und abzuwehren. Unsere ENS-Expertenregeln und individuellen Scan-Reaktionen sollen Sicherheitsverantwortliche in die Lage versetzen, mit präzisen Gegenmaßnahmen auf diese aufkommenden Bedrohungen zu reagieren.

Darüber hinaus steht auf CISA.gov ein Log4j-Scanner bereit, mit dem Unternehmen potenziell anfällige Web-Dienste identifizieren können, die von den Log4j-Schwachstellen betroffen sind.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

RANSOMWARE

Im 3. Quartal 2021 sind einige prominente Ransomware-Gruppen, untergetaucht, wieder aufgetaucht, haben sich neu erfunden oder sogar eine Umfirmierung versucht. Ungeachtet dessen stellen sie nach wie vor eine relevante, verbreitete, beliebte und potenziell verheerende Bedrohung für immer mehr Sektoren dar.

Auch wenn Ransomware-Aktivitäten im 2. Quartal 2021 verurteilt und aus zahlreichen Cybercrime-Foren verbannt wurden, hat unser Team in verschiedenen Foren Aktivitäten derselben Bedrohungsakteure unter anderer Identität beobachtet.

Trellix hilft bei Ransomware-Festnahmen und Beschlagnahmung von Lösegeldern

Im Dezember 2021, lieferte Trellix dem FBI und Europol Erkenntnisse zur Festnahme von REvil-Partnern und die Beschlagnahmung von 2 Millionen US-Dollar aus Lösegeldern.

Zu den erwähnenswerten Ransomware-Trends und -Kampagnen im 3. Quartal 2021 gehörten:

- BlackMatter wurde Ende Juli 2021 entdeckt. Diese Ransomware-Bedrohung begann mit einer starken Welle von Angriffen, die New Cooperative, ein Unternehmen aus der landwirtschaftlichen Lieferkette in den USA, mit der Offenlegung vertraulicher Geschäftsdaten drohten. New Cooperative berichtete, dass Funktionen in der Lieferkettenverwaltung sowie Zeitpläne in der Tierfütterung gesperrt wurden, und schätzte, dass 40 Prozent der Getreideproduktion in den USA beeinträchtigt sein könnten. BlackMatter behauptete zwar, die besten Teile anderer Malware-Varianten wie GandCrab, LockBit und DarkSide zu nutzen, allerdings zweifeln wir stark an, dass die Kampagne von einer neuen Entwicklergruppe durchgeführt wird. Dafür überschneidet sich die BlackMatter-Malware einfach zu stark mit der DarkSide-Malware, die mit dem Colonial Pipeline-Angriff verbunden war.
- Wir haben unsere Auffassung mitgeteilt, dass die Groove Gang als früherer Partner oder als Untergruppe mit der Babuk-Gruppe verbunden ist.
- REvil/Sodinokibi hat sich zur erfolgreichen Infizierung von mehr als 1 Million Benutzern durch einen Ransomware-Angriff auf Kaseya VSA, einen Anbieter von Software für verwaltete Services, bekannt. Die vermeldete Lösegeldforderung von REvil in Höhe von 70 Millionen US-Dollar war der höchste bisher öffentlich bekannt gewordene Lösegeldbetrag. Zu den Ergebnissen des Angriffs gehörte die erzwungene mehrtägige Schließung von hunderten Supermarkt-Filialen.
- LockBit 2.0 tauchte im Juli 2021 auf und nannte am Ende mehr als 200 Opfer auf seiner Data-Leak-Site.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

Staatliche Maßnahmen gegen Ransomware-Bedrohungen

Im 3. Quartal hat die US-Regierung mit der Website StopRansomware.gov eine proaktive Kampagne zur Begrenzung von Ransomware-Angriffen gestartet. In diesem Rahmen setzt sie Belohnungen in Höhe von bis zu 10 Millionen US-Dollar für Informationen aus, die zur Identifizierung oder Aufspürung staatlich unterstützter Bedrohungsakteure führen, die an Cyber-Aktivitäten gegen kritische US-Infrastruktur beteiligt waren.

Weitere Informationen dazu, wie diese Ransomware und neue Kampagnen die Unternehmen in den kommenden Monaten bedrohen könnten, finden Sie in unseren Trellix-Bedrohungsprognosen für 2022.

Ransomware-Forschung von Trellix

Um Unternehmen bei der Analyse und Abwehr von Ransomware-Angriffen in der Bedrohungslandschaft zu unterstützen, präsentiert unser Team seine Forschung und Ergebnisse in Bezug auf die Verbreitung vieler verschiedener Ransomware-Bedrohungen, einschließlich Familien, Techniken, Ländern, Sektoren und Vektoren.

