BERICHT

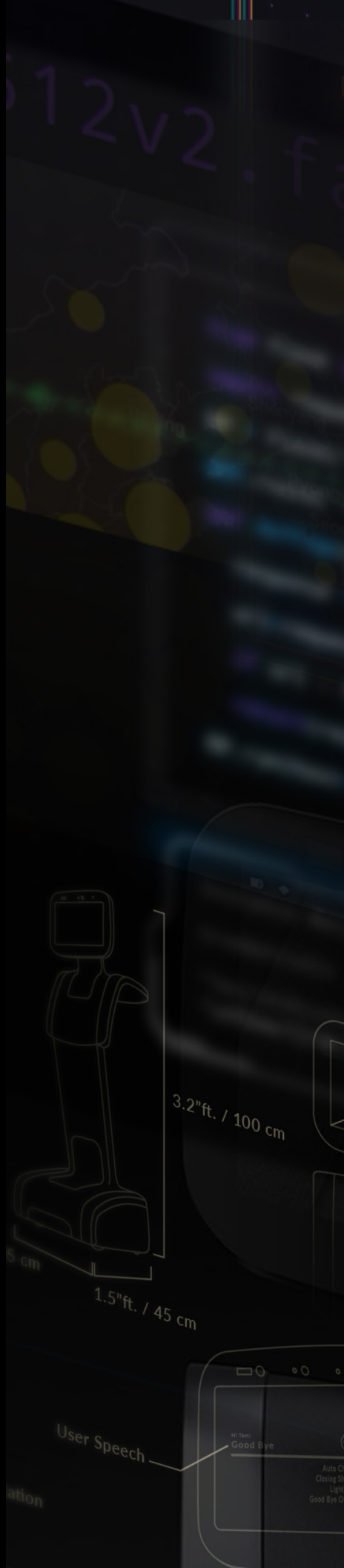
McAfee

# ADVANCED THREAT RESEARCH-REPORT

OKT. 2021

# INHALT





Wir konzentrieren uns ab sofort verstärkt auf die Verbreitungsmuster von Bedrohungen. Mit anderen Worten: Das Team achtet jetzt darauf, wie oft eine Bedrohung weltweit gefunden wird und – wichtiger noch – wen sie angreift.

## BRIEF UNSERES CHIEF SCIENTIST

Willkommen zu einem NEUEN Threats-Report und einem NEUEN Unternehmen.

Seit unserem letzten Threats-Report hat sich viel geändert. Wir haben erfahren, dass die Ransomware-Gruppe DarkSide trotz eines Namenswechsels immer noch aktiv und möglicherweise mit BlackMatter verbunden ist! Das ist aber noch nicht alles. Unsere jüngsten Erkenntnisse zu Infusionspumpen zeigen, wie wichtig Sicherheitsforschung ist (mehr dazu weiter unten in diesem Bericht).

Mein Team und ich haben den Wechsel zu McAfee Enterprise vollzogen, einem neu gegründeten Cyber-Sicherheitsunternehmen für Unternehmenskunden. Das bedeutet auch, dass wir unsere Arbeit nicht mehr als McAfee Labs veröffentlichen. Sie finden uns aber in unserem neuen Twitter-Feed McAfee Enterprise ATR: @McAfee_ATR.

Natürlich gehen die Veränderungen über einen einfachen Twitter-Feed hinaus, was sich in diesem Threats-Report teilweise widerspiegelt. Wir konzentrieren uns ab sofort verstärkt auf die Verbreitungsmuster von Bedrohungen. Mit anderen Worten: Das Team achtet jetzt darauf, wie oft eine Bedrohung weltweit gefunden wird und – wichtiger noch – wen sie angreift. Diese Erkenntnisse werden gestützt durch zusätzliche Analysen, die wir in diesem Bericht vorstellen. Sie umfassen aktive Forschung zu Bedrohungsakteuren sowie den von ihnen aktuell – und potenziell in Zukunft – ausgenutzten Schwachstellen.

Wir hoffen, dass Ihnen dieses neue Format gefällt, und freuen uns auf Ihre Rückmeldungen dazu, was Sie gut bzw. weniger gelungen fanden. Viel wichtiger aber noch: Was würden Sie sich hier für die Zukunft wünschen?

Bleiben Sie mit uns in Kontakt.

*– Raj Samani*

*McAfee Enterprise Chief Scientist und Fellow*

Twitter @Raj_Samani

## AUTOREN UND FORSCHER

Christiaan Beek
Ashley Dolezal
John Fokker
Melissa Gaffney
Tracy Holden
Tim Hux
Phillippe Laulheret
Douglas McKee
Lee Munson
Chris Palm
Tim Polzer
Steve Povolny
Raj Samani
Pankaj Solanki
Leandro Velasco

## RANSOMWARE

### ZUNEHMENDE VERBREITUNG VON RANSOMWARE

Als das Jahr 2021 ins dritte Quartal ging, setzten Cyber-Kriminelle neue und aktualisierte Bedrohungen in Kampagnen ein, die gegen prominente Sektoren gerichtet sind. Ransomware-Kampagnen sind ungebrochen aktiv, haben ihre Geschäftsmodelle jedoch weiterentwickelt, um von Unternehmen aller Größen wertvolle Daten zu extrahieren und Lösegelder in Millionenhöhe zu erpressen.

