Präsentiert von

Trellix ADVANCED RESEARCH CENTER

DER THREATS-REPORT

Februar 2023

INHALT

3 ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

5 BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

6 METHODEN

7 RANSOMWARE: 4. QUARTAL 2022

17 STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

22 LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

27 SCHWACHSTELLENINFORMATIONEN: 4. QUARTAL 2022

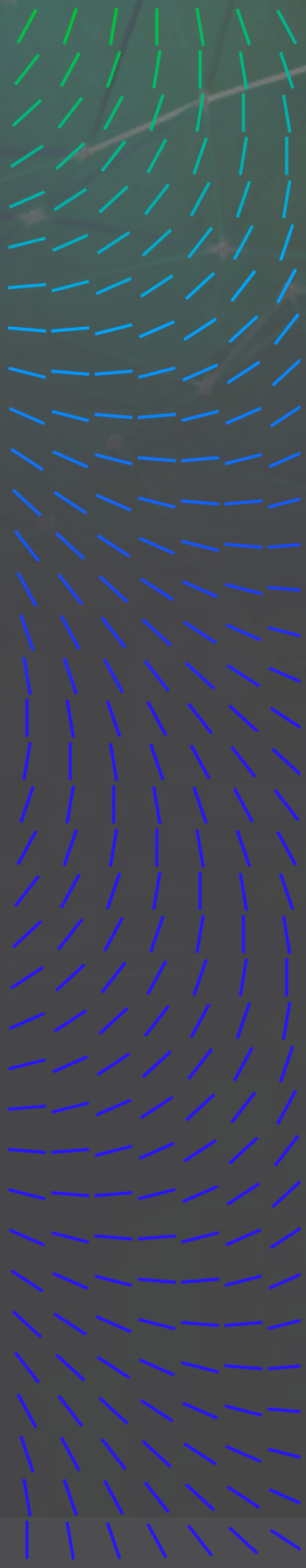
29 TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

33 NETZWERKSICHERHEIT: 4. QUARTAL 2022

35 VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

40 AUTOREN UND FORSCHER

40 RESSOURCEN



ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

Auch in den letzten Monaten des Jahres 2022 blieben Bedrohungsakteure eine ernstzunehmende Gefahr. Das Trellix Advanced Research Center reagierte darauf mit zusätzlichen Bedrohungsanalyse-Ressourcen für unser Team, das aus hunderten erfahrenen Sicherheitsanalysten und Forschern besteht.

„Mit anderen Worten: Wir verfügen über deutlich umfangreichere Bedrohungsdaten. Dies führt zu optimierten Sicherheitsabläufen und besseren Sicherheitsergebnissen durch weniger Stress. Bedrohungen entwickeln sich ständig weiter. Und wir halten Schritt."

In diesem Bericht erhalten Sie erstklassige Informationen darüber, welche Bedrohungsakteure, Malware-Familien, Kampagnen und Techniken im letzten Quartal am häufigsten aufgetreten sind. Doch das ist nicht alles. Wir haben auch weitere Quellen erschlossen, die Informationen aus Ransomware-Leak-Websites und Berichten der Sicherheitsbranche erfassen. Mit der Zunahme an Trellix-Ressourcen steigt auch die Zahl der Bedrohungsforschungskategorien, die beispielsweise Neues über Netzwerksicherheit, Cloud- und Endgeräte-Zwischenfälle sowie Sicherheitsabläufe abdecken.

Seit unserem letzten Bericht hat sich das Trellix Advanced Research Center mit Untersuchungen und Erkenntnissen aus aller Welt beschäftigt, zum Beispiel mit der Verbindung von Gamaredon, dem starken Anstieg an Cyber-Angriffen auf die Ukraine im 4. Quartal, dem Patchen von 61.000 anfälligen Open-Source-Projekten sowie mit der Veröffentlichung der Erkenntnisse zu den diesjährigen neuartigen Angriffen in den Bedrohungsprognosen 2023.

Die folgenden Erkenntnisse wurden durch die verbesserte Datenlage ermöglicht und veranschaulichen, wie das Trellix Advanced Research Center unseren Kunden und der Sicherheitsbranche hilft, besser auf Sicherheitsbedrohungen zu reagieren:

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

Ransomware

- Forschung über die Bedeutung von LockBit 3.0 als einflussreichste Ransomware-Gruppe im 4. Quartal
- Anhaltende weltweite Verbreitung von Ransomware, insbesondere in den USA
- Ransomware-Angriffe auf Branchen wie Industriegüter und -dienstleistungen

Staatliche Akteure

- Staatliche Akteure, die Branchen wie Behörden sowie das Verkehrs- und Transportwesen ins Visier nehmen
- US-Unternehmen, die von staatlichen Akteuren angegriffen wurden

Living off the Land (LOLBIN)

- Umfangreiche Erkenntnisse zum Einsatz von Cobalt Strike, die durch Bedrohungssuchmethoden des Trellix Advanced Research Center gewonnen wurden
- Die hohe Anzahl an Cobalt Strike Team-Servern bei chinesischen Cloud-Anbietern
- Bei den zehn am häufigsten missbrauchten Betriebssystem-Binärdateien wird Windows Command Shell bei nahezu der Hälfte der gemeldeten Vorfälle eingesetzt

Bedrohungsakteure

- China, Nordkorea und Russland führen die Liste der aktivsten Länder mit Bedrohungsakteuren an

Trends in der E-Mail-Sicherheit

- Das deutlich erhöhte Aufkommen an schädlichen E-Mails in arabischen Ländern, das während der Fußballweltmeisterschaft beobachtet wurde
- Erkenntnisse zu Phishing- und Vishing-Kampagnen, z. B. Nachahmungstechniken und bei Vishing häufig nachgeahmte Unternehmen

Netzwerksicherheit

- Die schwerwiegendsten, wichtigsten und relevantesten Angriffe, WebShells, Tools und Techniken des Quartals

Von Trellix XDR erfasste Telemetriedaten über Sicherheitsabläufe

- Häufige Sicherheitswarnungen, Exploits, Protokollquellen und MITRE ATT&CK-Techniken
- Cloud-Zwischenfälle
- Techniken und Erkennungen für Azure, AWS und GCP
- Häufige Techniken und Erkennungen

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

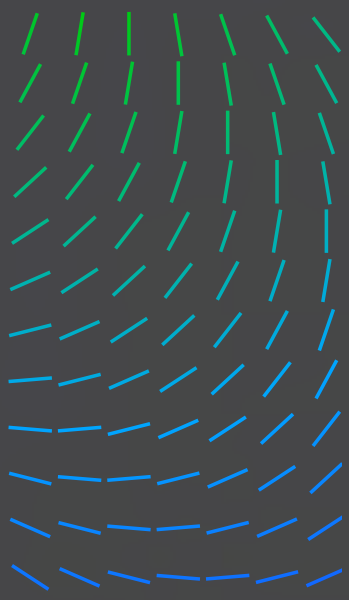
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

Unser Advanced Research Center-Team freut sich, den Bedrohungsbericht zu den Daten des 4. Quartals 2022 vorlegen zu können. Sie werden feststellen, dass dieser Bericht neue Produkt-Sensordaten berücksichtigt, die mit Erkenntnissen aus anderen Datenquellen wie Ransomware-Leak-Websites und beobachteten Infrastruktur-Bedrohungen kombiniert werden. Angesichts der zunehmenden Zahl an Bedrohungsakteuren und vielfältigen Methoden fühlen wir uns mehr denn je unserem Auftrag verpflichtet, unsere Kunden vor Bedrohungen zu schützen. Aufgrund der großen Unsicherheit durch die weiterhin komplexe geopolitische und ökonomische Lage steigt der Bedarf an globalen Bedrohungsanalysen.

Die wirtschaftliche Unsicherheit durch den Krieg in der Ukraine hat zu einem massiven Energiepreisschock geführt, wie ihn die Welt seit den 1970er Jahren nicht erlebt hat, der die globale Wirtschaft schwer beeinträchtigt. Zudem war die Rückkehr des Krieges in Europa ein Weckruf für diejenigen, die den Sicherheits- und Verteidigungsansatz der EU sowie ihre Fähigkeit in Frage stellen, ihre Interessen insbesondere im Cyberspace zu verteidigen. Außerdem erkannte die US-Regierung die Notwendigkeit, sich dem geostrategischen Wettbewerb und dem Schutz kritischer Infrastruktur zu widmen sowie ausländische Desinformationskampagnen zu bekämpfen. SolarWinds, Hafnium, die Ukraine und andere Ereignisse haben die Regierung und den US-Kongress zu überparteilichen Maßnahmen für Sicherheitsstandards und Fördergelder veranlasst, die in erheblichem Maße auf den Verpflichtungen der USA und der Arbeit früherer US-Regierungen aufbauen. Wie genau wirkt sich diese Unsicherheit nun auf die Cyber-Sicherheit unserer Unternehmen, öffentlichen und privaten Institutionen sowie auf unsere demokratischen Werte aus?

Im letzten Quartal sah unser Team, wie der virtuelle Raum von Staaten in den Bereichen Spionage, Kriegsführung und Desinformation aktiv zur Durchsetzung politischer, ökonomischer und territorialer Ziele genutzt wurde. Der Krieg in der Ukraine hat zudem zu neuen Formen von Cyber-Angriffen geführt, und die Hacktivisten wurden immer geschickter und wagemutiger darin, Webseiten zu verfälschen, Informationen zu leaken und DDoS-Angriffe durchzuführen. Währenddessen werden weiterhin herkömmliche Cyber-Angriffe wie Social-Engineering-Angriffe (z. B. Phishing) genutzt, um die Angriffsopfer zu täuschen und dazu zu bringen, vertrauliche oder persönliche Informationen preiszugeben.

Darüber hinaus spielt Ransomware bei Unternehmen weltweit weiterhin eine große Rolle. Ähnlich wie bereits während der COVID-19-Pandemie stellen sich Cyber-Kriminelle schnell auf Unsicherheiten und Krisen ein,

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

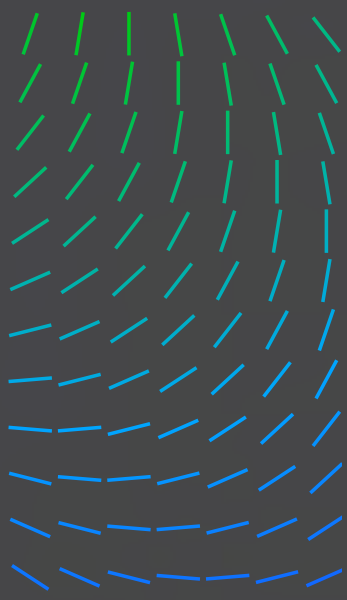
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



um davon zu profitieren. Ebenso wie sich die Bedrohungslandschaft weiterentwickelt, wird sich auch unsere Forschung ständig weiterentwickeln. Wir werden uns nach wie vor darauf konzentrieren, die Effektivität unserer Produkte zu verbessern und unsere Experten mit verwertbaren Informationen zu versorgen, damit sie wichtige Assets schützen können. Dieser Bericht macht deutlich, wie wichtig jedem Mitarbeiter die Arbeit des Trellix Advanced Research Centers ist. Alle Forscher und Experten in unserem Team widmen sich jedem Projekt mit Sorgfalt und viel Herzblut.

Teilen Sie uns mit, was Sie von diesem umfangreichen Bericht halten, und ob es Bereiche gibt, über die Sie mehr erfahren möchten. Kontaktieren Sie dazu mich oder unser Team auf Twitter unter @TrellixARC. Wir freuen uns auch darauf, Sie im April auf der RSA in San Francisco zu sehen.

John Fokker
Head of Threat Intelligence

METHODEN

Die Backend-Systeme von Trellix stellen Telemetriedaten bereit, die wir als Input für unsere vierteljährlichen Threats-Reports nutzen. Wir kombinieren unsere Telemetriedaten mit Open-Source-Daten zu Bedrohungen und unseren eigenen Untersuchungen weit verbreiteter Bedrohungen wie Ransomware, Aktivitäten staatlicher Akteure usw.

Bei Telemetrie geht es um Erkennungen, nicht um Infektionen. Eine Erkennung wird erfasst, wenn eines unserer Produkte eine Datei, URL, IP-Adresse oder einen anderen Indikator erkennt und dies an uns meldet.

Wir wissen beispielsweise, dass viele Unternehmen für Effektivitätstests Frameworks nutzen, die auf echte Malware-Proben zurückgreifen. Diese werden als Erkennung angezeigt, stellen jedoch keinesfalls eine Infektion dar.