Erkennungen von Ransomware-Familien

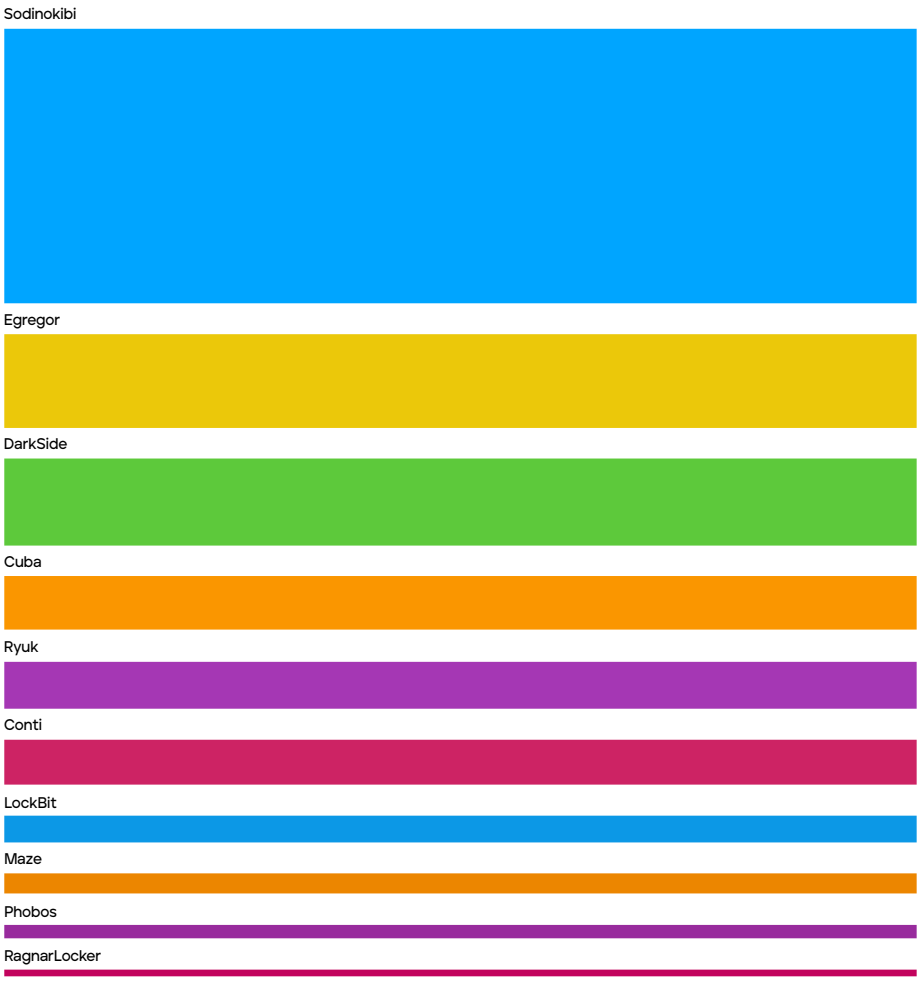


Abbildung 1. Sodinokibi (41 %) war im 3. Quartal 2021 die am weitesten verbreitete erkannte Ransomware-Familie, gefolgt von DarkSide (14 %) und Egregor (13 %).

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

Ausführliche Informationen finden Sie im Abschnitt zu Ransomware-Kundenländern, Kundensektoren und MITRE ATT&CK-Techniken weiter unten.

ANGRIFFSMUSTER/TECHNIK (APT)

Das Team verfolgt und überwacht APT-Kampagnen und die damit verbundenen Indikatoren und Techniken. Die Forschungsergebnisse unseres Teams geben Aufschluss über die APT-Bedrohungsakteure, Tools, Kundenländer, Kundensektoren und MITRE ATT&CK-Techniken im 3. Quartal 2021.