Im Mai beherrschte der öffentlichkeitswirksame Angriff von DarkSide auf den Treibstoffversorger Colonial Pipeline die Schlagzeilen. MVISION Insights konnte innerhalb kürzester Zeit die Hauptziele von DarkSide in den USA identifizieren, insbesondere Rechtsdienste, Großhändler und Fertigungsunternehmen sowie den Öl-, Gas- und Chemiesektor.

Die Stilllegung eines großen US-amerikanischen Treibstoffversorgers alarmierte Amtsträger ebenso wie Sicherheitskontrollzentren. Andere Ransomware-Gruppen, die mit ähnlichen Partnermodellen arbeiten, bereiten jedoch nicht weniger Sorgen. Die Ransomware-Familien Ryuk, REvil, Babuk und Cuba nutzten aktiv Geschäftsmodelle, die auf Partner setzen, um mithilfe typischer Eindringungsvektoren und vielfach der gleichen Tools Zugriff auf Unternehmensumgebungen zu erhalten und sich darin zu bewegen. Nicht lange nach dem DarkSide-Angriff machte die REvil-Gruppe mit einer Sodinokibi-Payload Schlagzeilen, die sie für den Angriff auf den weltweit aktiven IT-Infrastrukturanbieter Kaseya nutzten. Im 2. Quartal des Jahres 2021 führten REvil/Sodinokibi unsere Liste der Ransomware-Erkennungen an.

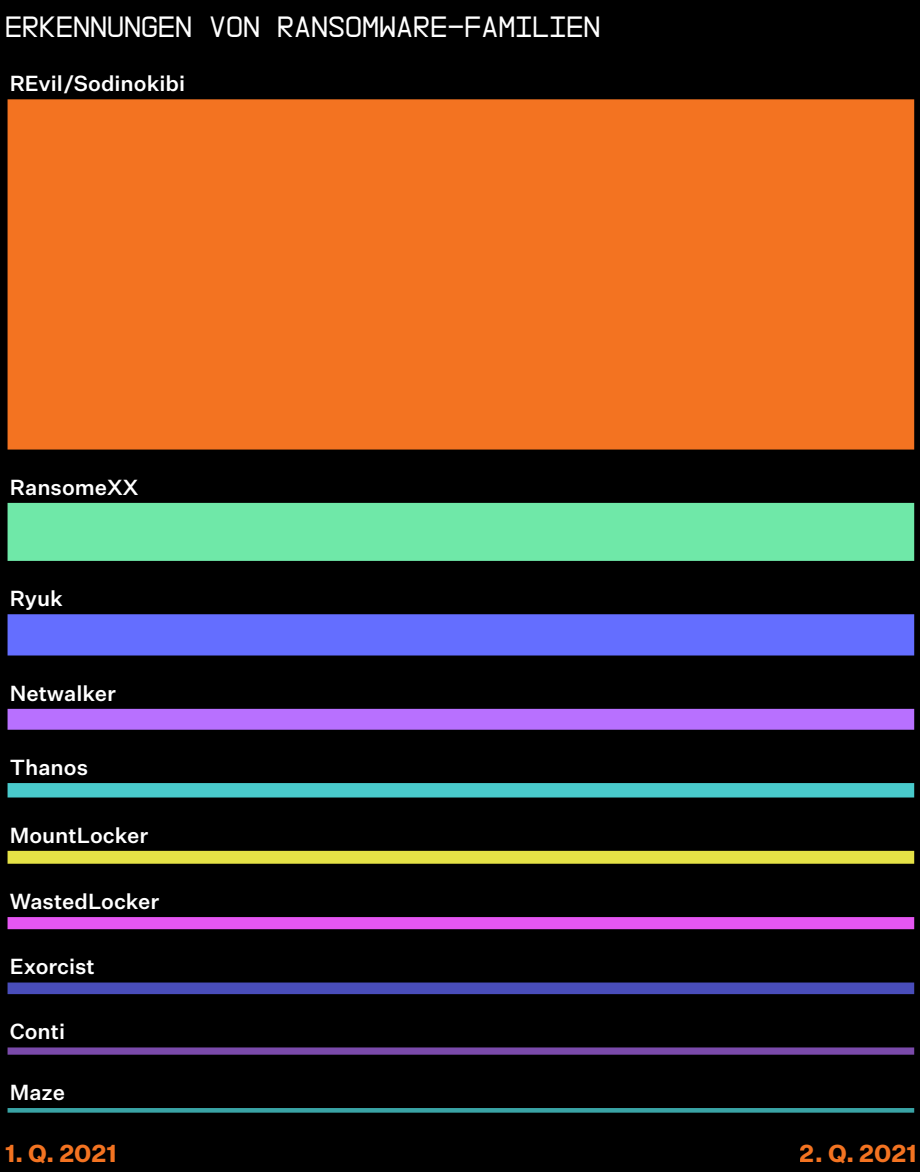



ABBILDUNG 1. REVIL/SODINOKIBI FÜHRTE MIT 73 % UNSERE LISTE DER 10 HÄUFIGSTEN RANSOMWARE-ERKENNUNGEN IM 2. QUARTAL 2021 AN.

Während DarkSide und REvil nach ihren schlagzeilenträchtigen Attacken von der Bildfläche verschwanden, rückte im Juli ein Nachfolger ins Rampenlicht. Die Ransomware BlackMatter trat in erster Linie in Italien, Indien, Luxemburg, Belgien, den USA, Brasilien, Thailand, Großbritannien, Finnland und Irland mit einem Ransomware-as-a-Service-Partnerprogramm auf, das Elemente von DarkSide, REvil sowie der Ransomware LockBit aufgriff. Durch den ähnlichen Code der Binärdatei sowie Übereinstimmungen bei der öffentlichen Website mit DarkSide wird allgemein davon ausgegangen, dass BlackMatter eine Fortsetzung der Ransomware DarkSide ist – was BlackMatter bestreitet.