Das Analysieren und Herausfiltern von False-Positives aus den Telemetriedaten wird kontinuierlich weiterentwickelt, wodurch neue Bedrohungskategorien entstehen können, die in früheren Berichten nicht vorkamen.

Außerdem entstehen dadurch neue Bedrohungskategorien, sodass immer mehr Trellix-Teams am vierteljährlichen Bericht mitwirken.

Die Privatsphäre unserer Kunden ist uns immer wichtig, auch bei der Telemetrie und Abbildung der Sektoren und Länder unserer Kunden.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

Der Kundenstamm variiert je nach Land, und es ist möglich, dass die Zahlen zwar einen Anstieg zeigen, wir uns die Daten aber genauer ansehen müssen, um sie richtig interpretieren zu können. Ein Beispiel: Der Telekommunikationssektor liegt in unseren Daten oft weit oben. Das muss aber nicht zwangsläufig bedeuten, dass dieser Sektor übermäßig häufig angegriffen wird. Der Telekommunikationssektor umfasst auch Internetdienstanbieter (Internet Service Provider, ISP) mit eigenen IP-Adressräumen, die von Unternehmen erworben werden können. Was bedeutet das? Meldungen aus dem IP-Adressraum des ISP werden zwar als Erkennungen für den Telekommunikationsbereich gewertet, könnten aber von ISP-Kunden stammen, die in einem anderen Sektor tätig sind.

RANSOMWARE: 4. QUARTAL 2022

In diesem Abschnitt stellen wir die verschiedenen Erkenntnisse vor, die wir über die Aktivitäten von Ransomware-Gruppen gesammelt haben. Die Informationen wurden aus mehreren Quellen erfasst, sodass ein besseres Bild über die Bedrohungslandschaft entsteht und Beobachtungsfehler verringert werden. Außerdem können wir auf diese Weise feststellen, welche Ransomware-Familie im 4. Quartal 2022 am einflussreichsten war. Die erste Quelle ist eine quantitative Quelle und zeigt die Ransomware-Kampagnen-Statistik, die aus der Korrelation der Kompromittierungsindikatoren (IOCs) für Ransomware und den Telemetriedaten von Trellix-Kunden gewonnen wurde. Die zweite ist eine qualitative Quelle und zeigt eine Analyse verschiedener Berichte der Sicherheitsbranche, die von der Threat Intelligence-Gruppe gründlich überprüft und analysiert wurden. Die dritte Quelle ist eine neue Kategorie und besteht aus Berichten über Ransomware-Opfer, die aus zahlreichen Leak-Websites von Ransomware-Gruppen zusammengetragen wurden. Die Daten wurden normalisiert, angereichert und analysiert, um eine anonymisierte Version der Ergebnisse zeigen zu können.

Mit den verschiedenen Perspektiven möchten wir möglichst viele der Puzzleteile bereitstellen, aus denen sich die aktuelle Bedrohungslandschaft zusammensetzt, denn sie liefern für sich allein genommen kein vollständiges Bild. Niemand hat Zugang zu allen Protokollen aller mit dem Internet verbundenen Systeme, nicht alle Sicherheitszwischenfälle werden gemeldet und nicht alle Opfer werden erpresst oder auf Leak-Websites gelistet. Deshalb kann die Kombination der verschiedenen Sichtweisen das Verständnis der zahlreichen Bedrohungen verbessern und zudem unsere eigenen blinden Flecken minimieren.

Eine fundierte Bewertung der Situation ergibt sich aus der Kombination quantitativer und qualitativer Daten aus verschiedenen Quellen, um eventuelle Nachteile und blinde Flecken zu reduzieren.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

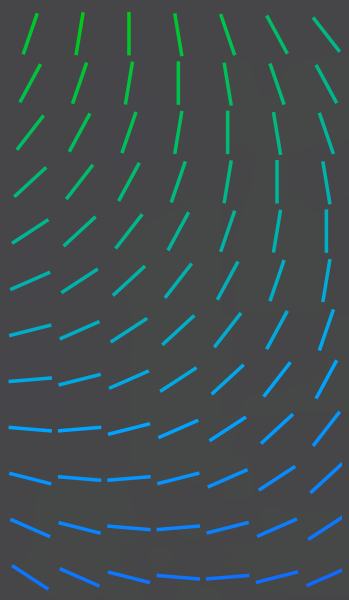
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



Ransomware-Highlights im 4. Quartal 2022

Einflussreichste Ransomware-Gruppe im 4. Quartal 2022: LockBit 3.0

Die Auswertung der verschiedenen Trellix-Quellen hat ergeben, dass LockBit 3.0 die einflussreichste Ransomware-Gruppe im 4. Quartal 2022 war. Der Rang der Gruppe ergibt sich anhand folgender Faktoren:

3. Gemäß der Analyse der Ransomware-Telemetriedaten aus den weltweit verteilten Trellix-Sensoren lag LockBit 3.0 auf Rang drei der einflussreichsten Ransomware-Gruppen des Quartals.

2. Laut der Analyse zahlreicher Kampagnen durch die Threat Intelligence-Gruppe lag LockBit 3.0 – zusammen mit der Ransomware Cuba – auf Rang zwei der am häufigsten von der Sicherheitsbranche gemeldeten Ransomware-Gruppen.

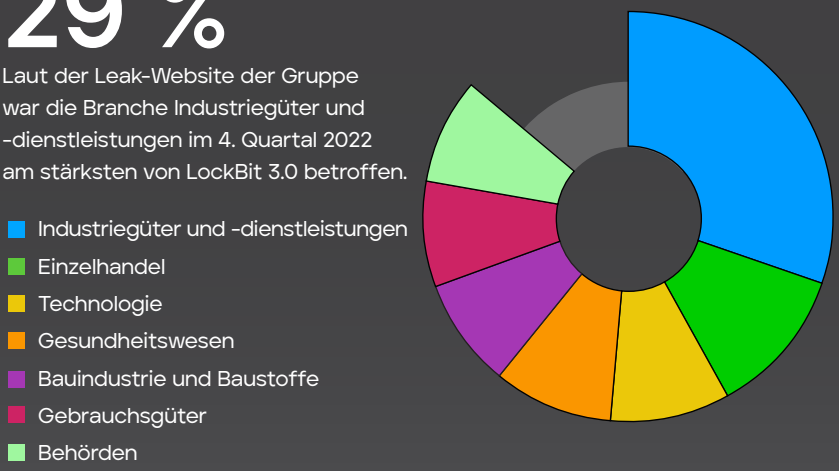
1. Die Leak-Website von LockBit 3.0 meldete die höchste Zahl von Ransomware-Opfern des Quartals. Die Gruppe versucht daher besonders intensiv, ihre Opfer durch Anprangern und Bloßstellen unter Druck zu setzen.

Dies sind weitere Kategorien und Erkenntnisse zu LockBit 3.0 aus dem 4. Quartal 2022:

VON LOCKBIT 3.0 BETROFFENE BRANCHEN, 4. QUARTAL 2022

29 %

Laut der Leak-Website der Gruppe war die Branche Industriegüter und -dienstleistungen im 4. Quartal 2022 am stärksten von LockBit 3.0 betroffen.



ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

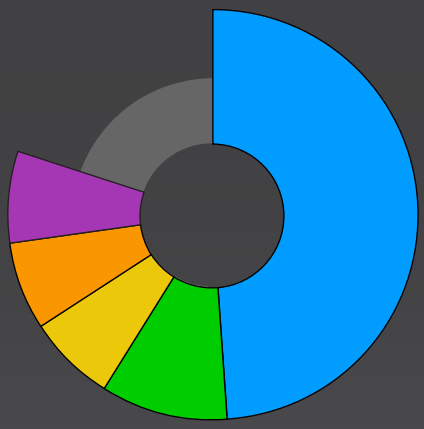
RESSOURCEN

VON LOCKBIT 3.0 BETROFFENE UNTERNEHMEN, NACH LAND, 4. QUARTAL 2022

49 %

Laut der Leak-Webseite der Gruppe waren US-Unternehmen im 4. Quartal 2022 am häufigsten (49 %) von LockBit 3.0 betroffen, gefolgt von britischen Unternehmen.

- USA
- Großbritannien
- Kanada
- Frankreich
- Brasilien



Von LockBit 3.0 verwendete Tools und Exploits

VON LOCKBIT 3.0 BEKANNTERMASSEN AUSGENUTZTE SCHWACHSTELLEN

CVE-2018-13379
CVE-2020-0787
CVE-2021-20028
CVE-2021-34473
CVE-2021-34523

VON LOCKBIT 3.0 GENUTZTE BÖSWILLIGE TOOLS

Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
Grabff	WinPEAS

VON LOCKBIT 3.0 GENUTZTE HARMLOSE TOOLS

BCDEdit	MiniDump	NSIS	Schtasks.exe
CMD	MpCmdRun.exe	PCHunter	VSSAdmin
Fltmc.exe	Mshta	PowerShell	wevtutil
Fsutil	Mstsc	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MEGASYNC	Nltest		

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

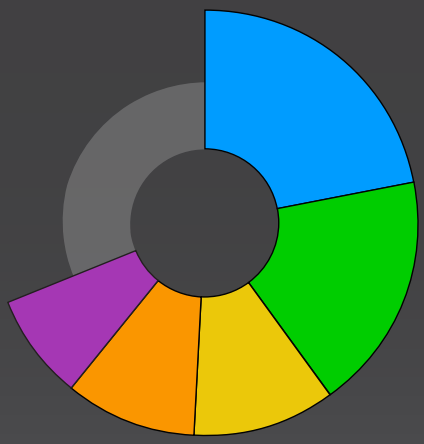
Ransomware aus der Perspektive unserer Telemetriedaten

Die folgenden Statistiken basieren auf Korrelationen zwischen unseren Telemetriedaten und unserer Knowledge Base für Bedrohungsdaten. Nach einer Analysephase identifizieren wir mithilfe dieser Daten Kampagnen innerhalb eines bestimmten Zeitraums und extrahieren ihre Merkmale. Die gezeigten Statistiken beziehen sich auf die Kampagnen, nicht auf die Erkennungen selbst. Unsere globalen Telemetriedaten haben Kompromittierungsindikatoren (IOCs) aufgezeigt, die zu verschiedenen Kampagnen von verschiedenen Ransomware-Gruppen gehören. Die folgenden Ransomware-Familien mit ihren jeweiligen Tools und Techniken zählen zu den am häufigsten vertretenen Familien in den identifizierten Kampagnen. Gleichzeitig sind die folgenden Länder und Branchen am stärksten von den identifizierten Kampagnen betroffen.

AM WEITESTEN VERBREITETE RANSOMWARE-FAMILIEN, 4. QUARTAL 2022

22 %

Cuba war im 4. Quartal 2022 die häufigste Ransomware-Familie. Zeppelin wurde oft von Vice Society eingesetzt. Erfahren Sie mehr über die Leaks der Yanluowang-Daten



- Cuba
- Hive
- LockBit
- Zeppelin
- Yanluowang

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

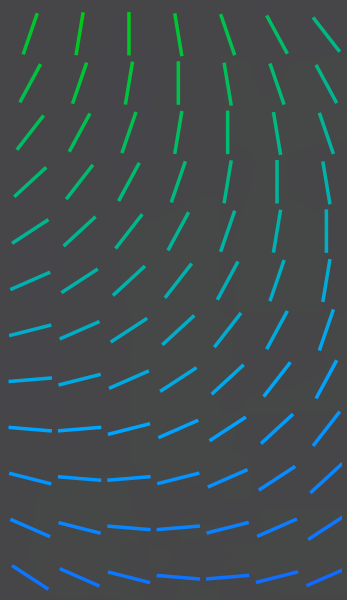
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



AM HÄUFIGSTEN VON RANSOMWARE-GRUPPEN GENUTZTE BÖSWILLIGE TOOLS, 4. QUARTAL 2022

41 %

Cobalt Strike war im 4. Quartal 2022 das von Ransomware-Gruppen am häufigsten genutzte böswillige Tool.

1.	Cobalt Strike	41 %
2.	Mimikatz	23 %
3.	BURNTCIGAR	13 %
4.	VMProtect	12 %
5.	POORTRY	11 %

AM HÄUFIGSTEN VON RANSOMWARE-GRUPPEN GENUTZTE MITRE-ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1.	Datenverschlüsselung für mehr Auswirkung	17 %
2.	Erkennung von System-informationen	11 %
3.	PowerShell	10 %
4.	Eintrittstool-Übertragung	10 %
5.	Windows Command Shell	9 %

AM HÄUFIGSTEN VON RANSOMWARE-GRUPPEN GENUTZTE HARMLOSE TOOLS, 4. QUARTAL 2022

21 %

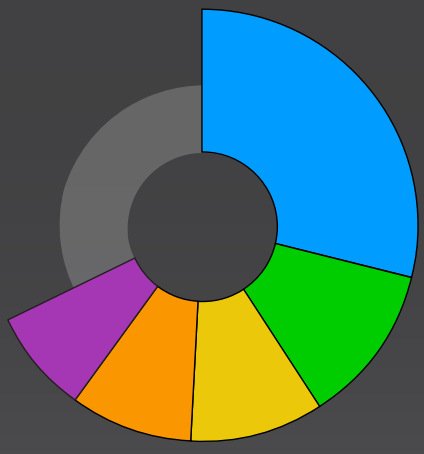
CMD war im 4. Quartal 2022 das von Ransomware-Gruppen am häufigsten genutzte harmlose Tool.

