VERHINDERN EINER RANSOMWARE-KATASTROPHE

Ransomware ist kein „normaler“ Cyberangriff, sondern kann sich rasend schnell über freigegebene Ordner verbreiten.

ZUSAMMENFASSUNG

Ransomware ist eine Gefahr für Unternehmen, die jedes Jahr Kosten in Millionenhöhe verursacht und leider immer ausgeklügelter wird. Glücklicherweise lassen sich mithilfe von Mozy und Spanning von EMC Endpunkte und Software as a Service-Anwendungsdaten mit einfach bereitzustellenden, effizienten und cloudbasierten Backuplösungen schützen.

Juni 2016

Wenn Sie mehr darüber erfahren möchten, wie Sie mithilfe von Endpunktdatensicherheit eine Ransomware-Katastrophe verhindern können, besuchen Sie Mozy. Für weitere Informationen über den Schutz Ihrer SaaS-Daten besuchen Sie Spanning.

Art.-Nr.: H15174

INHALTSVERZEICHNIS

EINLEITUNG

Ransomware ist eine Bedrohung, die Unternehmen jedes Jahr Kosten in Millionenhöhe beschert und leider immer ausgeklügelter wird. Mithilfe einer Vielzahl von Angriffen, einschließlich gezielter E-Mails und infizierter Websites, können Kriminelle Malware in Ihr Netzwerk einschleusen, die dann den Zugang zu Ihren Daten oder anderen Systemen verhindert, bis Sie ein Lösegeld bezahlen. Es ist sehr schwierig, jeden Ransomware-Angriff zu blockieren. Deshalb raten viele Experten, einschließlich des FBI, Unternehmen zu mehrstufigen Abwehrmaßnahmen in Verbindung mit geschützten Backups, um eine schnelle Recovery zu ermöglichen. Unternehmen, die diesen Rat befolgen, konzentrieren sich häufig auf wichtige interne Systeme und denken nicht an ihre Endpunkte – Desktops und Laptops – oder SaaS-Anwendungen, die Daten enthalten, deren Verfügbarkeit für Mitarbeiter von kritischer Bedeutung ist. Glücklicherweise können Sie mithilfe von Mozy und Spanning von EMC Ihre Daten mit einfach bereitzustellenden, effizienten und cloudbasierten Backuplösungen besser schützen.

DER AUFSTIEG VON RANSOMWARE

Die erste bekannte Ransomware war Trojan.Gpcoder. Sie wurde im Jahr 2005 entdeckt und infizierte Windows-Betriebssysteme. Mehr als 10 Jahre später bestehen keine Zweifel, dass Ransomware auf dem Vormarsch ist. In der Tat betrug der Zuwachs an neuer Ransomware im zweiten Quartal 2015 laut dem aktuellen Internet Security Threat Report von McAfee Labs satte 58 Prozent.[1] Es gibt keinen überzeugenden Grund zu der Annahme, dass die Bedrohung durch diese Art von Schadsoftware nicht weiterhin deutlich ansteigen wird. Der Grund ist einfach: „Ransomware ist sehr einfach zu entwickeln, einfach auszuführen und braucht nicht viel, um ihre Opfer davon zu überzeugen, für den Zugriff auf ihre wertvollen Dateien oder Systeme ein Lösegeld zu bezahlen.“[2]

In einer aktuellen Analyseübersicht berichtet Recorded Future von einem deutlichen Anstieg bei Ransomware-Infektionen in Europa im Vorjahresvergleich.[3] Obwohl Ransomware keine geografischen Grenzen kennt, sind die sechs am stärksten von dieser Art von Schadsoftware betroffenen Länder die Vereinigten Staaten von Amerika, Japan, Großbritannien, Italien, Deutschland und Russland.[4] Betrachten wir den folgenden Ransomware-Angriff aus diesem Jahr.