Eine weitere „alte“ Ransomware mit neuem Dreh wurde Mitte 2021 entdeckt. Die Ransomware LockBit 2.0 ist eine aktualisierte Version von LockBit aus dem Jahr 2020 mit neuen Funktionen, die automatisch Geräte domänenübergreifend verschlüsselt, Daten exfiltriert und per RDP auf Systeme zugreift. Zudem kann LockBit 2.0 neue Partner innerhalb eines angegriffenen Unternehmens anwerben.

Ransomware-Entwickler starteten aber auch neue Kampagnen. Die Ransomware-Familie Hive wurde zum ersten Mal im Juni 2021 vorrangig in Indien, Belgien, Italien, den USA, der Türkei, Thailand, Mexiko, Deutschland, Kolumbien und der Ukraine gefunden. Das in der Programmiersprache Go geschriebene Hive wird als Ransomware-as-a-Service betrieben. Die Ransomware kompromittiert Gesundheitsdienstleister und Betreiber kritischer Infrastrukturen.

Unser Team nimmt Ransomware verstärkt in den Fokus und beleuchtet unter anderem eine unerwartete Reaktion in Untergrundforen und angegriffenen Sektoren sowie die Differenz zwischen Open-Source-Bedrohungsdaten und Telemetrie.

## ERFOLGREICHE RANSOMWARE AUS UNTERGRUNDFOREN VERBANNT

Im 2. Quartal 2021 erlebte Ransomware einen derartigen Höhenflug, dass sie ihren Eingang in die Cyber Agenda der US-Regierung fand. Doch auch in bislang sicheren Cybercrime-Untergrundforen gab es Veränderungen.

Die Auswirkungen von Ransomware-Angriffen wurden sehr deutlich, als Colonial Pipeline durch die DarkSide-Attacke stillgelegt wurde. Diese abrupte Blockade der Lieferkette betraf fast die gesamte Ostküste der USA und führte zu massenhaften Hamsterkäufen der Verbraucher bei Treibstoff. Der Angriff und seine Auswirkungen auf Bevölkerung und Wirtschaft zeigte die grausamen Folgen von Ransomware-Attacken und brachte die Sicherheitsbehörden auf den Plan.

Die politischen Auswirkungen des Colonial Pipeline-Angriffs führten dazu, dass die Ransomware-Gruppe DarkSide ihre Aktivitäten abrupt einstellte. Etliche weitere kriminelle Gruppen gaben bekannt, dass sie Ziele in Zukunft überprüfen und bestimmte Sektoren ausschließen würden.

Eine Woche später gaben mit XSS und Exploit zwei der einflussreichsten Untergrundforen einen Bann für Ransomware-Werbung bekannt. Jahrelang boten diese Foren eine sichere Anlaufstelle für Cyber-Kriminalität und den Ransomware-Boom, der zu einem lebhaften Handel unter anderem mit kompromittierten Netzwerken, Stealer-Protokollen und Crypter-Services führte. Da es sich bei vielen Bedrohungsakteuren hinter den großen Ransomware-Familien um Berufsverbrecher handelt, die häufig enge Beziehungen mit den Forumsadministratoren und Moderatoren pflegen, glauben wir, dass diese Geste das Weiterbestehen der Foren sichern sollte.

Doch obwohl die mit Ransomware verbundenen Online-Konten gebannt wurden, konnte unser Team beobachten, dass die Bedrohungsakteure immer noch in mehreren Foren mit anderen Pseudonymen aktiv sind.

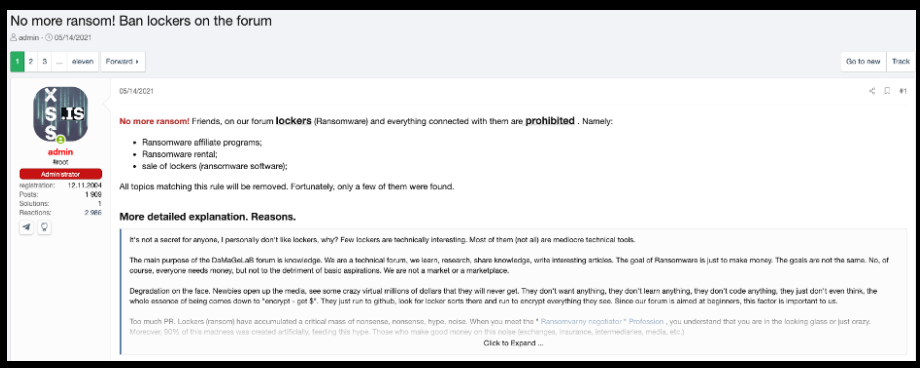



ABBILDUNG 2. NACHRICHT DES XSS-ADMINISTRATORS, DER DEN RANSOMWARE-BANN BEKANNT GIBT.

In diesem Zeitraum hatte die Ransomware-Gruppe Babuk ganz eigene Probleme. Eines davon, einen Fehler in *nix ESXi Locker, haben wir in unserem Blog ausführlich vorgestellt.