APT-Bedrohungsakteure



Abbildung 2. APT41 (24 %) und APT29 (22 %) waren die am weitesten verbreiteten APT-Bedrohungsakteure im 3. Quartal 2021 und für fast die Hälfte der überwachten APT-Aktivitäten verantwortlich.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

APT-Tools

Das Team hat Kompromittierungsindikatoren für die verfolgten APT-Kampagnen und die folgenden damit verbundenen Tools identifiziert. Bekanntermaßen nutzen APT-Gruppen gängige Systemdienstprogramme, um Sicherheitskontrollen zu umgehen und ihre Operationen durchzuführen:



Abbildung 3. Cobalt Strike (34 %) war das am weitesten verbreitete APT-Tool im 3. Quartal 2021 gefolgt von Mimikatz (27 %), Net.exe (26 %) und PsExec (20 %). Das von staatlichen Akteuren missbrauchte Cobalt Strike-Angriffspaket wurde in über einem Drittel der APT-Aktivitäten erkannt.

Ausführliche Informationen finden Sie im Abschnitt zu APT-Kundenländern, Kundensektoren und MITRE ATT&CK-Techniken weiter unten.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

ADVANCED THREAT RESEARCH

Unser Team hat Bedrohungskategorien im 3. Quartal 2021 verfolgt. Die Forschung gibt Aufschluss über die prozentuale Verteilung beim Typ der verwendeten ATR-Malware sowie bei den Kundenländern, Kundensektoren, in Angriffen verwendeten MITRE ATT&CK-Techniken und Branchensektoren.

ATR-Toolbedrohungen

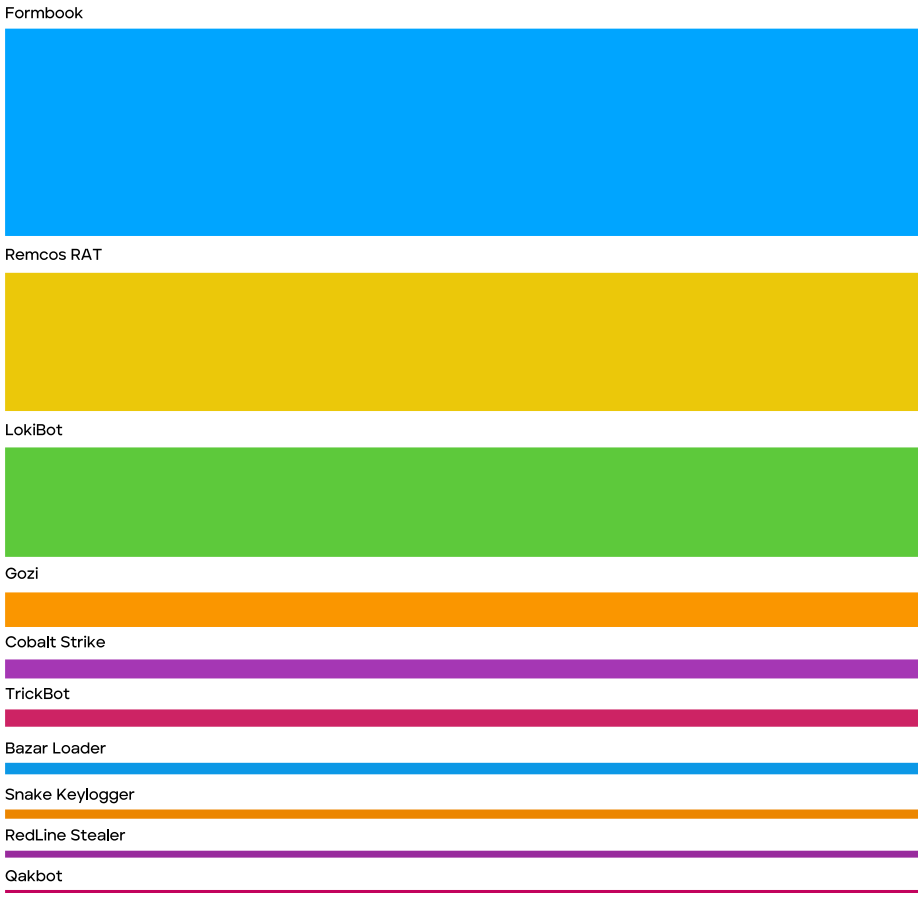


Abbildung 4. Formbook (36 %), Remcos RAT (24 %) und LokiBot (19 %) waren für fast 80 % der Erkennungen bei den ATR-Toolbedrohungen im 3. Quartal 2021 verantwortlich.