1.	CMD	21 %
2.	PowerShell	14 %
3.	Net	10 %
4.	Reg	8 %
5.	PsExec	8 %

AM STÄRKSTEN VON RANSOMWARE-GRUPPEN BETROFFENE LÄNDER, 4. QUARTAL 2022

29 %

Laut den Trellix-Telemetriedaten war die USA im 4. Quartal 2022 das am stärksten von Ransomware-Gruppen betroffene Land.



- USA
- China
- Katar
- Japan
- Indonesien

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

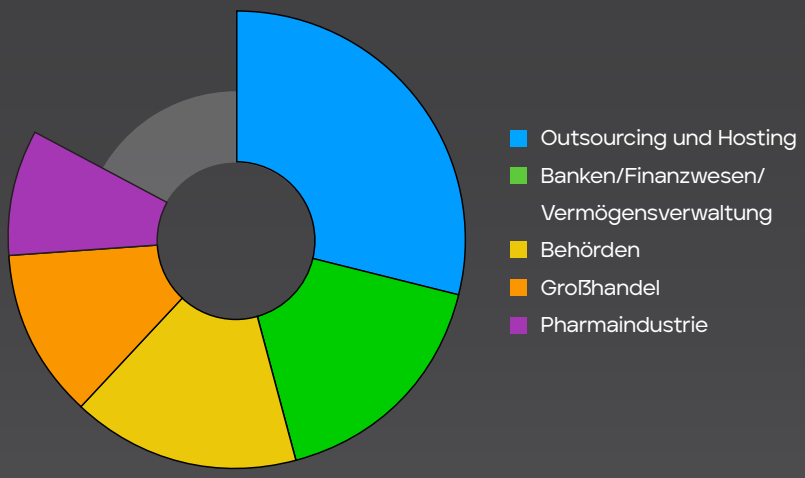
AUTOREN UND FORSCHER

RESSOURCEN

AM STÄRKSTEN VON RANSOMWARE-GRUPPEN BETROFFENE BRANCHEN, 4. QUARTAL 2022

29 %

Laut den Trellix-Telemetriedaten war Outsourcing und Hosting im 4. Quartal 2022 die am stärksten von Ransomware-Gruppen betroffene Branche. Dies korreliert mit der durchschnittlichen Größe der betroffenen Unternehmen, die auf Leak-Websites aufgeführt werden. Häufig haben diese Unternehmen keinen eigenen zugewiesenen IP-Adressenblock und sind auf Drittanbieter angewiesen.



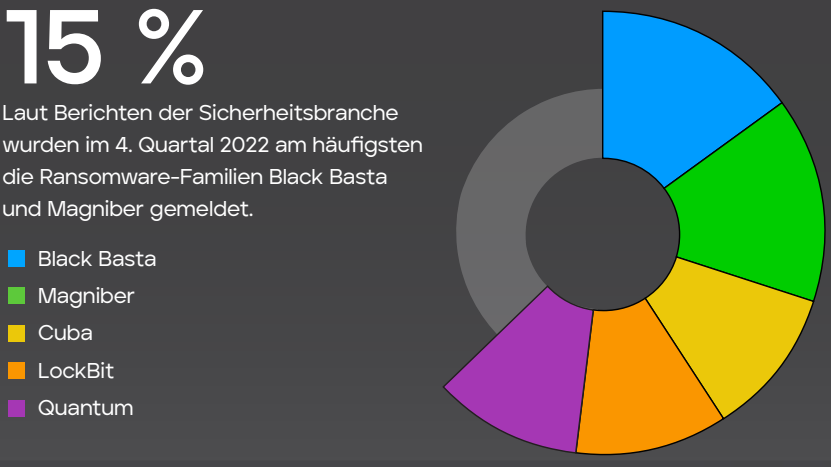
Von der Sicherheitsbranche gemeldete Ransomware

Die folgenden Statistiken beruhen auf öffentlichen Berichten sowie interner Forschung. Bitte beachten Sie, dass nicht alle Ransomware-Zwischenfälle gemeldet werden. Viele Ransomware-Familien sind seit einiger Zeit aktiv und fallen dadurch in den jeweiligen Quartalen naturgemäß weniger auf als neue Familien. Daher geben diese Zahlen Aufschluss über die Ransomware-Familien, die von der Sicherheitsbranche im 4. Quartal 2022 als besonders einflussreich und relevant eingestuft wurden.

AM HÄUFIGSTEN GEMELDETE RANSOMWARE-FAMILIEN, 4. QUARTAL 2022

15 %

Laut Berichten der Sicherheitsbranche wurden im 4. Quartal 2022 am häufigsten die Ransomware-Familien Black Basta und Magniber gemeldet.



ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

HÄUFIGE ANGRIFFSTECHNIKEN VON RANSOMWARE-FAMILIEN, 4. QUARTAL 2022

19 %

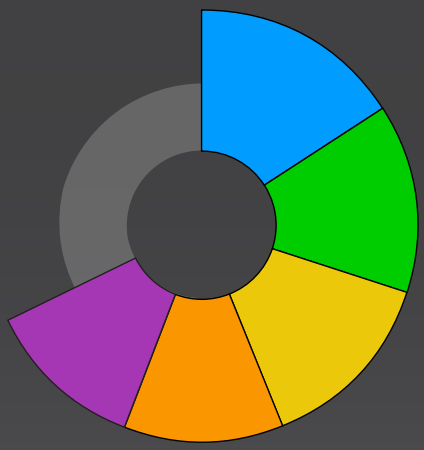
Laut Berichten der Sicherheitsbranche wurde im 4. Quartal 2022 am häufigsten die Ransomware-Angriffstechnik „Datenverschlüsselung für mehr Auswirkung“ gemeldet.

1.	Datenverschlüsselung für mehr Auswirkung	19 %
2.	Windows Command Shell	11 %
3.	Erkennung von Systeminformationen	10 %
4.	Eintrittstool-Übertragung	10 %
5.	PowerShell	10 %

AM HÄUFIGSTEN VON RANSOMWARE-FAMILIEN ANGEGRIFFENE BRANCHEN, 4. QUARTAL 2022

16 %

Laut Berichten der Sicherheitsbranche wurde das Gesundheitswesen im 4. Quartal 2022 von allen Branchen am häufigsten von Ransomware-Familien angegriffen.



- Gesundheitswesen
- Finanzsektor
- Behörden
- Fertigungsunternehmen
- Transport

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

AM HÄUFIGSTEN VON RANSOMWARE-FAMILIEN ANGEGRIFFENE LÄNDER, 4. QUARTAL 2022

19 %

Laut den Berichten der Sicherheitsbranche wurde im 4. Quartal 2022 die USA am stärksten von Ransomware-Gruppen angegriffen.

VON RANSOMWARE-FAMILIEN AUSGENUTZTE CVES, 4. QUARTAL 2022

1.	CVE-2021-31207	16 %
	CVE-2021-34474	16 %
	CVE-2021-34523	16 %
2.	CVE-2021-34527	13 %
3.	CVE-2021-26855	9 %
	CVE-2021-27065	9 %

VON RANSOMWARE-FAMILIEN GENUTZTE BÖSWILLIGE TOOLS, 4. QUARTAL 2022

44 %

Laut Berichten der Sicherheitsbranche wurde im 4. Quartal 2022 von den gemeldeten Ransomware-Familien das böswillige Tool Cobalt Strike am häufigsten eingesetzt.

1.	Cobalt Strike	44 %
2.	QakBot	13 %
3.	IcedID	9 %
4.	BURNTCIGAR	7 %
5.	Carbanak	7 %
	SystemBC	7 %

VON RANSOMWARE-FAMILIEN GENUTZTE HARMLOSE TOOLS, 4. QUARTAL 2022

21 %

Laut Berichten der Sicherheitsbranche wurde im 4. Quartal 2022 von den gemeldeten Ransomware-Familien das harmlose Tool PowerShell am häufigsten eingesetzt.

1.	PowerShell	21 %
2.	CMD	18 %
3.	Rundll32	11 %
4.	VSSAdmin	10 %
5.	WMIC	9 %

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

Berichte über Ransomware-Opfer auf Leak-Websites, 4. Quartal 2022

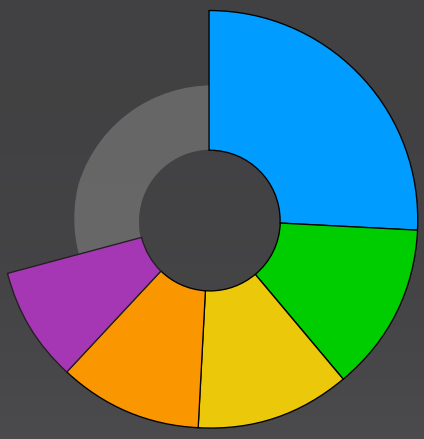
Die Daten in diesem Abschnitt stammen von sogenannten Leak-Websites verschiedener Ransomware-Gruppen, die ihre Opfer mit der Veröffentlichung von Informationen der Betroffenen auf ihren Webseiten erpressen. Wenn die Verhandlungen ins Stocken geraten oder die Opfer das Lösegeld nicht bis zum Ablauf der Frist zahlen, veröffentlicht die Gruppe Informationen, die sie von den Opfern erbeutet hat. Wir sammeln mithilfe des Open-Source-Tools RansomLook zahlreiche Beiträge, die wir intern normalisieren und anreichern, um eine anonymisierte Version der Opferanalyse zu erstellen.

Dabei muss beachtet werden, dass nicht alle Ransomware-Opfer auf den jeweiligen Leak-Websites erscheinen. Viele Opfer zahlen das Lösegeld und werden dort nicht erwähnt. Die Zahlen sind ein Gradmesser für die Opfer, die von Ransomware-Gruppen erpresst oder bestraft wurden, und sollten nicht mit der Gesamtzahl der Opfer gleichgesetzt werden.

RANSOMWARE-GRUPPEN MIT DEN MEISTEN GEMELDETEN OPFERN, 4. QUARTAL 2022

26 %

Unter den Top-10-Ransomware-Gruppen mit der größten Anzahl von Opfern auf den jeweiligen Leak-Websites entfielen im 4. Quartal 2022 allein 26 % auf LockBit 3.0.



ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

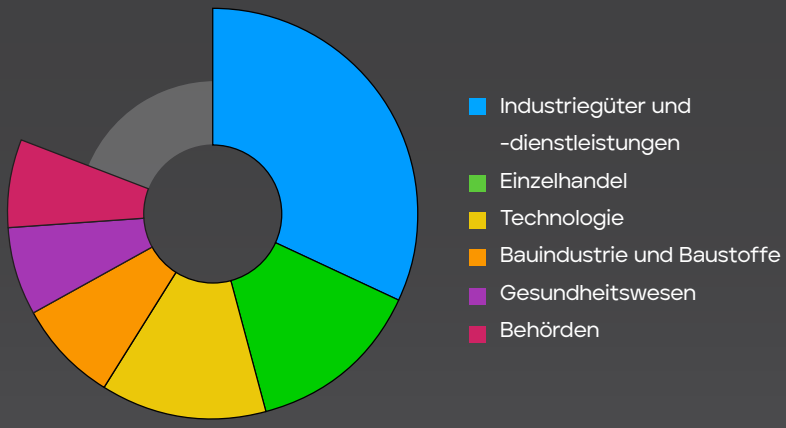
AUTOREN UND FORSCHER

RESSOURCEN

LAUT LEAK-WEBSITES VON RANSOMWARE-GRUPPEN BETROFFENE BRANCHEN, 4. QUARTAL 2022

32 %

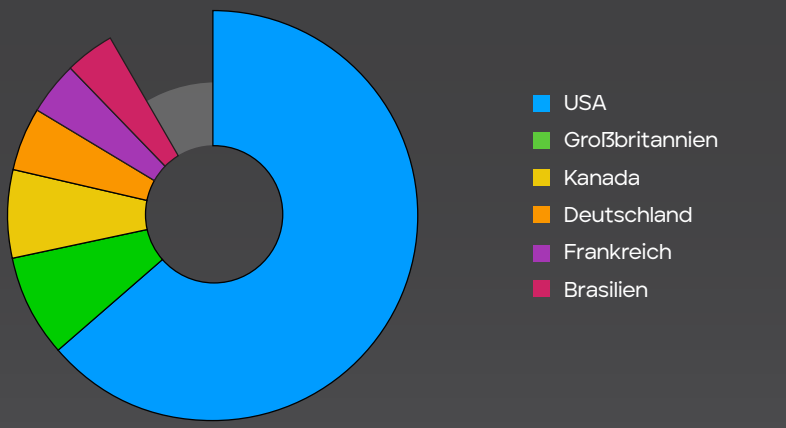
Laut den Leak-Websites waren im 4. Quartal 2022 Industriegüter und -dienstleistungen die am stärksten von Ransomware-Gruppen betroffene Branche. Industriegüter und -dienstleistungen umfassen alle materiellen Produkte und immateriellen Dienstleistungen, die hauptsächlich im Bauwesen und in der Herstellung verwendet werden.