Letztendlich führten Streitigkeiten innerhalb des Babuk-Teams zur Trennung und dem Start eines neuen Forums für die Ransomware RAMP. Hier treffen sich viele Cyber-Kriminelle mit Ransomware-Bezug, um Geschäfte zu machen und TTPs auszutauschen. Trotz des Banns in einigen größeren Cybercrime-Foren gab es keine Anzeichen für einen Rückgang bei Ransomware. Damit bleibt diese Schadsoftware-Kategorie auch weiterhin eine der schwerwiegendsten Cyber-Bedrohungen für Unternehmen aller Größen.

## ZIELSEKTOREN FÜR RANSOMWARE: DIE DIFFERENZ BEI DER DATENQUALITÄT ZWISCHEN OPEN-SOURCE-BEDROHUNGSDATEN UND TELEMETRIE

Viele Ransomware-Gruppen nutzen Portale, in denen sie die kompromittierten Opfer bekannt geben und Auszüge aus den erbeuteten Daten zeigen. Damit wollen sie ihre Opfer unter Druck setzen, das Lösegeld zu bezahlen, da die Daten andernfalls geleakt und – in einigen Fällen – verkauft werden. Leak-Websites sind Demonstrationen fehlgeschlagener Verhandlungen und zeigen nicht das tatsächliche Ausmaß der Angriffe durch die Ransomware-Gruppen. Dennoch lassen sich Rückschlüsse zu den gemeldeten Branchen und Regionen ziehen.

Unser Team überwacht viele dieser Seiten und erfasst den Namen der Ransomware-Familie sowie Branche und Land des Opfers. Durch die Erfassung und Analyse dieser Daten konnten wir feststellen, welche 10 Sektoren in den USA am häufigsten angegriffen werden:

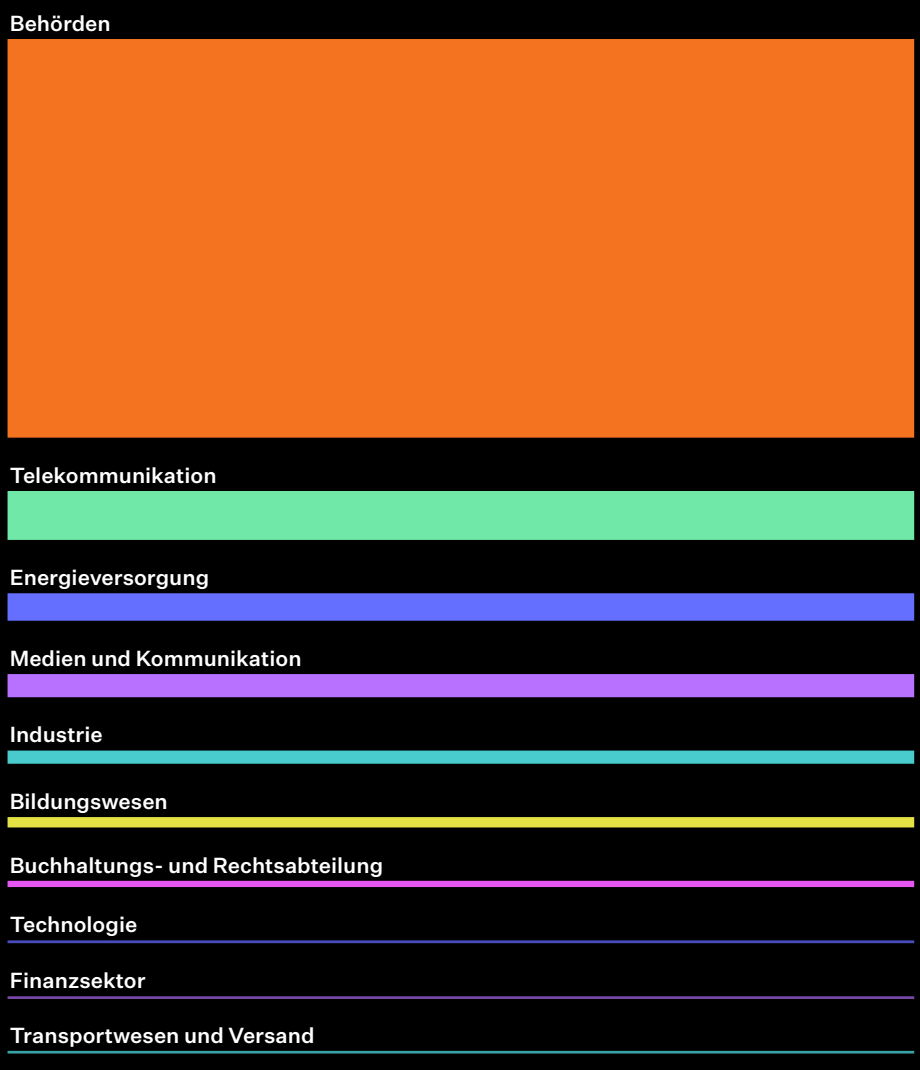



ABBILDUNG 3. DER BEHÖRDENSEKTOR WURDE IM 2. QUARTAL 2021 AM HÄUFIGSTEN ANGEGRIFFEN, GEFOLGT VON TELEKOMMUNIKATIONSUNTERNEHMEN, ENERGIEVERSORGERN SOWIE MEDIEN UND KOMMUNIKATION.