Ausführliche Informationen finden Sie im Abschnitt zu ATR-Kundenländern, Kundensektoren und MITRE ATT&CK-Techniken weiter unten.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

Länder und Kontinente: 3. Quartal 2021

Bei Ländern und Kontinenten wurden im 3. Quartal 2021 folgende erhebliche Zunahmen öffentlich gemeldeter Zwischenfälle verzeichnet:

- Nordamerika verzeichnete die meisten Zwischenfälle unter den Kontinenten, sah aber eine Abnahme um 12 % vom 2. Quartal zum 3. Quartal 2021.
- Die USA registrierten die meisten gemeldeten Zwischenfälle im 3. Quartal 2021. Im Vergleich zum 2. Quartal verringerte sich ihre Zahl jedoch um 9 %.
- Frankreich verzeichnete den stärksten Anstieg (400 %) bei den im 3. Quartal 2021 gemeldeten Zwischenfällen.
- Russland registrierte im 3. Quartal 2021 den größten Rückgang (-79 %) bei den Zwischenfällen im Vergleich zum 2. Quartal 2021.

Angegriffene Branchen: 3. Quartal 2021

Bei den Branchen wurden im 3. Quartal 2021 folgende erhebliche Zunahmen öffentlich gemeldeter Zwischenfälle verzeichnet:

- Mehrere Branchen (28 %) wurden besonders häufig angegriffen, gefolgt vom Gesundheitswesen (17 %) und dem öffentlichen Sektor (15 %).
- Zu den Sektoren, die deutliche Zunahmen vom 2. Quartal zum 3. Quartal 2021 verzeichneten, gehören der Finanz-/Versicherungssektor (21 %) und das Gesundheitswesen (7 %).

Angriffsvektoren: 3. Quartal 2021

Bei den Vektoren wurden im 3. Quartal 2021 folgende erwähnenswerte Zwischenfälle öffentlich gemeldet:

- Malware war im 3. Quartal 2021 die am häufigsten gemeldete Angriffstechnik. Die gemeldeten Malware-Zwischenfälle nahmen jedoch im Vergleich zum 2. Quartal 2021 um 24 % ab.
- Zu den Sektoren mit Steigerungen vom 2. Quartal zum 3. Quartal 2021 gehören verteilte Denial of Service-Angriffe (112 %) und gezielte Angriffe (55 %).

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

LIVING OFF THE LAND

Cyber-Kriminelle greifen zu Living off the Land-Techniken (LotL), die seriöse Software und Funktionen in einem System nutzen, um schädliche Aktionen an diesem System durchzuführen. In Bezug auf die Ereignisse im 3. Quartal hat Trellix einen Trend bei den Tools ausgemacht, die von Angreifern verwendet werden, die unentdeckt bleiben wollen. Obwohl staatlich unterstützte Bedrohungsgruppen und größere kriminelle Bedrohungsgruppen durchaus über die erforderlichen Ressourcen verfügen, um Tools intern zu entwickeln, nutzen sie oft lieber bereits vorhandene Binärdateien und administrativ installierte Software in einem Zielsystem, um bestimmte Angriffsphasen zu implementieren.

Um native Binärdateien oder administrativ verwendete Software für die Aufklärung eines prominenten Ziels zu identifizieren, können Angreifer Informationen zu den verwendeten Technologien aus Stellenanzeigen, Kundenreferenzen, mit denen die Hersteller werben, oder von Insider-Komplizen sammeln.

Native Binärdateien der Betriebssysteme		Anmerkungen
PowerShell (41,53 %)	T1059.001	PowerShell wird oft genutzt, um Skripte und PowerShell-Befehle auszuführen.
Windows-Befehlszeile (CMD) (40,40 %)	T1059.003	Die Windows-Befehlszeile ist das primäre CLI-Dienstprogramm für Windows. Es wird oft genutzt, um Dateien und Befehle in einem alternativen Datenstrom auszuführen.
Rundll32 (16,96 %)	T1218.011, T1564.004	Rundll32 kann genutzt werden, um lokale DLL-Dateien, DLL-Dateien aus einer Freigabe, DLL-Dateien aus dem Internet und alternativen Datenströmen auszuführen.
WMIC (12,87 %)	T1218, 1564.004	WMIC ist eine Befehlszeilenschnittstelle für WMI und kann von Angreifern genutzt werden, um Befehle oder Schaddaten lokal, in alternativen Datenströmen oder auf einem Remote-System auszuführen.
Excel (12,30 %)	T1105	Auf vielen Systeme findet sich nicht nativ installierte Tabellenkalkulationssoftware. Wenn Angreifer Anhänge mit schädlichen Codes oder Skripten senden, die von Benutzern ausgeführt werden, können Schaddaten von einem Remote-Standort geladen werden.
Schtasks (11,70 %)	T1053.005	Ein Angreifer kann Tasks planen, die die Persistenz erhalten, weitere Malware ausführen oder automatisierte Tasks durchführen.
Regsvr32 (10,53 %)	T1218.010	Mit Regsvr32 können Angreifer DLL-Dateien registrieren, schädlichen Code ausführen und Anwendungs-Whitelists umgehen.
MSHTA (8,78 %)	T1218.005	Mit MSHTA können Angreifer JavaScript-, JScript- und VBScript-Dateien ausführen, die in HTA-Dateien lokal und in alternativen Datenströmen versteckt oder von einem Remote-Standort geladen werden können.
Certutil (4,68 %)	T1105, 1564.004, T1027	Dieses Windows-Befehlsdienstprogramm wird verwendet, um Zertifizierungsstelleninformationen zu erhalten und Zertifizierungsdienste zu konfigurieren. Alternativ können Angreifer mit certutil Remote-Tools und Remote-Inhalte erfassen, Dateien kodieren und dekodieren sowie auf alternative Datenströme zugreifen.
Net.exe (4,68 %)	T1087 und Subtechniken	Dieses Windows-Befehlszeilendienstprogramm ermöglicht einem Angreifer Aufklärungsaktionen wie das Identifizieren von Benutzer-, Netzwerk- und Dienstfunktionen auf dem Rechner eines Opfers.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