LAUT LEAK-WEBSITES VON RANSOMWARE-GRUPPEN BETROFFENE LÄNDER, 4. QUARTAL 2022

63 %

Im 4. Quartal 2022 kamen 63 % der zehn am häufigsten auf Leak-Websites von Ransomware-Gruppen aufgeführten Unternehmen aus den USA, gefolgt von Großbritannien (8 %) und Kanada (7 %).



ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

In diesem Abschnitt stellen wir die von uns gesammelten Erkenntnisse über die Aktivitäten staatlicher Akteure vor. Die Informationen wurden aus mehreren Quellen zusammengetragen, um ein besseres Bild der Bedrohungslandschaft zu gewinnen und Beobachtungsfehler zu verringern. Zunächst präsentieren wir die Statistik, die aus der Korrelation der IOCs staatlicher Akteure und den Telemetriedaten von Trellix-Kunden gewonnen wurden. Danach folgen die Erkenntnisse aus verschiedenen Berichten, die von der Sicherheitsbranche veröffentlicht und von der Threat Intelligence-Gruppe gründlich überprüft und analysiert wurden.

Wichtige Fakten zu staatlichen Akteuren, 4. Quartal 2022

- In den USA und Deutschland gab es einen deutlichen Anstieg bei Angriffen staatlicher Akteure.
- China und Vietnam agierten im 4. Quartal als staatliche Akteure.

Statistiken zu staatlichen Akteuren aus der Perspektive unserer globalen Telemetrie

Die folgenden Statistiken basieren auf Korrelationen zwischen unseren Telemetriedaten und unserer Knowledge Base für Bedrohungsdaten. Nach einer Analysephase identifizieren wir in den Daten Kampagnen innerhalb eines bestimmten Zeitraums und extrahieren ihre Merkmale. Die gezeigten Statistiken beziehen sich auf die Kampagnen, nicht auf die Erkennungen selbst. Aufgrund zahlreicher Protokollverdichtungen, des Einsatzes von Bedrohungssimulationen durch unsere Kunden und allgemeiner Korrelationen mit der Knowledge Base für Bedrohungsdaten werden die Daten manuell gefiltert, um gewünschte Kriterien zu erfüllen.

Unsere globalen Telemetriedaten haben Kompromittierungsindikatoren (IOCs) aufgezeigt, die mit verschiedenen Kampagnen von APT-Gruppen (Advanced Persistent Threat, hochentwickelte hartnäckige Bedrohungen) in Zusammenhang stehen. Die folgenden Länder und Bedrohungsakteure mit ihren jeweiligen Tools und Techniken sind bei den identifizierten Kampagnen am häufigsten vertreten. Gleichzeitig sind die folgenden Länder und Branchen am stärksten von den identifizierten Kampagnen betroffen.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

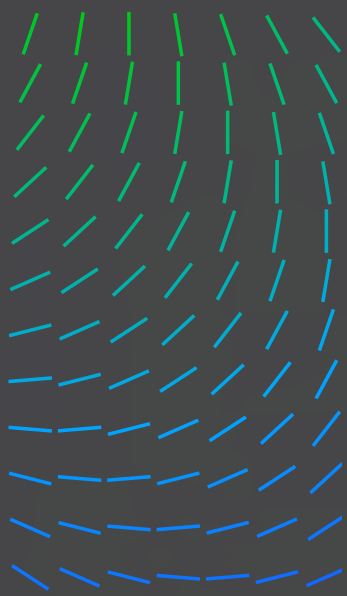
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

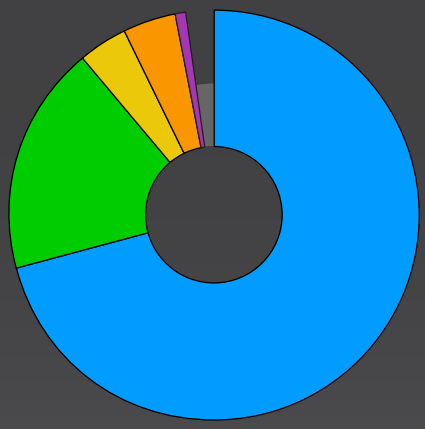


Erkenntnisse basierend auf Telemetriedaten über staatliche Akteure

LÄNDER MIT DEN MEISTEN AKTIVITÄTEN STAATLICHER AKTEURE, 4. QUARTAL 2022

71 %

China war im 4. Quartal 2022 das Land mit den meisten Aktivitäten staatlicher Akteure.

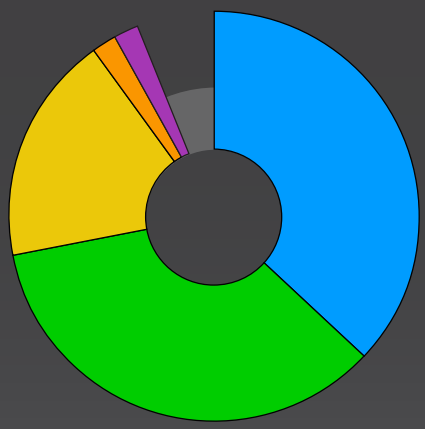


- China
- Nordkorea
- Russland
- Iran
- Libanon

AKTIVSTE GRUPPEN VON BEDROHUNGSAKTEUREN, 4. QUARTAL 2022

37 %

Laut den Telemetriedaten über staatliche Akteure war im 4. Quartal 2022 Mustang Panda die aktivste Gruppe von Bedrohungsakteuren.



- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

BEI AKTIVITÄTEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1.	DLL-Side-Loading	14 %
2.	Rundll32	13 %
3.	Verschleierte Dateien oder Informationen	12 %
4.	Windows Command Shell	11 %
5.	Schlüssel zur Registrierungsausführung/ Systemstartordner	10 %

BEI AKTIVITÄTEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE BÖSWILLIGE TOOLS, 4. QUARTAL 2022

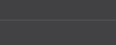
1.	PlugX	24 %
2.	BLUEHAZE	23 %
3.	DARKDEW	23 %
4.	MISTCLOAK	23 %
5.	Remote-Zugriffs-Trojaner JSX	2 %

BEI AKTIVITÄTEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE HARMLOSE TOOLS, 4. QUARTAL 2022

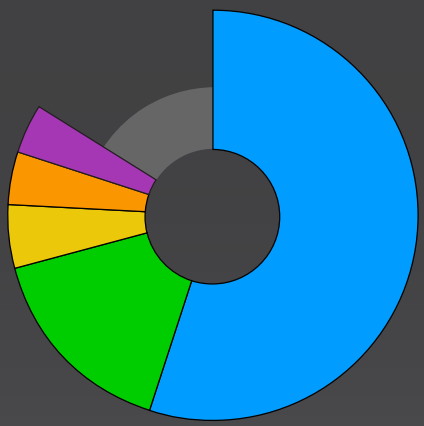
1.	Rundll32	22 %
2.	CMD	19 %
3.	Reg	17 %
4.	Ncat	12 %
5.	Regsvr32	6 %

AM STÄRKSTEN VON AKTIVITÄTEN STAATLICHER AKTEURE BETROFFENE LÄNDER, 4. QUARTAL 2022

55 %



Die USA war das im 4. Quartal 2022 am stärksten von Aktivitäten staatlicher Akteure betroffene Land.



- USA
- Vietnam
- Indien
- Deutschland
- China

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

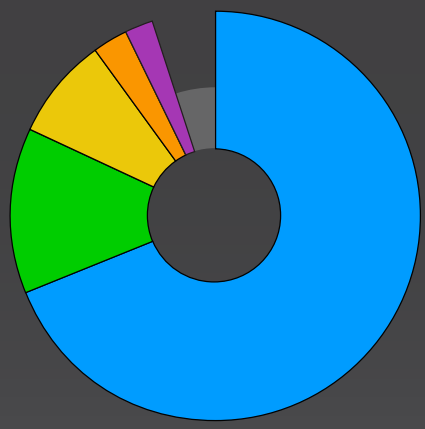
AUTOREN UND FORSCHER

RESSOURCEN

AM STÄRKSTEN VON AKTIVITÄTEN STAATLICHER AKTEURE BETROFFENE BRANCHEN, 4. QUARTAL 2022

69 %

Das Transportwesen war die im 4. Quartal 2022 am stärksten von Aktivitäten staatlicher Akteure betroffene Branche.



- Verkehrs- und Transportwesen
- Energiesektor/Öl- und Gassektor
- Großhandel
- Einzelhandel
- Banken/Finanzwesen/ Vermögensverwaltung

Zwischenfälle durch staatliche Akteure laut öffentlichen Berichten, 4. Quartal 2022

Die Statistiken beruhen auf öffentlichen Berichten und interner Forschung – nicht auf Telemetriedaten aus den Protokollen unserer Kunden. Bitte beachten Sie, dass nicht alle Zwischenfälle mit staatlichen Akteuren gemeldet werden. Viele Kampagnen nutzen Techniken, Taktiken und Prozeduren (TTPs), die bereits bekannt sind und daher seltener gemeldet werden. In der Branche liegt der Fokus stärker auf neuartigen Kampagnen, bei denen die Akteure etwas Neues versucht oder einen Fehler begangen haben. Die Zahlen geben Aufschluss darüber, was von der Sicherheitsbranche im 4. Quartal 2022 als aufschlussreich und relevant eingestuft wurde.

BEI KAMPAGNEN STAATLICHER AKTEURE AM HÄUFIGSTEN GEMELDETE LÄNDER, 4. QUARTAL 2022

37 %

Im 4. Quartal 2022 kamen 37 % der öffentlich gemeldeten Kampagnen von staatlichen Akteuren aus China.

1.	China	37 %
2.	Nordkorea	24 %
3.	Iran	1 %
4.	Russland	1 %
5.	Indien	1 %

BEI GEMELDETEN AKTIVITÄTEN STAATLICHER AKTEURE AM HÄUFIGSTEN AUFTRETENDE BEDROHUNGSAKTEURE, 4. QUARTAL 2022

33 %

Lazarus war im 4. Quartal 2022 der aktivste Bedrohungsakteur unter den gemeldeten Aktivitäten staatlicher Akteure.

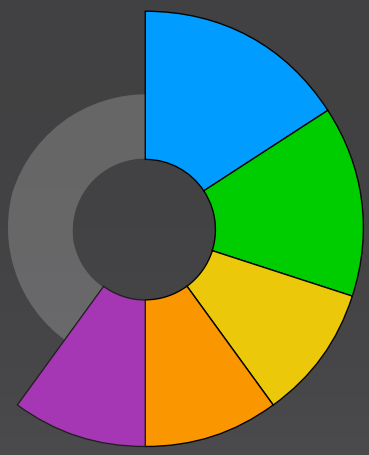
1.	Lazarus	33 %
2.	Mustang Panda	17 %
3.	APT34 APT37 APT41 COLDRIVER Patchwork Polonium SideWinder Winnti-Gruppe	je 1 %

AM HÄUFIGSTEN VON GEMELDETEN KAMPAGNEN STAATLICHER AKTEURE ANGEGRIFFENE LÄNDER, 4. QUARTAL 2022

16 %

Die USA war das im 4. Quartal 2022 am häufigsten von Kampagnen staatlicher Akteure angegriffene Land.