Unsere Telemetriedaten, die wir aus Sensoren in den USA erhalten, ordneten beobachtete Ransomware-Aktivitäten zu und verglichen sie mit den Sektoren, die in Open-Source-Bedrohungsdaten (OSINT) gemeldet wurden:

| Per Telemetrie gemeldete Sektoren | Per OSINT gemeldete Sektoren |
|---|---|
| Behörden | Fertigungsunternehmen |
| Finanzsektor | Einzelhandel |
| Bildungswesen | Gesundheitswesen |
| Telekommunikation | Bauwesen |
| Energieversorgung | Transportwesen |
| Medien | Bildungswesen |
| Industrie | Geschäftsdienstleistungen |
| Immobilienwesen | Rechtswesen |
| Rechtswesen | Finanzsektor |
| Technik | IT |

TABELLE 1. JE GRÖßER DIE DISTANZ ZWISCHEN DEN BEIDEN SEKTOREN, DESTO BESSER SIND SIE GESCHÜTZT. UMGEKEHRT GILT: JE NÄHER SIE LIEGEN, DESTO STÄRKER IST DER BETREFFENDE SEKTOR DURCH RANSOMWARE GEFÄHRDET.

Was bedeutet der Unterschied? Was macht die Differenz aus? Mit unseren Telemetriedaten beobachten wir Ransomware-Aktivitäten, die in Sektoren erkannt und blockiert wurden, in denen unsere Kunden tätig sind. Dass in den Telemetriedaten der Behördensektor als am häufigsten angegriffener Sektor identifiziert wird, zeigt, dass viele Angriffsversuche NICHT erfolgreich sind. In den OSINT-Daten beobachten wir, dass Sektoren, die für ihre kritischen Geschäftsprozesse stark von IT-Diensten abhängen, weit oben in der Zielpriorität der Ransomware-Betreiber stehen.

## VON RANSOMWARE-FAMILIEN GENUTZTE MITRE ATT&CK-MUSTER/TECHNIKEN: 2. QUARTAL 2021

### ANGRIFFSMUSTER/TECHNIK

1. Datenverschlüsselung für größere Auswirkung
2. Datei- und Verzeichniserkennung
3. Verschleierte Dateien oder Informationen
4. Prozessinjektion
5. Entschleierung/Dekodierung von Dateien oder Informationen
6. Prozesserkennung
7. Verhinderung der Systemwiederherstellung
8. PowerShell
9. Erkennung von Systeminformationen
10. Änderung der Registrierung

TABELLE 2. DATENVERSCHLÜSSELUNG FÜR GRÖßERE AUSWIRKUNG WAR IM 2. QUARTAL 2021 DAS AM HÄUFIGSTEN BEOBACHTETE ANGRIFFSMUSTER.

## B BRAUN: AUFDECKUNG VON SCHWACHSTELLEN IN WELTWEIT GENUTZTER INFUSIONSPUMPE

Die Medizinbranche steht vor ganz eigenen Sicherheitsherausforderungen. Potenzielle Angriffe auf medizinische Zentren könnten sich als noch größere Gefahr erweisen als eine systemweite Ransomware-Attacke. Unser Team hat gemeinsam mit Culinda eine Reihe von Schwachstellen in den Produkten B. Braun Infusomat Space Large Pump und B. Braun SpaceStation aufgedeckt.

Anhand der Forschungsergebnisse konnten wir diese fünf bislang unentdeckten Schwachstellen im medizinischen System identifizieren:

1. CVE-2021-33886: Nutzung von außen kontrollierter Formatzeichenfolgen (CVSS 7.7)
2. CVE-2021-33885: Unzureichende Überprüfung der Datenauthentizität (CVSS 9.7)
3. CVE-2021-33882: Fehlende Authentifizierung für kritische Funktion (CVSS 8.2)
4. CVE-2021-33883: Klartextübertragung vertraulicher Informationen (CVSS 7.1)
5. CVE-2021-33884: Uneingeschränkter Upload von Dateien mit gefährlichem Typ (CVSS 5.8)

Ein böswilliger Akteur könnte mithilfe dieser Schwachstellen die Konfiguration einer Pumpe manipulieren, während sich die Pumpe im Standby-Modus befindet. Das kann dazu führen, dass dem Patienten beim nächsten Einsatz eine falsche Medikamentendosis verabreicht wird – schließlich findet keinerlei Authentifizierung statt.

Kurz nachdem unser Team die ersten Erkenntnisse an B. Braun meldete, reagierte das Unternehmen und arbeitete mit uns zusammen, um die in unserem Bericht vorgeschlagenen Behebungsmaßnahmen zu implementieren.

Diese Erkenntnisse stellen einen Überblick sowie einige technische Details der gefährlichsten Angriffskette dar und gehen auf die besonderen Herausforderungen der Medizinbranche ein. Eine kurze Zusammenfassung finden Sie in unserem Blog.

## CLOUD-BEDROHUNGEN

### HÄUFIGKEIT VON CLOUD-BEDROHUNGEN

Aufgrund der Pandemie waren Veränderungen bei der Cloud-Sicherheit notwendig, um den flexibleren Arbeitsplätzen der Belegschaft Rechnung zu tragen. Gleichzeitig blieb die Arbeitsbelastung gleich oder nahm sogar noch zu, sodass Cyber-Kriminellen im 2. Quartal 2021 noch mehr potenzielle Exploits und Ziele geboten wurden.

Die Cloud-Bedrohungsforschung unseres Teams zeigte, dass Finanzdienstleister im 2. Quartal 2021 am stärksten durch Cloud-Bedrohungskampagnen gefährdet waren.