Reg.exe *(4,10 %)*	1003,002, 1564,004		Mit Reg.exe können Angreifer Registrierungswerte hinzufügen, ändern, löschen und exportieren, die in alternativen Datenströmen gespeichert werden können. Darüber hinaus kann reg.exe verwendet werden, um Anmeldedaten aus einer SAM-Datei herunterzuladen.

Verwaltungs-Tools			Anmerkungen
Remote-Dienste *(15,21 %)*	T1021.001, T1021.004, T1021.005	AnyDesk ConnectWise Control RDP UltraVNC PuTTY WinSCP	Remote-Dienst-Tools in Windows und in Drittanbieter-Software können von Angreifern genutzt werden, um sich zusammen mit gültigen Konten Remote-Zugriff auf einen Rechner oder eine Infrastruktur zu verschaffen, Eintrittstools zu übertragen und Malware auszuführen sowie Daten zu exfiltrieren.
Archivdienst-programme *(4,68 %)*	T1560.001	7-Zip WinRAR WinZip	Angreifer können mit Archivdienst-programmen gesammelte Daten komprimieren, um ihre Exfiltrierung vorzubereiten, sowie normale und ausführbare Dateien dekomprimieren.
PsExec *(4,68 %)*	T1569.002		PsExec ist ein Tool, mit dem Befehle und Programme auf einem Remote-System ausgeführt werden.
BITSAdmin *(2,93 %)*	T1105, T1218, T1564.004		BiTSAdmin wird oft genutzt, um die Persistenz aufrechtzuerhalten, Artefakte zu bereinigen und weitere Aktionen aufzurufen, sobald ein festgelegtes Kriterium erfüllt ist.
fodhelper.exe *(1,17 %)*	T1548.002		Fodhelper.exe ist ein Windows-Dienst-programm, mit dem Angreifer schädliche Dateien mit erhöhten Privilegien auf dem Rechner eines Opfers ausführen können.
ADFind *(0,59 %)*	T1016, T1018, T1069 und Subtechniken, T1087 und Subtechniken, T1482		Mit diesem Befehlszeilen-Dienstprogramm können Angreifer Active Directory-Informationen wie vertrauenswürdige Domänen, Berechtigungsgruppen, Remote-Systeme und Netzwerk-konfigurationen ausspionieren.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

BUG-REPORT

Ungeziefer auf der Windschutzscheibe

(Douglas McKee, Principal Engineer und Senior Security Researcher, und andere Blogger verfolgen und analysieren Schwachstellen im monatlichen Bug-Report.)

Während die Welt Ende 2021 gefühlt mit Tempo 200 durch die Zeit raste, landete viel „Ungeziefer" auf unserer sprichwörtlichen Windschutzscheibe. Ein Teil davon ließ sich zwar problemlos abwaschen, manche hinterließen jedoch bleibende Flecken. Das Team verfolgt und bewertet dieses Ungeziefer, die neuen Schwachstellen, nach ihrer Veröffentlichung im Monatsrhythmus und berichtet, welche nach unserem „Gefühl" die wichtigsten werden könnten. Richtig – wir liefern keinen CVSS-Score und kein OWASP-Ranking, sondern analysieren auf der Basis jahrelanger Erfahrungen. Wir nutzen also unser gutes, altes Bauchgefühl.