- USA
- Großbritannien
- Pakistan
- Russland
- Ukraine

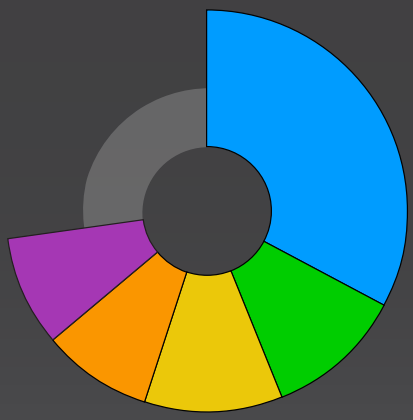


AM HÄUFIGSTEN VON GEMELDETEN KAMPAGNEN STAATLICHER AKTEURE ANGEGRIFFENE BRANCHEN, 4. QUARTAL 2022

33 %

Von allen Branchen wurden Behörden im 4. Quartal 2022 am häufigsten durch gemeldete Kampagnen staatlicher Akteure angegriffen, gefolgt von Militär (11 %) und Telekommunikation (11 %).

- Behörden
- Militär
- Telekommunikation
- Energieversorgung
- Finanzsektor



BEI GEMELDETEN KAMPAGNEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE BÖSWILLIGE TOOLS, 4. QUARTAL 2022

1.	PlugX	22 %
2.	Cobalt Strike	17 %
3.	Metasploit	13 %
4.	BlindingCan	9 %
5.	Scanbox ShadowPad ZeroCleare	je 9 %

BEI GEMELDETEN KAMPAGNEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE HARMLOSE TOOLS, 4. QUARTAL 2022

1.	CMD	32 %
2.	Rundll32	20 %
3.	PowerShell	14 %
4.	Reg	8 %
5.	Schtasks.exe	7 %

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

BEI GEMELDETEN KAMPAGNEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1.	Eintrittstool-Übertragung	13 %
2.	Erkennung von Systeminformationen	13 %
3.	Verschleierte Dateien oder Informationen	12 %
4.	Web-Protokolle	11 %
5.	Entschleierung/Dekodierung von Dateien oder Informationen	11 %

BEI GEMELDETEN KAMPAGNEN STAATLICHER AKTEURE BEOBACHTETE AUSGENUTZTE SCHWACHSTELLEN, 4. QUARTAL 2022

CVE-2017-11882	CVE-2020-17143
CVE-2021-44228	CVE-2021-21551
CVE-2018-0802	CVE-2021-26606
CVE-2021-26855	CVE-2021-26857
CVE-2021-27065	CVE-2021-26858
CVE-2021-34473	CVE-2021-28480
CVE-2021-34523	CVE-2021-28481
CVE-2015-2545	CVE-2021-28482
CVE-2017-0144	CVE-2021-28483
CVE-2018-0798	CVE-2021-31196
CVE-2018-8581	CVE-2021-31207
CVE-2019-0604	CVE-2021-40444
CVE-2019-0708	CVE-2021-45046
CVE-2019-16098	CVE-2021-45105
CVE-2020-0688	CVE-2022-1040
CVE-2020-1380	CVE-2022-30190
CVE-2020-1472	CVE-2022-41128
CVE-2020-17141	

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

Aus den Beobachtungen der Trellix Insights Global Threat Intelligence-Plattform ergaben sich folgende Informationen und Einblicke in die Bedrohungslandschaft des 4. Quartals 2022:

WICHTIGE FAKTEN ZU LOLBIN-ANGRIFFEN, 4. Quartal 2022

- Living off the Land-Techniken werden weiterhin genutzt, z. B. für Erstzugriff, Ausführung, Erkennung, Persistenz und Wirkung.
- Daten aus dem 4. Quartal 2022 zeigen, dass nach wie vor Befehls- und Skripttechniken über die Windows-Befehlszeile (Windows Command Shell) oder PowerShell ausgeführt werden und dies damit die am häufigsten (aus)genutzte Technik ist.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

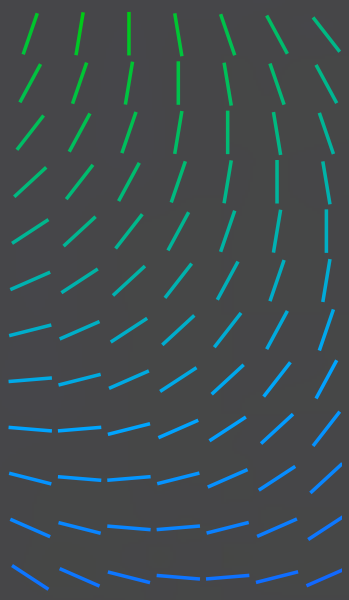
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



- Cyber-Kriminelle – erfahrene APT-Akteure, finanziell motivierte Gruppen sowie Hacktivisten – setzen LOLBIN-Taktiken sehr häufig ein.

Auch Neulinge, Gelegenheitskriminelle und Skript-Kiddies, die sich als Akteure versuchen, nutzen die bereits in das beliebte Exploit-Framework integrierten Binärdateien beim amateurhaften Hacken von Rechnern oder Ausnutzen von Schwachstellen.

Living off the Land-Techniken werden weiterhin für schädliche Zwecke wie Erstzugriff, Ausführung, Erkennung, Persistenz und Wirkung (aus)genutzt. Die Daten aus dem 4. Quartal 2022 zeigen, dass nach wie vor Befehls- und Skripttechniken über die Windows-Befehlszeile (Windows Command Shell) und PowerShell ausgeführt werden und dies die am häufigsten (aus)genutzte Technik ist.

BETRIEBSSYSTEM-BINÄRDATEIEN MIT DER WEITESTEN VERBREITUNG, 4. QUARTAL 2022

47 %

Bei den zehn im 4. Quartal 2022 am häufigsten missbrauchten Betriebssystem-Binärdateien wird Windows Command Shell bei nahezu der Hälfte (47 %) der gemeldeten Vorfälle eingesetzt, gefolgt von PowerShell (32 %) und Rundll32 (27 %).

1.	Windows Command Shell	47 %
2.	PowerShell	32 %
3.	Rundl32	27 %
4.	Schtasks	23 %
5.	WMI	21 %

Kriminelle – APT-Akteure, finanziell motivierte Gruppen sowie „woke“ Hacktivisten – setzen Living off the Land-Taktiken sehr häufig ein.

Über unsere Trellix Insights-Plattform erfasste Ereignisse, bei denen Bedrohungsakteure Windows-Binärdateien nutzten, führten zur Bereitstellung weiterer Malware wie Information Stealer-Programme, Remote-Zugriff-Trojaner oder Ransomware. Möglicherweise wurden Binärdateien wie MSHTA, WMI oder WScript ausgeführt, um weitere Schaddaten aus den von den Angreifern kontrollierten Ressourcen abzurufen.

AM HÄUFIGSTEN GENUTZTE DRITTANBIETER-TOOLS, 4. QUARTAL 2022

1.	Remote-Zugriffs-Tools	58 %
2.	Dateiübertragung	22 %
3.	Post-Exploitation-Tools	20 %
4.	Netzwerk-erkennung	16 %
5.	AD-Erkennung	10 %

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

Tools für Remote-Zugriff und -Kontrolle werden von Bedrohungsakteuren weiterhin bevorzugt missbraucht. Dazu zählen auch Tools, die eigentlich für Sicherheitsexperten gedacht sind. Häufig verwenden Bedrohungsakteure sie, um Beacons aufrechtzuerhalten, Exfiltrationen zu automatisieren oder Informationen zu sammeln und zu komprimieren.

Von kostenlosen und Open Source-Tools werden Packprogramme missbraucht, um eine legitime Software zusammen mit schädlichen Inhalten zu verpacken oder um Malware zu packen. Mit diesen Taktiken versuchen sie, einer Erkennung zu entgehen und Analysen zu erschweren.

ERKENNTNISSE ZU COBALT STRIKE, 4. Quartal 2022

Die Threat Intelligence-Gruppe des Trellix Advanced Research Center überwacht die Nutzung der Cobalt Strike Team-Server (Cobalt Strike-Command-and-Control-Server) und kombiniert dazu Bedrohungssuchmethoden für Schaddaten und Infrastruktur. Nachfolgend präsentieren wir Ihnen die Erkenntnisse, die wir bei der Analyse der gesammelten Cobalt Strike-Beacons gewonnen haben:

15 %
COBALT STRIKE-TESTLIZENZEN

Nur 15 % der identifizierten Cobalt Strike-Beacons hatten eine Testlizenz für Cobalt Strike. Diese Version von Cobalt Strike besitzt die meisten bekannten Funktionen des Post-Exploitation-Tools, fügt jedoch verräterische Zeichen hinzu und entfernt die Verschlüsselung während der Übertragung, sodass die Schaddaten leicht von Sicherheitslösungen erkannt werden können.

87 %
RUNDLL32.EXE

Rundll32.exe ist der Standard-prozess zum Erstellen von Sitzungen und zur Ausführung von Post-Exploitation-Aufgaben. Er wurde in 87 % der identifizierten Beacons gefunden.

5 % HOST HTTP-HEADER

Mindestens 5 % der beobachteten Cobalt Strike-Beacons verwendeten den Host HTTP-Header – eine Option, die das Domain Fronting mit Cobalt Strike erleichtert. Beim Domain Fronting werden CDNs (Content Delivery Networks) missbraucht, die mehrere Domänen hosten. Die Angreifer verbergen eine HTTPS-Anfrage zu einer schädlichen Webseite unter einer TLS-Verbindung zu einer legitimen Webseite.

22 % DNS-BEACONS

22 % der identifizierten Cobalt Strike-Beacons waren DNS-Beacons. Dieser Schaddaten-Typ kommuniziert mit dem Cobalt Strike Team-Server der Angreifer (dem autoritativen Server der Domäne) über DNS-Anfragen, um seine Aktivitäten zu verschleiern.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

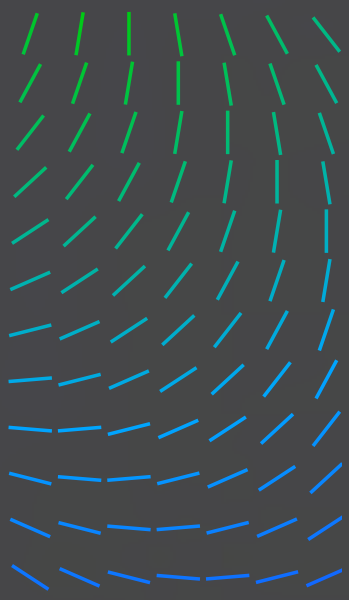
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

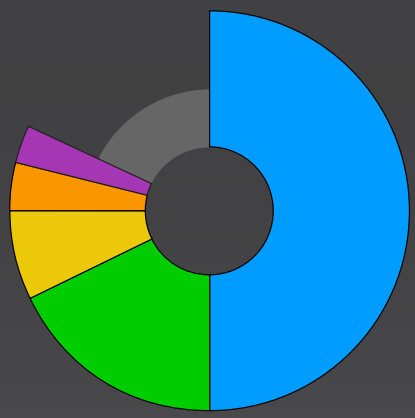
RESSOURCEN



LÄNDER, DIE COBALT STRIKE TEAM-SERVER AM HÄUFIGSTEN HOSTEN, 4. QUARTAL 2022

50 %

Die Hälfte aller im 4. Quartal 2022 erkannten Cobalt Strike Team-Server befanden sich in China, was vor allem auf den Umfang des in China verfügbaren Cloud-Hosting-Angebots zurückzuführen ist.



- China
- USA
- Hongkong
- Russland
- Niederlande

GOOTLOADER, 4. QUARTAL 2022

Gootloader ist eine modulare Malware, die in einigen Fällen synonym mit einer anderen Malware namens „GootKit" oder „GootKit Loader" verwendet wird. Die aktuellen modularen Funktionen der Malware Gootloader werden zur Verteilung weiterer Schaddaten wie REvil, Kronos, Cobalt Strike und Icedid genutzt.

Vor kurzem wurde beobachtet, wie Gootloader Suchmaschinen-optimierung (Search Engine Optimization, SEO) nutzte, um ahnungslose Benutzer auf kompromittierte oder gefälschte Webseiten zu locken, auf denen sich eine Archivdatei befand, die eine schädliche JavaScript-Datei enthielt. Bei dieser Technik müssen die Benutzer jedoch das Archiv öffnen und den Inhalt ausführen, wodurch wiederum der JavaScript-Code über den Windows Scripting Host ausgeführt wird. Nach der erfolgreichen Ausführung kommuniziert Gootloader mit einem C&C-Server (Command-and-Control) und ruft weitere Malware ab.

Bei Gootloader handelt es sich vermutlich um Malware-as-a-Service (MaaS), die im Abonnement angeboten wird. Sie ermöglicht Bedrohungsakteuren, mehrere zusätzliche Schaddaten zu laden und stellt daher eine erhebliche Bedrohung für Unternehmensumgebungen dar.