### HÄUFIGSTE CLOUD-BEDROHUNGEN: 2. QUARTAL 2021

1. Übermäßige Nutzung an ungewöhnlichen Standorten
2. Datenexfiltration durch Insider
3. Missbrauch von Zugriffsberechtigungen
4. Hohes Risiko von Datenexfiltrationen
5. Exfiltration von Zugriffsberechtigungen
6. „Landen-Erweitern-Exfiltrieren"-Strategie
7. Verdächtiger Superheld
8. Datenexfiltration durch privilegierten Benutzer

TABELLE 3. DEFINITION FÜR **ÜBERMÄßIGE NUTZUNG AN UNGEWÖHNLICHEN STANDORTEN**: DER BENUTZER HAT INNERHALB KURZER ZEIT SEHR GROßE DATENMENGEN ABGERUFEN ODER HERUNTERGELADEN. DAS IST EIN PROBLEM, WEIL 1.) UNTERNEHMENSKUNDEN ZUVOR NIE SO GROßE DATENVOLUMEN ABGERUFEN HABEN UND 2.) DAS DATENVOLUMEN SELBST IM VERGLEICH ZU EINEM GROßEN BENUTZERPOOL SEHR GROß IST. BEDROHUNGEN MIT **ÜBERMÄßIGER NUTZUNG AN UNGEWÖHNLICHEN STANDORTEN** STELLTEN DIE GRÖßTE DER WELTWEITEN CLOUD-BEDROHUNGEN DAR, GEFOLGT VON **DATENEXFILTRATION DURCH INSIDER** UND **MISSBRAUCH VON ZUGRIFFSBERECHTIGUNGEN**. IN DIE KATEGORIE **ÜBERMÄßIGE NUTZUNG AN UNGEWÖHNLICHEN STANDORTEN** FIELEN 62 % DER ERFASSTEN BEDROHUNGEN.

### WELTWEIT ANGEGRIFFENE CLOUD-BRANCHEN: 2. QUARTAL 2021

#### GROßE UNTERNEHMEN

1. Finanzdienstleistungen
2. Gesundheitswesen
3. Fertigungsunternehmen
4. Einzelhandel
5. Professional Services
6. Reisen und Gastgewerbe
7. Software und Internet
8. Technologie
9. Computer und Elektronik
10. Gemeinnützige Unternehmen

TABELLE 4. **AM HÄUFIGSTEN DURCH CLOUD-BEDROHUNGEN ANGEGRIFFEN WURDEN FINANZDIENSTLEISTER**, GEFOLGT VOM **GESUNDHEITSWESEN**, **FERTIGUNGSUNTERNEHMEN**, **EINZELHANDEL** UND **PROFESSIONAL SERVICES**. CLOUD-ATTACKEN AUF **FINANZDIENSTLEISTER** MACHTEN 33 % DER 10 AM HÄUFIGSTEN ANGEGRIFFENEN BRANCHEN AUS, GEFOLGT VOM **GESUNDHEITSWESEN** UND **FERTIGUNGSUNTERNEHMEN** (8 %).

## GESAMTZAHL DER CLOUD-ZWISCHENFÄLLE NACH BRANCHE WELTWEIT/USA: 2. QUARTAL 2021

| WELTWEITE CLOUD-BRANCHE | LAND |
|---|---|
| 1. Finanzdienstleistungen | USA |
| 2. Finanzdienstleistungen | Singapur |
| 3. Gesundheitswesen | USA |
| 4. Einzelhandel | USA |
| 5. Professional Services | USA |
| 6. Finanzdienstleistungen | China |
| 7. Fertigungsunternehmen | USA |
| 8. Finanzdienstleistungen | Frankreich |
| 9. Einzelhandel | Kanada |
| 10. Finanzdienstleistungen | Australien |

TABELLE 5. **FINANZDIENSTLEISTER** WURDEN WELTWEIT IN 50 % DER 10 GRÖßTEN CLOUD-ZWISCHENFÄLLE DES 2. QUARTALS 2021 IN DEN **USA**, **SINGAPUR**, **CHINA**, **FRANKREICH**, **KANADA** UND **AUSTRALIEN** ANGEGRIFFEN. CLOUD-ZWISCHENFÄLLE, BEI DENEN BRANCHEN IN DEN **USA** ANGEGRIFFEN WURDEN, MACHTEN 34 % DER ZWISCHENFÄLLE IN DEN TOP 10-LÄNDERN AUS.

### CLOUD-BRANCHEN IN DEN USA

1. Finanzdienstleistungen
2. Gesundheitswesen
3. Einzelhandel
4. Professional Services
5. Fertigungsunternehmen
6. Medien und Unterhaltung
7. Reisen und Gastgewerbe
8. Behörden
9. Software und Internet
10. Schulungs-Services

TABELLE 6. **FINANZDIENSTLEISTER** GEHÖRTEN IM 2. QUARTAL 2021 ZU DEN AM HÄUFIGSTEN MIT CLOUD-BEDROHUNGEN ANGEGRIFFENEN ZIELEN IN DEN USA. ZWISCHENFÄLLE BEI **FINANZDIENSTLEISTERN** MACHTEN 29 % DER GESAMTZAHL VON CLOUD-ZWISCHENFÄLLEN BEI DEN TOP 10-SEKTOREN AUS.