Eine kurze Reflexion

Beim Blick auf unsere meistgemeldeten Bugs der letzten Monate heben sich einige vom Rest ab. Apache hatte ein hartes Jahr, in dem sein Webserver (CVE-2021-41773) und die Log4j-Komponente (CVE-2021-44228) von wirkungsvollen Bugs betroffen waren. Auch Palo Alto verdient eine besondere Erwähnung wegen eines Bugs, der in ihrem GlobalProtect VPN (CVE-2021-3064) gefunden wurde und eine einzigartige Wirkung während der weltweiten Pandemie entfaltete. An dieser Stelle wollen wir jedoch kurz innehalten und für einen Moment ehrlich sein. Das Prädikat „Wirkungsvoll" wird der Log4j-Schwachstelle von Apache nicht gerecht, denn sie war 2021 mit großem Abstand der größte Bug und hat darüber hinaus das Potenzial, diesen Titel auch in den nächsten Jahren zu verteidigen. Wenn Sie fernab jeder Zivilisation leben und noch nicht davon gehört haben, empfehle ich Ihnen dringend die Lektüre unseres Bug-Reports vom Dezember. Vergessen Sie nicht, sich jeden Monat über die neuesten und wichtigsten Schwachstellen zu informieren.

Warum sind diese Bugs so gefährlich? Einfach gesagt, können sie remote und ohne Authentifizierung für Tools am Perimeter Ihres Netzwerks ausgenutzt werden. Diese Bugs können der erste Eintrittspunkt in ein Netzwerk sein, ohne dass Angreifer „nach ihren Zielen phishen" müssen, und zusätzlich das Tor für einen größeren Angriff öffnen.

Wenn Ihr CISO gern russisches Roulette spielt und sagt, dass er nur ein Produkt patchen kann, empfehlen wir Ihnen, sich unbedingt für die Log4j-Schwachstelle zu entscheiden, weil dies einfach ist und sie von vielen böswilligen Akteuren aktiv ausgenutzt wurde. Obwohl die Palo Alto VPN-Schwachstelle schwerwiegend ist und VPNs seit 2020 immer öfter ausgenutzt werden, rangiert sie noch hinter Log4j und den anderen Apache-Schwachstellen, weil sie eine ältere Version der VPN-Software betrifft und bei Angriffen bisher nicht aktiv ausgenutzt wurde.

Termiten

Bestimmtes Ungeziefer, z. B. Termiten, kann durch das Raster fallen, aber trotzdem eine verheerende Wirkung entfalten.

Ein Microsoft Windows Installer Service-Bug namens CVE-2021-41379, mit dem lokale Rechte erweitert werden konnten, war im November so ein sprichwörtlicher Termit. Microsoft hat mitgeteilt, dass der Bug lokalen Zugriff erfordert, und ihn angeblich mit einem offiziellen Patch korrigiert. Diese Strategie ging jedoch nach hinten los, als der Patch nicht wie erwartet funktionierte.

Nachdem der Patch fehlgeschlagen und ein öffentlich verfügbarer PoC verfügbar war, nutzten böswillige Akteure dies sofort für ihre Zwecke, wie in Insights beschrieben. Zusätzliche Brisanz erfährt das Problem, weil unser Team Versionen dieses Exploits für Angriffe gesehen hat, die im Dark Web verkauft werden.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