Cyberterroristen hatten das Computersystem eines großen US-Krankenhauses übernommen und alle Daten verschlüsselt, um den Zugriff darauf zu verhindern. Ursprünglich verlangten die Hacker ein Lösegeld von 3,6 Mio. USD gegen die Freigabe der Daten. Obwohl die Angreifer ihre Forderungen später auf 40 Bitcoins (ein Gegenwert von 17.000 USD) im Tausch gegen den Dechiffrierschlüssel reduzierten, hatten sie der ganzen Welt gegenüber klargestellt: Patientendaten und medizinische Datensätze sind vor Hackern nicht sicher. Denn wenn die Daten dieses Krankenhauses in Los Angeles als Geisel genommen werden konnten, warum nicht auch die von jedem anderen Unternehmen? Und das ist tatsächlich die Realität: Alle Arten von Unternehmen, einschließlich der Bereiche Medizin, Regierung, Bildung, Industrie usw., können das Ziel einer Erpressung mit Ransomware sein.

WAS IST RANSOMWARE UND WIE WIRD SIE VERBREITET?

Ransomware ist kein „normaler“ Cyberangriff. Sie kann sich sehr schnell über freigegebene Ordner verbreiten, die sich innerhalb und außerhalb des infizierten Unternehmens befinden. Ransomware sperrt entweder den Computer („Locker Ransomware“) oder verschlüsselt die Dateien des Benutzers („Crypto Ransomware“) und fordert diesen zur Zahlung eines Geldbetrags auf. Die Zahlung erfolgt dann in der Regel digital – zum Beispiel in Form von Bitcoin wie beim genannten Krankenhaus in Los Angeles – im Tausch gegen einen Dechiffrierschlüssel, der den Computer oder die Dateien entsperrt.

Ransomware erhält über das schwächste Glied im Netzwerk Zugriff auf ein Computersystem, in der Regel ist das die E-Mail oder ein soziales Netzwerk des Benutzers. Sobald ein Benutzer auf einen schädlichen Link klickt oder einen infizierten Anhang öffnet, verteilt sich die Malware im gesamten System. Einmal geöffnet kann die in gefälschten PDF-Dateien, nachgeahmten Lieferhinweisen von Kurierdiensten und betrügerischen angeblichen Anschreiben von Finanzinstitutionen verborgene Schadsoftware die Netzwerksicherheit eines Unternehmens schnell umgehen und sich über Netzwerklaufwerke und andere Endpunkte, die mit Sync- und Share-Tools wie Microsoft OneDrive, Google Drive und Dropbox verbunden sind, über das lokale System hinaus verbreiten.

Laut US-CERT (United States Computer Emergency Readiness Team) sind Cyberkriminelle, die Ransomware verwenden, so effektiv, weil sie bei ihren Opfern Angst und Panik auslösen, unter anderem dadurch, dass sie einschüchternde Meldungen anzeigen wie „Über Ihren Computer wurden Websites mit illegalen Inhalten besucht. Zum Entsperren Ihres Computers müssen Sie eine Strafe von 100

[1] McAfee Labs Threat Report, page 33, Intel Security Group, August 2015.
[2] Ransomware a Favorite of Cybercriminals, Matthew Rosenquist, McAfee Blog Central; September 1, 2015.
[3] Locking Up Europe With Ransomware: Origination, Targeting, and Payment, Recorded Future, Inc., 2016.
[4] The evolution of ransomware, Version 1, page 5; Kevin Savage, Peter Coogan, Hon Lau; Symantec; August 6, 2015.

USD bezahlen."[5] Ransomware ist aber auch aus anderen Gründen bei Cyberkriminellen so beliebt, nämlich aufgrund der Leichtigkeit, mit der sie erstellt und bereitgestellt werden kann.

Die Quintessenz von Ransomware ist einfach: Wer das Lösegeld nicht bezahlt, kann nicht mehr auf seinen Computer und die darauf gespeicherten Daten zugreifen. Und auch anderen Personen bleibt der Zugriff auf freigegebene Dokumente und Daten verwehrt, was die Auswirkungen exponentiell verschärft. Leider ist es so, dass auch zahlende Opfer nicht zuverlässig damit rechnen können, wieder Zugriff auf ihre Dateien zu erhalten. Die harte Realität ist, dass der Angreifer möglicherweise keine Dechiffrierschlüssel bereitstellt. In der Tat kam eine kürzlich durchgeführte Umfrage zu dem Schluss, dass nur 71 Prozent der Opfer von Ransomware, die das Lösegeld gezahlt hatten, wieder Zugriff auf ihre Dateien erlangten.[6]