Über unseren internen Gootloader-Tracker haben wir eine aktuelle Variante identifiziert, die am 18. November 2022 beobachtet wurde, sowie ältere Varianten, die nach dem 13. November 2022 nicht mehr auftraten. Die neueste Variante enthält folgende Änderungen:

- Entfernung der Funktion zur Manipulation von Registrierungen
- Steigerung der Remote-Netzwerk-Anfragen auf zehn URLs statt drei

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

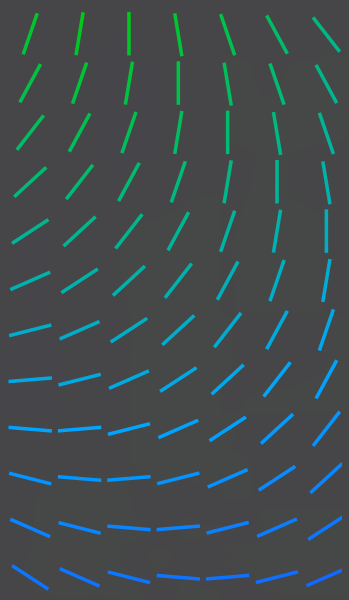
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



- PowerShell-Skripte können über CScript aufgerufen werden
- Persistenz für alle Benutzeranmeldungen

Unser Tracking-Prozess für Gootloader

Die neue Gootloader-Variante wurde mit mehreren Verschleierungsebenen weiterentwickelt. Jede verschachtelte Phase verwendet nach dem Entpacken Variablen, die aus den vorherigen Phasen geladen wurden. Dadurch wird die Analyse erschwert. Die bei unserer YARA-Bedrohungssuche gesammelten Proben werden in ein statisches JavaScript- und PowerShell-Analyseprogramm eingespeist, um IOCs wie C&C-Server und eindeutige ID-Signaturen zu extrahieren. Die IOCs können dazu dienen, bestimmte Instanzen von Gootloader auf anderen Systemen zu erkennen und zu beobachten.

Danach wird mithilfe von Anfragen an die Trellix-Datenbank für URL-Reputation festgestellt, bei welchen der extrahierten Gootloader-IOCs es sich um schädliche, potenziell kompromittierte legitime Domänen und bei welchen es sich um legitimen Domänen handelt, die als Köder Analysen behindern sollen.

Erkenntnisse basierend auf Gootloader-Telemetriedaten

Die nachstehenden Statistiken beziehen sich auf die Kampagnen, die aus den extrahierten IOCs und den Protokollen unserer Kunden korreliert wurden, und nicht die Erkennungen selbst. Bei Gootloader beruhen die meisten Erkennungen auf Domänentreffern. Da die Malware Köder-Domänen verwendet, sollten die Statistiken mit Vorsicht und mit mittlerer Konfidenz interpretiert werden.

AM STÄRKSTEN MIT GOOTLOADER ANGEGRIFFENE LÄNDER, 4. QUARTAL 2022

37 %

Die USA war im 4. Quartal 2022 das Land, das am stärksten mit Gootloader angegriffen wurde.

1.	USA	37 %
2.	Italien	19 %
3.	Indien	11 %
4.	Indonesien	9 %
5.	Frankreich	5 %

AM HÄUFIGSTEN VON GOOTLOADER GENUTZTE MITRE-ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1. Entschleierung/ Dekodierung von Dateien oder Informationen
2. JavaScript
3. Verschleierte Dateien oder Informationen
4. PowerShell
5. Process Hollowing

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

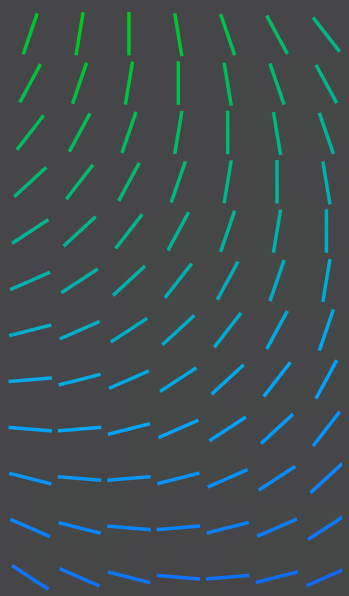
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

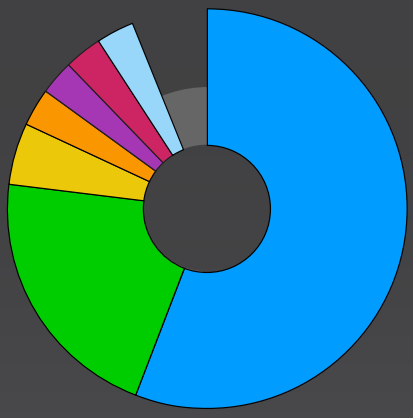
RESSOURCEN



AM STÄRKSTEN MIT GOOTLOADER ANGEGRIFFENE BRANCHEN, 4. QUARTAL 2022

56 %

Die Telekommunikationsbranche wurde im 4. Quartal 2022 am häufigsten mit Gootloader angegriffen.



Am häufigsten von Gootloader genutzte MITRE ATT&CK-Techniken, 4. Quartal 2022

Entschleierung/Dekodierung von Dateien oder Informationen
JavaScript
Verschleierte Dateien oder Informationen
PowerShell
Process Hollowing
Reflective Code Loading
Schlüssel zur Registrierungsausführung/Systemstartordner
Rundll32
Geplanter Task

SCHWACHSTELLENINFORMATIONEN: 4. QUARTAL 2022

Unser Schwachstellen-Dashboard gibt einen Überblick über die Analysen der neuesten schwerwiegenden Schwachstellen. Die Analyse und die Triage werden von Schwachstellenexperten des Trellix Advanced Research Center durchgeführt. Diese Forscher, die sich auf Reverse Engineering und Schwachstellenanalyse spezialisiert haben, beobachten kontinuierlich die neuesten Schwachstellen und wie diese von Bedrohungsakteuren in Angriffen genutzt werden. Daraus leiten sie Behebungsempfehlungen ab und geben kompakte und äußerst technische Expertenhinweise, die Ihnen helfen, das Wichtige vom Unwichtigen zu trennen, sodass Sie sich auf die für Ihr Unternehmen schwerwiegendsten Schwachstellen konzentrieren und schneller reagieren können.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

WICHTIGE FAKTEN ZU SCHWACHSTELLENINFORMATIONEN, 4. QUARTAL 2022

41 % Auf Lanner entfielen 41 % der anfälligen Produkte und Anbieter, die im 4. Quartal 2022 von CVEs betroffen waren.

29 % Die Firmware von IAC-AST2500A in der Version 1.10.0 enthielt die meisten im 4. Quartal 2022 gemeldeten CVEs aller Produkte.

SCHWERWIEGENDSTE ANFÄLLIGE PRODUKTE, ANBIETER UND CVES, 4. QUARTAL 2022

1.	Lanner	41 %
2.	Microsoft	19 %
3.	BOA	15 %
4.	Oracle	8 %
5.	Apple Chrome Citrix Fortinet Linux	je 5 %

GEMELDETE CVES NACH PRODUKTEN, 4. QUARTAL 2022

29 %

Die Firmware von IAC-AST2500A Version 1.10.0 enthielt die meisten im 4. Quartal 2022 gemeldeten CVEs aller Produkte, gefolgt von BOA-Server (10 %), IAC-AST2500A (6 %) und Exchange (6 %).

Gemeldete CVEs in Produkten	Eindeutige CVEs
IAC-AST2500A, Firmware-Version 1.10.0	9
BOA-Server	3
Exchange	3
IAC-AST2500A	2
tvOS	1
iPadOS	1
iOS	1
Windows	1
Safari	1
SQLite bis einschließlich 3.40.0	1
Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	1
MacOS	1
Linux-Kernel vor 5.15.61	1
Internet Explorer	1

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

Gemeldete CVEs in Produkten	Eindeutige CVEs
FortiOS (sslvpnd)	1
Citrix ADC/Citrix Gateway	1
Chrome, Versionen vor 108.0.5359.94/.95	1
BOA-Server, Boa 0.94.13	1

GEMELDETE CVES, 4. QUARTAL 2022

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

Die Statistiken zur E-Mail-Sicherheit basieren auf Telemetriedaten, die aus verschiedenen bei Kunden in aller Welt installierten E-Mail-Sicherheits-Appliances generiert wurden. Die Zusammenfassung und Analyse der Erkennungsprotokolle führt zu folgenden Ergebnissen:

WICHTIGE FAKTEN ZU TRENDS IN DER E-MAIL-SICHERHEIT, 4. QUARTAL 2022

100 % Das Volumen schädlicher E-Mails ist in arabischen Ländern im Oktober im Vergleich zu August und September um 100 % gestiegen.

40 % Die am meisten genutzte Malware-Familie war Qakbot, die bei 40 % der Kampagnen gegen arabische Länder eingesetzt wurde.

42 % Die Telekommunikationsbranche war im 4. Quartal 2022 am stärksten von schädlichen E-Mails betroffen. Auf sie entfielen 42 % der schädlichen E-Mail-Kampagnen gegen Unternehmen.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

87 % Phishing-E-Mails mit schädlichen URLs wurden im 4. Quartal 2022 mit Abstand am häufigsten als Angriffsvektor eingesetzt.

64 % Vom 3. zum 4. Quartal 2022 nahmen Nachahmungsversuche um 64 % zu.

82 % Insgesamt wurden 82 % aller CEO-Betrugs-E-Mails über kostenlose E-Mail-Dienste verschickt.

78 % Bei 78 % aller BEC-Angriffe (Business Email Compromise) wurden gängige CEO-Formulierungen verwendet.

142 % Vishing-Angriffe spielten im 4. Quartal 2022 eine große Rolle und nahmen gegenüber dem 3. Quartal um 142 % zu.

AM HÄUFIGSTEN IN E-MAILS GENUTZTE MALWARE-TAKTIKEN, 4. QUARTAL 2022

40 %

Qakbot war im 4. Quartal 2022 die am häufigsten genutzte Malware-Taktik für E-Mails.

1.	Qakbot	40 %
2.	Emotet	26 %
3.	Formbook	26 %
4.	Remcos	4 %
5.	QuadAgent	4 %

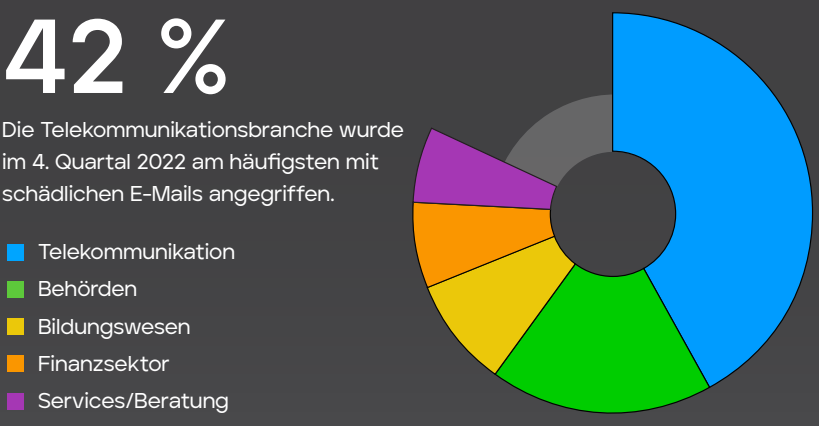
AM HÄUFIGSTEN MIT PHISHING-E-MAILS ANGEGRIFFENE PRODUKTE UND MARKEN, 4. QUARTAL 2022

1.	Generisch	62 %
2.	Outlook	13 %
3.	Microsoft	11 %
4.	Ekinet	8 %
5.	Cloudfare	3 %

AM HÄUFIGSTEN VON BÖSWILLIGEN E-MAILS BETROFFENE BRANCHEN, 4. QUARTAL 2022

42 %

Die Telekommunikationsbranche wurde im 4. Quartal 2022 am häufigsten mit schädlichen E-Mails angegriffen.



ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

WICHTIGE FAKTEN ZU TRENDS BEI NACHAHMUNGS-E-MAILS, 4. QUARTAL 2022

82 % Insgesamt wurden 82 % aller CEO-Betrugs-E-Mails über kostenlose E-Mail-Dienste verschickt.

78 % Bei 78 % aller BEC-Angriffe (Business Email Compromise) wurden gängige CEO-Formulierungen verwendet.

64 % Die Zahl der schädlichen E-Mails, die CEOs oder andere Führungskräfte nachahmten, ist im 4. Quartal gegenüber dem 3. Quartal 2022 um 64 % gestiegen.

Gängige CEO-Formulierungen bei BEC-Angriffen im 4. Quartal 2022:

„Sie müssen sofort etwas für mich erledigen."