Ransomware: Kundenländer

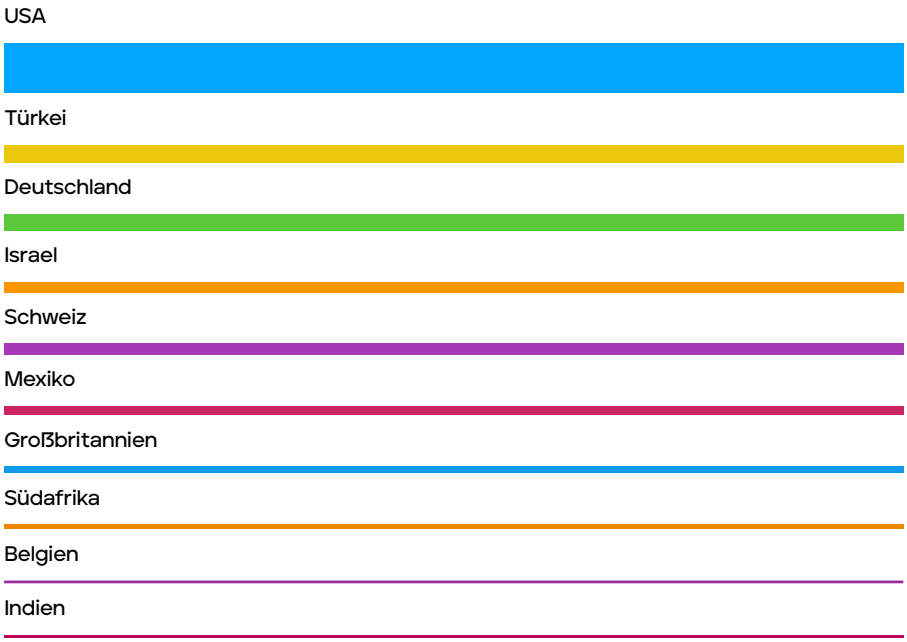


Abbildung 5. Im 3. Quartal 2021 machten Kunden in den Vereinigten Staaten mehr als ein Drittel aller Ransomware-Erkennungen aus.

Ransomware: Kundensektoren



Abbildung 6. Der Bank-/Finanzsektor (22 %), die Versorgungsunternehmen (20 %) und der Einzelhandel (16 %) machten im 3. Quartal 2021 fast 60 % aller bei Kunden erkannten Ransomware-Fälle aus.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

Ransomware: MITRE ATT&CK-Techniken



Abbildung 7. Die Dateneingabe (2,6 %), die Datei- und Verzeichniserkennung (2,5 %) und verschleierte Dateien oder Informationen (2,4 %) führten die Liste der von Ransomware genutzten MITRE ATT&CK-Techniken an, die im 3. Quartal 2021 erkannt wurden.

APT: Kundenländer



Abbildung 8. Kundenerkennungen von Angriffsmustern/Techniken in der Türkei machten 17 % aller Erkennungen im 3. Quartal 2021 aus, gefolgt von den Vereinigten Staaten (15 %) und Israel (12 %).

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

APT: Kundensektoren



Abbildung 9. Die meisten APT-Erkennungen im 3. Quartal 2021 gab es im Bank-/Finanzsektor (37 %), gefolgt von Versorgungsunternehmen (17 %), Einzelhandel (16 %) und Behörden (11 %).

APT: MITRE ATT&CK-Techniken



Abbildung 10. Der Spearphishing-Anhang (16,8 %), verschleierte Dateien oder Informationen (16,7 %) und PowerShell (16 %) waren die am weitesten verbreiteten im 3. Quartal 2021 erkannten APT MITRE ATT&CK-Techniken.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

ATR: Kundenländer

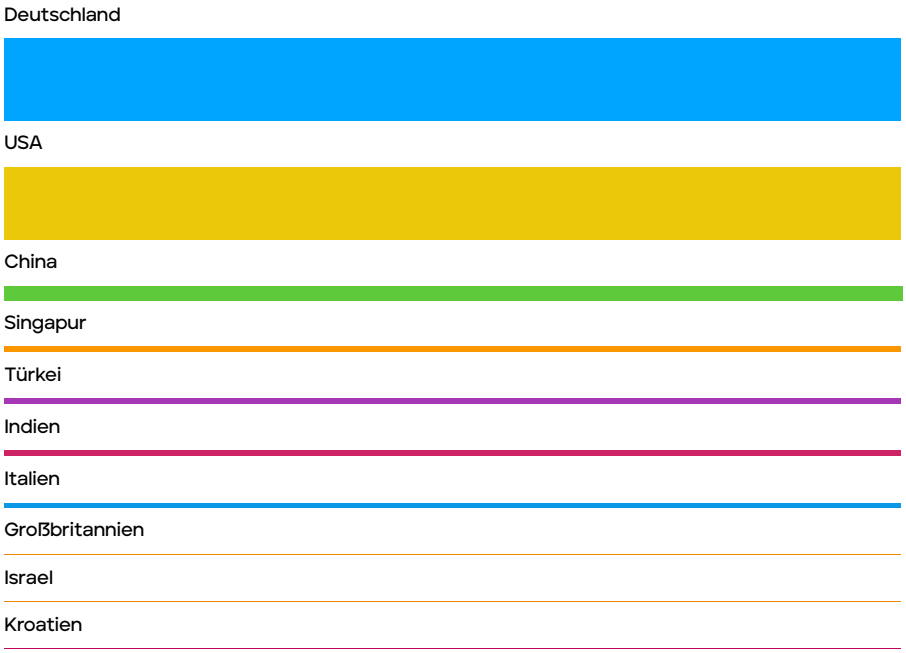


Abbildung 11. Mehr als die Hälfte aller im 3. Quartal 2021 erkannten ATR-Toolbedrohungen entfielen auf Deutschland (32 %) und die Vereinigten Staaten (28 %).