RANSOMWARE IN DER REALITÄT

In der 2015 von ESET veröffentlichten Infosecurity Europe-Umfrage kam heraus, dass 84 Prozent der Befragten der Überzeugung waren, dass ihre Unternehmen durch eine Ransomware-Infektion ernsthaft beschädigt werden würden. Nahezu ein Drittel dieser Gruppe (31 Prozent) räumte ein, dass sie zur Zahlung an die Täter gezwungen sein würden, um ihre entschlüsselten Daten zurückzuerhalten.[7]

Unternehmen wissen, dass es sehr schwierig ist, sich vor jeder Bedrohung zu schützen, aber Ransomware stellt eine ganz besondere Herausforderung dar. Beispielsweise verwendet laut Autor und Experte für Spywareschutz Stu Sjouwerman „... die aktuell führende Ransomware CryptoWall eine sehr anspruchsvolle und sichere Verschlüsselung. Ohne ein Backup sind Sie verloren ...".[8]

Crypto Ransomware wie CryptoWall macht gemäß dem neuesten Internet Security Threat Report den Großteil aller Ransomware aus. „Nie zuvor in der Geschichte der Menschheit waren Menschen auf der ganzen Welt einem Erpressungsversuch in diesem enormen Umfang wie heute ausgesetzt."[9] Im Jahr 2015 wurden 362.000 verschiedene Arten von Crypto Ransomware gezählt (ein Plus von 35 Prozent gegenüber dem Vorjahr), im Durchschnitt 992 pro Tag.[10]

Obwohl Sie und Ihre Daten möglicherweise kein Opfer von CryptoWall werden, kommen jedes Jahr buchstäblich Millionen von neuen Malwarevarianten hinzu. 2015 waren es 431 Millionen neue Varianten, ein Anstieg von 36 Prozent gegenüber dem Vorjahr.[11] Eine wirksame Verteidigung gegen Ransomware erfordert nicht nur eine Bedrohungserkennung und -prävention, sondern auch eine Backup- und Recovery-Strategie. Werden diese Maßnahmen nicht ergriffen, kann das zu erheblichen Kosten führen. Beachten Sie, dass in kürzlich vorgenommenen Untersuchungen 36 Prozent der teilnehmenden öffentlichen und privaten Organisationen weltweit ungeplante Systemausfälle und/oder Datenverlust aufgrund einer externen oder internen Sicherheitsverletzung verzeichnen mussten. Die veranschlagten Durchschnittskosten der einzelnen Organisationen aufgrund von Systemausfallzeiten beliefen sich innerhalb der letzten 12 Monate auf 555.000 US-Dollar. Für Organisationen, die innerhalb der letzten 12 Monate auch einen Datenverlust zu verzeichnen hatten, liegt die Zahl noch wesentlich höher – hierbei lagen die Kosten bei 914.000 US-Dollar. Es besteht kein Zweifel, Ihre Daten müssen geschützt werden – und Sie müssen sich auf Ihre Schutzbereitschaft verlassen können.[12]

WIE LÄSST SICH ABHILFE SCHAFFEN?

Daten, ohne die ein Unternehmen den täglichen Betrieb nicht aufrechterhalten kann, oder die der Einhaltung behördlicher Auflagen unterliegen, müssen immer geschützt werden. Hacker kümmert es nicht notwendigerweise, wem die Informationen gehören. Sie werden einfach alles daransetzen, jede Schwachstelle in der IT-Infrastruktur zu nutzen, um die Daten eines Unternehmens zu stehlen, zu beschädigen oder gegen Lösegeld zurückzuhalten. Wie die meisten Kriminellen sind Cyberkriminelle Opportunisten, die sich einfache Ziele aussuchen. Sind Sie ein einfaches Ziel? Stellen Sie sich die folgenden Fragen:

- Kennen Ihre Mitarbeiter das Risiko, das unerwünschte E-Mails bergen?
- Sind Ihre Firewalls und E-Mail-Filter stets aktuell?
- Verwenden Sie abgelaufene Virenschutzsoftware?
- Werden bei Ihnen Daten von Endpunkten mit cloudbasierten Systemen zur Dateisynchronisierung und -freigabe synchronisiert?