### GESAMTZAHL DER CLOUD-ZWISCHENFÄLLE NACH LAND: 2. QUARTAL 2021

| LAND |
|---|
| 1. USA |
| 2. Indien |
| 3. Australien |
| 4. Kanada |
| 5. Brasilien |
| 6. Japan |
| 7. Mexiko |
| 8. Großbritannien |
| 9. Singapur |
| 10. Deutschland |

TABELLE 7. DIE LÄNDER MIT DEN MEISTEN CLOUD-ZWISCHENFÄLLEN WAREN DIE USA, GEFOLGT VON INDIEN, AUSTRALIEN, KANADA UND BRASILIEN. CLOUD-ZWISCHENFÄLLE IN DEN USA MACHTEN 52 % DER ZWISCHENFÄLLE IN DEN TOP 10-LÄNDERN AUS.

## BEDROHUNGEN GEGEN LÄNDER, KONTINENTE, BRANCHEN UND EINGESETZTE VEKTOREN

### LÄNDER UND KONTINENTE: 2. QUARTAL 2021

Bei Ländern und Kontinenten wurden im 2. Quartal 2021 folgende erhebliche Zunahmen öffentlich gemeldeter Zwischenfälle verzeichnet:

- Die **USA** registrierten die meisten gemeldeten Zwischenfälle im 2. Quartal 2021.
- **Europa** verzeichnete im 2. Quartal mit 52 % den größten Anstieg gemeldeter Zwischenfälle.

### ANGEGRIFFENE BRANCHEN: 2. QUARTAL 2021

Bei den Branchen wurden im 2. Quartal 2021 folgende erhebliche Zunahmen öffentlich gemeldeter Zwischenfälle verzeichnet:

- Einige Branchen wurden besonders häufig angegriffen.
- Erhebliche Zunahmen verzeichneten der **öffentliche Sektor** (64 %) und die **Unterhaltungsbranche** (60 %).

### ANGRIFFSVEKTOREN: 2. QUARTAL 2021

Bei den Vektoren wurden im 2. Quartal 2021 folgende erhebliche Zunahmen öffentlich gemeldeter Zwischenfälle verzeichnet:

- **Malware** war im 2. Quartal 2021 die am häufigsten gemeldete Angriffstechnik.
- **Spam** verzeichnete zwischen dem 1. und 2. Quartal 2021 mit 250 % den höchsten Anstieg bei gemeldeten Zwischenfällen. Danach folgten **schädliche Skripts** mit 125 % und **Malware** mit 47 %.

## WICHTIGSTE MITRE ATT&CK-TECHNIKEN: 2. QUARTAL 2021

| Taktiken | Techniken (Top 5 je Taktik) | Kommentare |
|---|---|---|
| Erster Zugriff | Spearphishing-Anhang | Spearphishing (Links und Anhänge) teilt sich mit der Technik zur Ausnutzung von öffentlicher Anwendung die Top 3 bei Techniken für den Erstzugriff. |
| | Ausnutzung von öffentlicher Anwendung | |
| | Spearphishing-Link | |
| | Gültige Konten | |
| | Externe Remote-Dienste | |
| Ausführung | Windows-Befehlszeile | In diesem Quartal haben wir mehrere Angriffe beobachtet, bei denen die PowerShell oder die Windows-Befehlszeile genutzt wurden, um Malware im Arbeitsspeicher auszuführen oder Dual-Use- bzw. legitime Tools zu missbrauchen, um Zugriff auf Netzwerke zu erlangen. Penetrationstest-Frameworks wie Cobalt Strike nutzen häufig Befehlszeilenskripte, um die Benutzung zu erleichtern. |
| | PowerShell | |
| | Böswillige Datei | |
| | Windows-Verwaltungs-instrumentation | |
| | Gemeinsam genutzte Module | |
| Persistenz | Schlüssel zur Registrierungs-ausführung/ Systemstartordner | |
| | Geplanter Task | |
| | Windows-Dienst | |
| | Gültige Konten | |
| | DLL Side Loading | |
| Berechtigungs-eskalation | Schlüssel zur Registrierungs-ausführung/ Systemstartordner | |
| | Prozessinjektion | Prozessinjektion ist auch weiterhin eine der häufigsten Techniken für die Berechtigungseskalation. |
| | Geplanter Task | |
| | Windows-Dienst | |
| | Portable Executable-Injektion | |

| Taktiken | Techniken (Top 5 je Taktik) | Kommentare |
|---|---|---|
| Umgehung der Schutzmaßnahmen | Entschleierung/ Dekodierung von Dateien oder Informationen | |
| | Verschleierte Dateien oder Informationen | |
| | Änderung der Registrierung | |
| | Systemprüfungen | |
| | Dateilöschung | |
| Zugriff auf Anmeldedaten | Keylogger | Keylogging und Erfassung von Anmeldeinformationen aus Web-Browsern sind typische Funktionen der meisten Remote-Zugriff-Trojaner. |
| | Anmeldeinformationen aus Web-Browsern | |
| | Herunterladen von Betriebssystem-Anmeldeinformationen | Diese Technik ist eine Kernfunktion von Mimikatz, einem Erfassungstool für Anmeldeinformationen, das ATR in vielen analysierten Kampagnen aus dem 2. Quartal beobachtet hat. |
| | Eingabenerfassung | |
| | LSASS-Arbeitsspeicher | |
| Erkennung | Erkennung von Systeminformationen | |
| | Datei- und Verzeichniserkennung | |
| | Prozesserkennung | |
| | Systemprüfungen | |
| | Abfrage der Registrierung | |
| Bewegung innerhalb des Netzwerks | Remote Desktop Protocol | |
| | Ausnutzung von Remote-Diensten | |
| | Remote-Dateikopie | |
| | KMU/Windows-Administratorfreigaben | |
| | SSH | |
| Erfassung | Bildschirmaufzeichnung | Im 2. Quartal fanden mehrere Kampagnen statt, bei denen Remote-Administration-Trojaner (RATs) zum Einsatz kamen. Viele RAT-Malware-Varianten nutzten Techniken zur Bildschirmaufzeichnung. |
| | Keylogger | |
| | Daten vom lokalen System | |
| | Zwischenablagedaten | |
| | Gesammelte Archivdaten | |