ATR: Kundensektoren



Abbildung 12. Die weitaus meisten Erkennungen (45 %) entfielen im 3. Quartal 2021 auf den Bank-/Finanzsektor.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

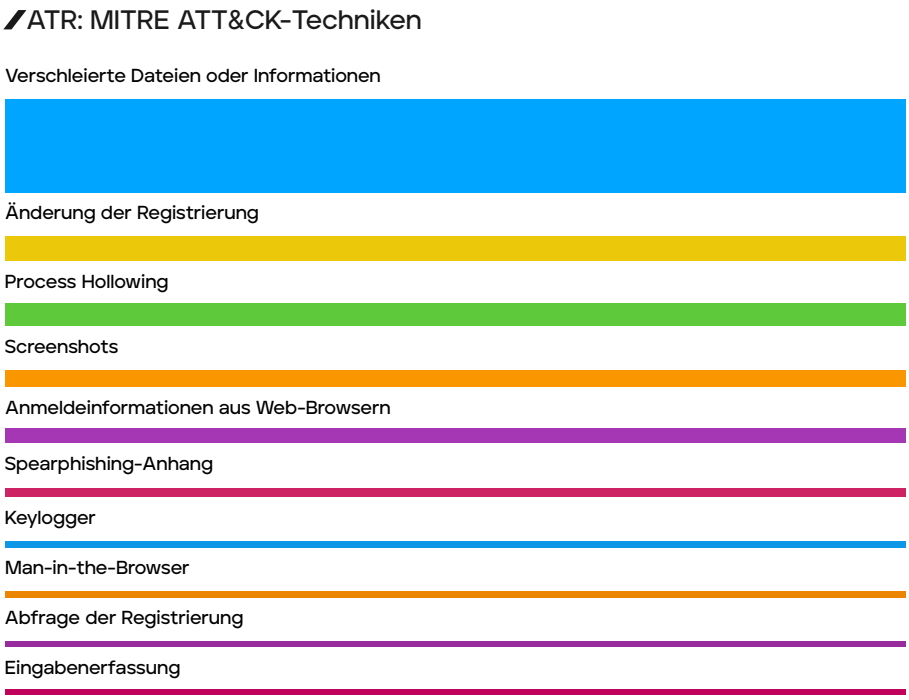


Abbildung 13. 5 % aller Erkennungen im 3. Quartal 2021 entfielen auf verschleierte Dateien oder Informationen.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

RESSOURCEN

Mit unseren Team-Ressourcen können Sie die neuesten Bedrohungen und Forschungen verfolgen:

Bedrohungszentrum: Die aktuell schwerwiegendsten Bedrohungen wurden von unserem Team erkannt.

Twitter:

Trellix Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Douglas McKee

Über Trellix

Trellix ist ein globales Unternehmen, das die Zukunft der Cyber-Sicherheit neu definiert. Seine offene und native eXtended Detection and Response-Plattform (XDR) hilft Unternehmen, die mit den raffiniertesten Bedrohungen von heute konfrontiert werden, das Vertrauen in den Schutz und die Resilienz ihrer Abläufe zu stärken. Zusammen mit einem umfassenden Partnerökosystem fördern die Sicherheitsexperten von Trellix die technologische Innovationsfähigkeit durch Machine Learning und Automatisierung, um über 40.000 Geschäfts- und Behördenkunden zu stärken. Mehr auf www.trellix.com.

Trellix Threat Labs

Abonnieren Sie unsere Informationen zu Bedrohungen.

BRIEF UNSERES CHIEF SCIENTIST

LOG4J: DER ALLWISSENDE SPEICHER

RANSOMWARE

ANGRIFFSMUSTER/ TECHNIK (APT)

ADVANCED THREAT RESEARCH

BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

LIVING OFF THE LAND

BUG-REPORT

FORSCHUNG ZU WEITEREN KUNDENSEKTOREN, KUNDENLÄNDERN UND MITRE ATT&CK-TECHNIKEN

RESSOURCEN

Trellix

6220 American Center Drive,
San Jose, CA 95002

Copyright © 2022 Musarubra US LLC
JANUAR 2022