„Sie müssen etwas für mich erledigen. Schicken Sie mir bitte Ihre Handynummer."

„Schicken Sie mir Ihre Telefonnummer. Sie müssen sofort etwas für mich erledigen."

„Schicken Sie mir bitte Ihre Handynummer und achten Sie auf meine Nachricht. Sie müssen etwas für mich erledigen."

„Bitte überprüfen und bestätigen Sie Ihre Handynummer und achten Sie auf meine Nachricht mit weiteren Anweisungen."

„Haben Sie meine vorherige E-Mail erhalten? Ich habe ein profitables Angebot für Sie."

VERGLEICH VON NACHAHMUNGSVERSUCHEN, 4. QUARTAL 2022

64 % Vom 3. zum 4. Quartal 2022 nahmen Nachahmungsversuche um 64 % zu.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

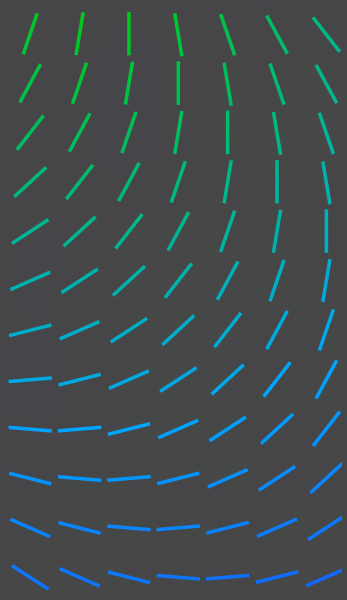
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



ERKENNTNISSE ZU PHISHING-KAMPAGNEN, 4. QUARTAL 2022

Web-Hosting-Anbieter zunehmend für Betrug und Diebstahl genutzt

Im 4. Quartal haben wir beobachtet, dass zunehmend legitime Web-Hosting-Anbieter für Betrugsversuche und zum Diebstahl von Anmeldeinformationen genutzt werden. Drei Dienstanbieter wurden dabei am häufigsten missbraucht: dweb.link, ipfs.link und translate.google. Zudem fiel uns ein hohes Volumen bei anderen Dienstanbieter-Domänen auf, einschließlich ekinet, storageapi_fleek und selcdn.ru. Die Angreifer nutzen immer wieder neue und beliebte Hosting-Dienste, um darauf Phishing-Seiten zu hosten und um Phishing-Schutzmaßnahmen zu umgehen. Angreifer greifen unter anderem deshalb vermehrt auf legitime Web-Hosting-Anbieter zurück, weil auf diesen Diensten hauptsächlich normale Dateien und Inhalte gehostet werden, sodass sie von Erkennungssystemen nicht blockiert werden können.

BEI PHISHING-E-MAILS AM HÄUFIGSTEN GENUTZTE ANGRIFFSVEKTOREN

87 %

Phishing-E-Mails mit schädlichen URLs wurden im 4. Quartal 2022 mit Abstand am häufigsten als Angriffsvektor verwendet.

1.	URL	87 %
2.	Anhang	7 %
3.	Header	6 %

STARK MISSBRAUCHTE WEB-HOSTING-ANBIETER, 4. QUARTAL 2022

154 %

Während Dweb der am häufigsten missbrauchte Web-Hosting-Anbieter im 4. Quartal 2022 war, zeigte Google Übersetzer die größte Zunahme (154 %) gegenüber dem 3. Quartal 2022.

1.	Dweb	81 %
2.	Ipfs	17 %
3.	Google Übersetzer	10 %

BEI PHISHING-ANGRIFFEN AM HÄUFIGSTEN GENUTZTE UMGEHUNGSTECHNIKEN, 4. QUARTAL 2022

63 %

Umgehungen mit 302-Weiterleitungen wurden im 4. Quartal 2022 am häufigsten eingesetzt.

- Phishing-Angriffe mit standortbasierter Umgehung nahmen im 4. Quartal deutlich zu.
- Captcha-basierte Angriffe nahmen im 4. Quartal ebenfalls zu.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

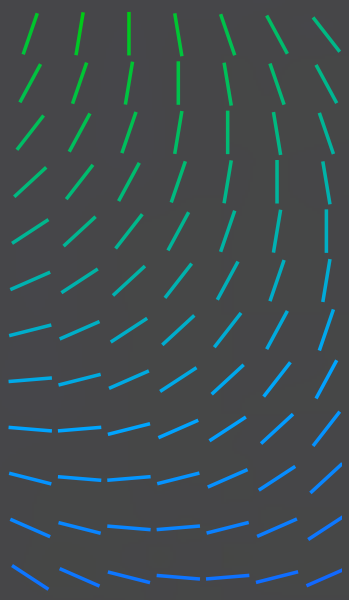
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



ERKENNTNISSE ZU VISHING, 4. QUARTAL 2022

Vishing ist eine weitere Form des Phishing, bei dem die Opfer dazu gebracht werden sollen, mit den Angreifern zu kommunizieren – in diesem Fall hauptsächlich über E-Mail, Textnachrichten, Telefon oder direkte Chat-Nachrichten.

142 % Vishing-Angriffe spielten im 4. Quartal 2022 eine große Rolle und nahmen gegenüber dem 3. Quartal um 142 % zu.

85 % Kostenlose E-Mail-Dienste sind bei Kriminellen, die Vishing betreiben, sehr beliebt geworden. Ein Großteil (85 %) der von uns im 4. Quartal 2022 erkannten Vishing-Angriffe wurden über einen kostenlosen E-Mail-Dienst verschickt.

Norton, McAfee, Geek Squad, Amazon und PayPal wurden im 4. Quartal am häufigsten für Vishing-Kampagnen missbraucht.

NETZWERKSICHERHEIT: 4. QUARTAL 2022

Das Trellix ARC-Team konzentriert sich auf die Erkennung und Blockierung netzwerkbasierter Angriffe, die unsere Kunden bedrohen. Wir sehen uns verschiedene Bereiche der Angriffskette an: Erkundung, Erstkompromittierung, C&C-Kommunikation sowie TTPs für laterale Bewegungen. Wir sind in der Lage, die Stärken der kombinierten Technologien so zu nutzen, dass wir unbekannte Bedrohungen besser erkennen können.

Bei Angriffen auf Netzwerksicherheit am häufigsten genutzte MITRE-ATT&CK-Techniken, 4. Quartal 2022

- T1083 – Erkennung von Dateien und Verzeichnissen
- T1573 – Verschlüsselter Kanal
- T1020 – Automatisierte Exfiltration
- T1210 – Ausnutzung von Remote-Diensten
- T1569 – Systemdienste
- T1059 – Befehls- und Skript-Interpreter: Windows Command Shell
- T1047 – Windows-Verwaltungsinstrumentation
- T1087 – Kontoerkennung
- T1059 – Befehls- und Skript-Interpreter
- T1190 – Ausnutzung von öffentlicher Anwendung

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

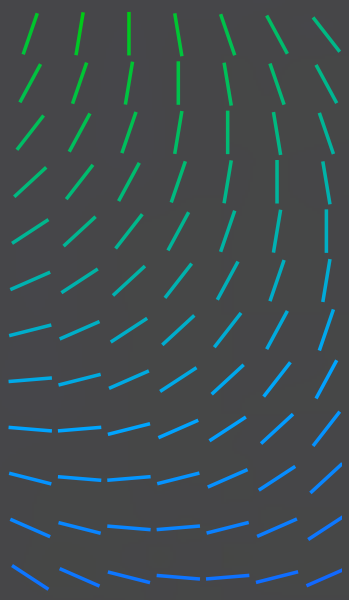
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



Schwerwiegendste Angriffe auf öffentlich zugängliche Dienste, 4. Quartal 2022

Täglich werden viele Netzwerk-Scans ausgeführt, um öffentlich zugängliche Rechner auf potenzielle Einfallstore in Kundenumgebungen zu prüfen. Alte Exploits suchen kontinuierlich nach ungepatchten Systemen.

- Zugriffsversuch auf Datei /etc/passwd erkannt
- Möglicher XSS-Angriff (webseitenübergreifende Skripterstellung)
- Sicherheitsscanner SIPVicious
- Datenverkehr von Nmap-Scanner erkannt
- Scan-Aktivitäten – Shellshock, Web-Server-Tests
- Remote-Ausführung von Bash-Code (Shellshock) HTTP CGI (CVE-2014-6278)
- Schwachstelle in Oracle WebLogic, die Remote-Ausführung von Code ermöglicht (CVE-2020-14882)
- Directory Traversal-Versuch (Verzeichnisdurchquerung)
- Apache Struts 2 ConversionErrorInterceptor OGNL-Skript-Injektion
- Remote-Ausführung von Code: Apache Log4j (CVE-2021-44228)

Häufig genutzte WebShells für Erstzugriff auf Netzwerke, 4. Quartal 2022

Folgende WebShells werden häufig genutzt, um die Kontrolle über anfällige Web-Server zu erlangen.

- Webshell China Chopper
- Webshell JFolder
- Webshell ASPXSpy
- Webshell C99
- Webshell Tux
- Webshell B374K/RootShell-Familie

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

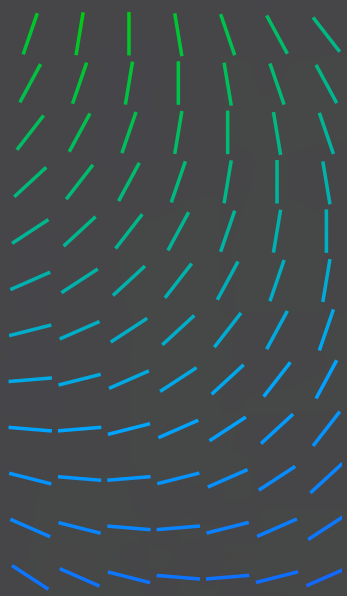
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



Relevanteste Tools, Techniken und Prozeduren für Aktivitäten innerhalb des Netzwerks, 4. Quartal 2022

Folgende WebShells werden häufig genutzt, um die Kontrolle über anfällige Web-Server zu erlangen.

Wir haben beobachtet, dass die Angreifer sehr viele TTPs während lateraler Bewegungen verwenden, zum Beispiel die Ausnutzung alter Schwachstellen und Tools wie SCShell und PSExec.

- SCshell: Dateilose laterale Bewegungen mithilfe des Dienst-Managers
- Aufruf eines Windows WMI-Remoteprozesses
- Aufruf der CMD-Shell über WMIEXEC per SMB
- EternalBlue-Exploit erkannt
- Versuch der CVE-2020-0796-Ausnutzung in Microsoft SMBv3
- Remote-Ausführung von Code: Apache Log4j (CVE-2021-44228)
- Auflistung von Remote-Domänen/Unternehmens-Administratorkonten
- Verdächtige Remote-Ausführung von PowerShell
- Verdächtige Netzwerkerkundung durch WMIC
- Auflistungsbefehl in Batch-Datei erkannt
- SMB PSEXEC-Aktivitäten

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

Diese Statistiken basieren auf Telemetriedaten, die aus verschiedenen Sensoren unserer Kunden generiert wurden. Die Zusammenfassung und Analyse der Erkennungsprotokolle führt zu folgenden Kategorien:

Schwerwiegendste Sicherheitszwischenfälle, 4. Quartal 2022

Dies ist eine Liste der häufigsten Sicherheitswarnungen für das 4. Quartal 2022:

EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [ungewöhnliche Anmeldung]

OFFICE 365 [hat Phishing erlaubt]

EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [versuchte Ausnutzung von CVE-2021-41773]

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN

WINDOWS ANALYTICS [Brute-Force-Erfolg]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [versuchte Ausnutzung von CVE-2022-1388]

AM HÄUFIGSTEN GENUTZTE MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1.	Ausnutzung von öffentlicher Anwendung (T1190)	29 %
2.	Protokoll für Anwendungsebene: DNS (T1071.004)	14 %
	Phishing (T1566)	14 %
3.	Kontenmanipulation (T1098.001)	
	Brute-Force (T1110)	
	Drive-by-Kompromittierung (T1189)	
	Ausführung durch Benutzer: Schädliche Datei (T1204.002)	
	Gültige Konten: Lokale Konten (T1078.003)	je 7 %

VERTEILUNG WICHTIGER PROTOKOLLQUELLEN, 4. QUARTAL 2022

1.	Netzwerk	40 %
2.	E-Mail	27 %
3.	Endgerät	27 %
4.	Firewall	6 %

BEOBACHTETE EXPLOITS, 4. QUARTAL 2022

AM HÄUFIGSTEN GENUTZTE EXPLOITS NACH BEOBACHTUNGEN IM 4. QUARTAL 2022

30 % Log4j war den Beobachtungen zufolge das im 4. Quartal 2022 am häufigsten genutzte Exploit.