| Taktiken | Techniken (Top 5 je Taktik) | Kommentare |
|---|---|---|
| Steuerung | Web-Protokolle | |
| | Eintrittstool-Transfer | |
| | Nicht-Standard-Port | |
| | Webdienst | |
| | Standardprotokoll für die Nicht-Anwendungsebene | |
| Exfiltration | Exfiltration über Steuerungskanal | |
| | Exfiltration über alternatives Protokoll | |
| | Exfiltration in Cloud-Speicher | Ransomware-Bedrohungsakteure exfiltrierten auch weiterhin Daten ihrer Opfer zu unterschiedlichen Cloud-Speicheranbietern. Erfolgt meist mit kommerziellen Tools wie RClone und MegaSync. |
| | Automatisierte Exfiltration | |
| | Exfiltration über unverschlüsseltes/ verschleiertes Nicht-C&C-Protokoll | |
| Wirkung | Datenverschlüsselung für mehr Auswirkung | Verschlüsselung von Daten für mehr Auswirkung ist eine weitere Technik, die von ATR bei mehreren Kampagnen und Bedrohungen beobachtet wurde. In diesem Quartal haben mehrere Ransomware-Familien einen Linux-basierten Locker eingesetzt, der ESXi-Server angreift, was diese Technik noch beliebter macht. |
| | Verhinderung der Systemwiederherstellung | Die Verhinderung der Systemwiederherstellung ist eine Technik, die häufig von Ransomware-Gruppen eingesetzt wird, bevor sie die finalen Schaddaten ausbringen. Durch das Löschen der Volumenschattenkopien erschweren sie den Opfern die Wiederherstellung nach dem Angriff. |
| | Kaperung von Ressourcen | |
| | Dienstbeendigung | |
| | Systemausfall/ Systemneustart | |

TABELLE 8. HINWEISE AUS DEN WICHTIGSTEN MITRE ATT&CK-TECHNIKEN VON KRIMINELLEN UND APT-GRUPPEN FÜR DAS 2. QUARTAL 2021.

## DIE WICHTIGSTEN REGELN ZUR ABWEHR DIESER BEDROHUNGEN

Im 2. Quartal 2021 erlebten und kommentierten wir viele unterschiedliche Bedrohungstypen. Wir bieten aber auch Empfehlungen sowie Produkte, mit denen Sie sich bzw. Ihr Unternehmen zuverlässig schützen können:

Informieren Sie sich darüber, wie das Konfigurieren von ENS 10.7, Manipulationsschutz und Rollback vor der Ransomware Cuba schützen, oder lesen Sie unseren detaillierten Blog, der sich an Sicherheitsverantwortliche richtet.

Frischen Sie Ihre Kenntnisse dazu auf, wie Sie lästige Pop-Up-Fenster in Ihrem Browser blockieren können und wie unsere Kunden dank McAfee WebAdvisor und McAfee Web Control vor schädlichen Websites geschützt sind.

Lesen Sie, wie Betrüger Windows Defender imitieren, um gefährliche Windows-Anwendungen zu verteilen, und welche unserer Sicherheitstipps dagegen helfen. Unsere Kunden können sich freuen, dass die Real Protect-Cloud Schutz durch Machine Learning bietet, während McAfee WebAdvisor und McAfee Web Control bekannt schädliche Websites blockieren.

Lernen Sie empfohlene Vorgehensweisen für die Absicherung und Überwachung Ihres Netzwerks kennen, damit DarkSide, die gefährlichste Ransomware dieses Quartals, keine Chance hat. Zudem bieten wir in diesem Blog eine Vielzahl an Informationen zu Abdeckung und Schutz durch EPP, MVISION Insights, MVISION EDR und McAfee ENS.

Und schließlich sollten Sie sich darüber informieren, warum virtuelle Maschinen so wertvoll für Cyber-Kriminelle sind und warum betroffene VMware-Benutzer sofort alle Patches einspielen sollten. Wer nicht sofort Patches installieren kann, erhält von uns praktische Tipps sowie eine Erinnerung daran, dass unsere Network Security Platform auch Signaturen der fraglichen CVEs bietet.

## RESSOURCEN

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

MVISION Insights-Vorschau-Dashboard: Sehen Sie sich eine Vorschau der einzigen proaktiven Lösung an, um neuen Bedrohungen einen Schritt voraus zu sein.

McAfee-Bedrohungszentrum: Die aktuell schwerwiegendsten Bedrohungen wurden von unserem Bedrohungsforscherteam erkannt.

### TWITTER

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Douglas McKee



Ohmstr. 1
85716 Unterschleißheim
+49 (0)89 3707-0
www.mcafee.com/de