1.	Log4j (CVE-2021-44228)	30 %
2.	Fortinet (CVE-2022-40684)	16 %
3.	Apache Server (CVE-2021-41773)	15 %
4.	Atlassian Confluence (CVE-2022-26134)	14 %
5.	F5 Big-IP (versuchte Ausnutzung von CVE-2022-1388)	13 %
6.	Microsoft Exchange (ProxyShell-Exploit-Versuch)	11 %

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

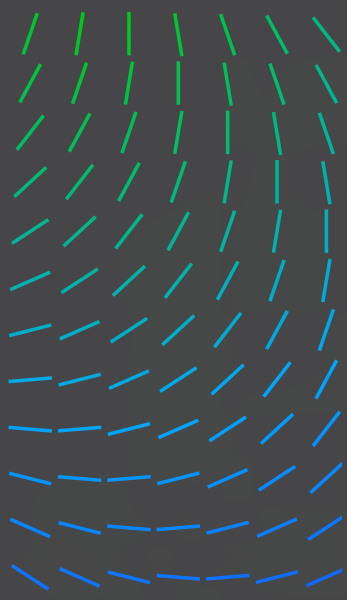
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



CLOUD-ZWISCHENFÄLLE, 4. QUARTAL 2022

Angriffe auf Cloud-Infrastrukturen nehmen kontinuierlich zu, da viele Unternehmen ihre Systeme umstellen. Die Analysten von Gartner gehen davon aus, dass bis zum Jahr 2025 ganze 85 % der Unternehmen auf die Cloud umsteigen werden.

Bei der Analyse der Telemetriedaten des 4. Quartals 2022 haben wir Folgendes beobachtet:

- Erkennungen im Zusammenhang mit AWS treten am häufigsten auf, wahrscheinlich da AWS als führender Anbieter im Cloud-Markt gilt.
- Die meisten Angriffe zielten darauf ab, durch Brute-Force- bzw. Password-Spraying-Methoden Erstzugriff auf gültige Konten zu erlangen, was auf den ersten Angriffsvektor in der Cloud-Angriffsfläche hinweist.
- Da die meisten Unternehmenskonten mit MFA (Mehrfaktor-Authentifizierung) gesichert sind, führen erfolgreiche Brute-Force-Versuche die Angreifer auf MFA-Plattformen, wodurch es zu einem Anstieg an MFA-bezogenen Erkennungen kommt.

Die nachfolgenden Abschnitte bieten eine kurze Beschreibung der Cloud-basierten Telemetriedaten unseres Kundenstamms, aufgeschlüsselt nach den verschiedenen Cloud-Anbietern.

BEI AWS AM HÄUFIGSTEN GENUTZTE MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1.	Gültige Konten (T1078)	18 %
2.	Änderung der Datenverarbeitungsinfrastruktur des Cloud-Kontos (T1578)	12 %
3.	Kontenmanipulation (T1098)	9 %
4.	Cloud-Konten (T1078.004)	8 %
5.	Brute Force (T1110) Beeinträchtigung von Schutzmaßnahmen (T1562)	je 6 %

BEI AZURE AM HÄUFIGSTEN GENUTZTE MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1.	Gültige Konten (T1078)	23 %
2.	Mehrfaktor-Authentifizierung (T1111)	19 %
3.	Brute-Force (T1110)	14 %
4.	Proxy (T1090)	14 %
5.	Kontenmanipulation (T1098)	5 %

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

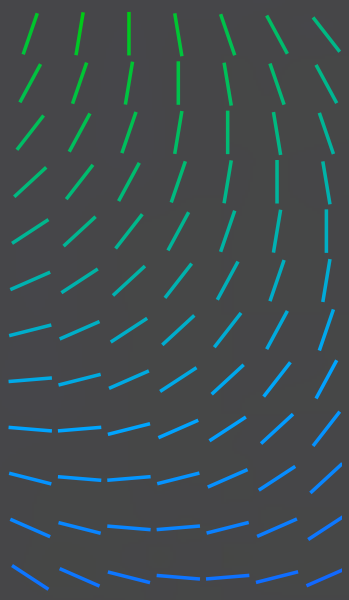
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



HÄUFIGSTE AWS-ERKENNUNGEN NACH MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

MITRE ATT&CK	Regel
Kontenmanipulation (T1098)	AWS – Privilegierte Richtlinie, die an IAM-Identität gebunden ist AWS S3 – Bucket-Richtlinie löschen
Gültige Konten (T1078)	AWS Analytics – ungewöhnliche Konsolenanmeldung AWS Analytics – ungewöhnliche Verwendung von API-Schlüssel AWS GuardDuty – ungewöhnliches Benutzerverhalten AWS GuardDuty – anonymer Zugriff gewährt
Beeinträchtigung von Schutzmaßnahmen (T1562)	AWS CloudTrail – Richtlinienänderungen in CloudTrail AWS CloudTrail – Trail löschen
Anmeldeinformationen in Dateien (T1552.001)	Warnung – möglicher Diebstahl von geheimen AWS-Schlüsseln
Änderung der Datenverarbeitungs-infrastruktur des Cloud-Kontos (T1578)	AWS CloudTrail – S3-Bucket löschen AWS CloudTrail – S3-Bucket-ACL ablegen AWS CloudTrail – Objekt-ACL ablegen

HÄUFIGSTE AZURE-ERKENNUNGEN NACH MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

MITRE ATT&CK-Technik	Regel
Gültige Konten (T1078)	Azure AD – Riskante Anmeldung Azure – Anmeldung von ungewöhnlichem Ort Azure – Anmeldung von Konto, das 60 Tage inaktiv war
Brute-Force (T1110)	Azure – Mehrere Authentifizierungsfehler Graph – Brute-Force-Angriff auf Azure-Portal Graph – verteilte Versuche, Kennwörter zu knacken
Mehrfaktor-Authentifizierung (T1111)	Azure – MFA wegen Betrugswarnung abgelehnt Azure – MFA wegen blockiertem Benutzer abgelehnt Azure – MFA wegen betrügerischem Code abgelehnt Azure – MFA wegen betrügerischer Anwendung abgelehnt

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

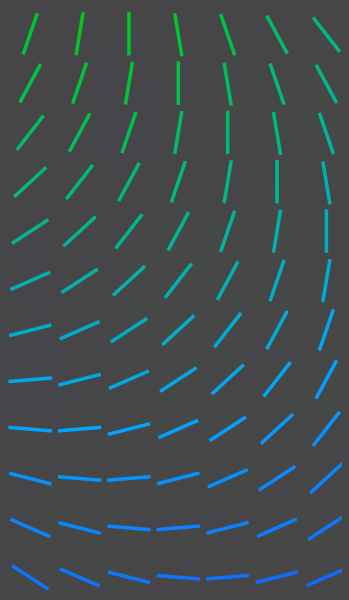
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



Externe Remote-Dienste (T1133)	Azure – Anmeldung von Tor-Netzwerk
Kontenmanipulation (T1098)	Azure – ungewöhnliche Rücksetzung des Benutzerkennworts

BEI GCP AM HÄUFIGSTEN GENUTZTE MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

1.	Gültige Konten (T1078)	36 %
2.	Ausführung über API (T0871)	18 %
3.	Kontoerkennung (T1087.001) Kontenmanipulation (T1098) Beeinträchtigung von Schutzmaßnahmen (T1562) Änderung der Datenverarbeitungsinfrastruktur des Cloud-Kontos (T1578) Remote-Dienste (T1021.004)	je 9 %

HÄUFIGE GCP-ERKENNUNGEN NACH MITRE ATT&CK-TECHNIKEN, 4. QUARTAL 2022

MITRE ATT&CK-Technik	Regel
Gültige Konten (T1078)	GCP – Erstellung eines Dienstkontos GCP Analytics – ungewöhnliche Aktivitäten GCP – Erstellung eines Dienstkonto-Schlüssels
Remote-Dienste (T1021.004)	GCP – Firewall-Regel erlaubt gesamten Datenverkehr über SSH-Port
Kontenmanipulation (T1098)	GCP – IAM-Richtlinie des Unternehmens geändert
Kontoerkennung (T1087.001)	Warnung [„gcps net user"]
Übertragung von Daten auf Cloud-Konto (T1527)	GCP – Logsenke verändert
Änderungen der Datenverarbeitungsinfrastruktur des Cloud-Kontos (T1578)	GCP – Löschschutz deaktiviert

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

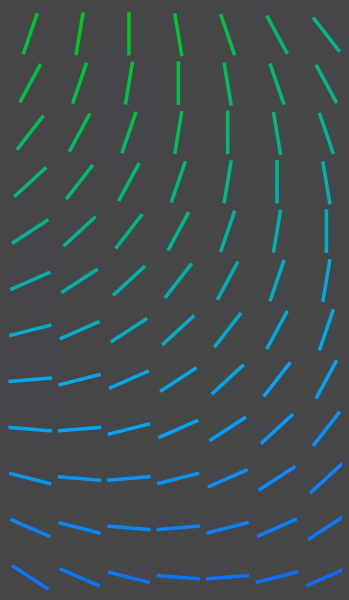
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



AUTOREN UND FORSCHER

Alfred Alvarado
Henry Bernabe
Adithya Chandra
Dr. Phuc Duy Pham
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

RESSOURCEN

Nutzen Sie die folgenden Ressourcen, um sich stets über die vom Trellix Advanced Research Center erkannten neuesten und gefährlichsten Bedrohungen zu informieren:

TWITTER

Trellix ARC

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

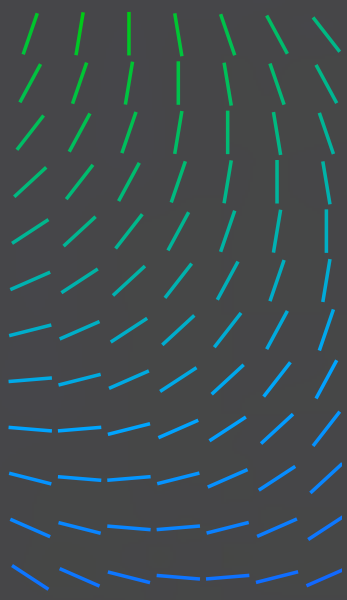
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



ÜBER DAS TRELLIX ADVANCED RESEARCH CENTER

Das Trellix Advanced Research Center hat die umfassendste Richtlinie der Cyber-Sicherheitsbranche und ist Vorreiter bei neuen Methoden, Trends und Akteuren der gesamten Bedrohungslandschaft. Als führender Partner von Sicherheitsteams in aller Welt liefert das Trellix Advanced Research Center Informationen und neueste Inhalte für Sicherheitsanalysten und stärkt gleichzeitig unsere führende XDR-Plattform.

ÜBER TRELLIX

Trellix ist ein globales Unternehmen, das die Zukunft der Cyber-Sicherheit und verantwortungsvolle Arbeit 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 förderte Trellix die technologische Innovationsfähigkeit durch Machine Learning und Automatisierung, um über 40.000 Geschäfts- und Behördenkunden durch Living Security zu stärken. Weitere Informationen unter www.trellix.com.

ÜBERBLICK ÜBER BEDROHUNGEN IM 4. QUARTAL 2022

BRIEF UNSERES HEAD OF THREAT INTELLIGENCE

METHODEN

RANSOMWARE: 4. QUARTAL 2022

STATISTIKEN ZU STAATLICHEN AKTEUREN: 4. QUARTAL 2022

LIVING OFF THE LAND (LOLBIN) UND DRITTANBIETER-TOOLS: 4. QUARTAL 2022

SCHWACHSTELLEN-INFORMATIONEN: 4. QUARTAL 2022

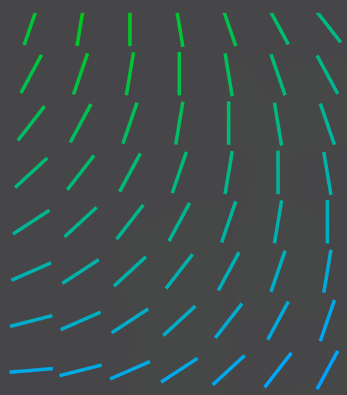
TRENDS IN DER E-MAIL-SICHERHEIT: 4. QUARTAL 2022

NETZWERKSICHERHEIT: 4. QUARTAL 2022

VON TRELLIX XDR ERFASSTE TELEMETRIEDATEN ÜBER SICHERHEITSABLÄUFE

AUTOREN UND FORSCHER

RESSOURCEN



Weitere Informationen finden Sie unter Trellix.com.

Trellix

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.

072022-05