---

[5] Ransomware and Recent Variants, United States Computer Emergency Readiness Team; March 31, 2016.
[6] Crypto-Ransomware: Survey of IT Experts, page 16, Jeffrey Henning, Researchscape International; February 4, 2016.
[7] UK Companies Commonly Held Hostage by Hackers, Urban Schrott, ESET Ireland; June 29, 2015.
[8] Ransomware victims: Just pay up, grin, and bear it, says the FBI, The Register; October 27, 2015.
[9] Internet Security Threat Report, Volume 21, page 58, Symantec, April 2016.
[10] Ibid., page 8.
[11] Ibid.
[12] EMC Global Data Protection Index, independent research by Vanson Bourne, March–April 2016.

Es ist wichtig zu beachten, dass gängige Backuplösungen wie ein USB-Laufwerk oder ein NAS-Gerät (Network Attached Storage) keine zuverlässigen Methoden zum Sichern und Schützen Ihrer Daten darstellen. Ransomware verbreitet sich in der Regel im gesamten Dateisystem eines Unternehmens, einschließlich angeschlossener Laufwerke oder Netzwerkfreigaben, und verschlüsselt sowohl Produktions- als auch Backupdaten.

Die zuverlässigste Methode zum Schutz von Unternehmensdaten ist immer noch das Backup. Je schneller und einfacher sich ein Backup auf den Zustand vor der Infektion wiederherstellen lässt, desto weniger wahrscheinlich ist es, dass Sie durch einen schwerwiegenden Ausfall der Business Continuity beeinträchtigt werden. Was müssen Sie bei der Auswahl einer Backuplösung beachten, um den Schutz Ihrer Daten sicherzustellen? Bedenken Sie:

- Erfolgt das Backup extern (außerhalb Ihres primären Standorts)?
- Können Sie überprüfen, ob die Backups durchgeführt werden?
- Können Sie überprüfen, dass die Daten auf den ursprünglichen Zustand wiederhergestellt werden können?
- Wie schnell können Sie Daten wiederherstellen, die als Geisel genommen wurden?

Das Vorhandensein eines realisierbaren Backup- und Recovery-Plans ist nicht nur solide betriebliche Praxis, sondern je nach Branche oder Typ des Unternehmens häufig auch durch Gesetze oder Vorschriften vorgeschrieben:

- Gemäß HIPAA müssen Unternehmen im Gesundheitswesen einen realisierbaren Backup- und Disaster-Recovery-Plan zum Schutz ihrer elektronischen Patientendaten vorweisen und diesen regelmäßig testen lassen.[13]
- Zwei Kontrollorgane für das Finanz- und Bankenwesen, die OCIE und die FFIEC, haben die Cybersicherheit – einschließlich der Möglichkeit zur Wiederherstellung nach Incidents – zu einem Kernbestandteil ihrer Durchsetzungs- und Auditprioritäten gemacht.[14]
- Die SEC hat Aktiengesellschaften auf die Notwendigkeit ausreichender Cyberkontrollen, einschließlich Backup- und Recovery-Funktionen, und die Pflicht hingewiesen, materielle Cybersicherheitsrisiken öffentlich anzuzeigen. In der heutigen Welt könnte die Unfähigkeit zur Wiederherstellung nach einer zunehmend allgemeinen Bedrohung wie Ransomware unter die Offenlegungspflicht fallen.[15]

Mit den geeigneten Backup- und Recovery-Lösungen können Sie auch nach einem Hardwareausfall, Diebstahl, Virenangriff (einschließlich eines Erpressungsversuchs mit Ransomware!), versehentlichem Löschen, einer Naturkatastrophe oder einer von Menschen verursachten Katastrophe sicherstellen, dass Ihre Daten zur Verfügung stehen, auf den ursprünglichen Zustand wiederhergestellt werden können und Ihr Unternehmen die geltenden Vorschriften einhält.

SICHERN IHRER DATEN MIT EMC

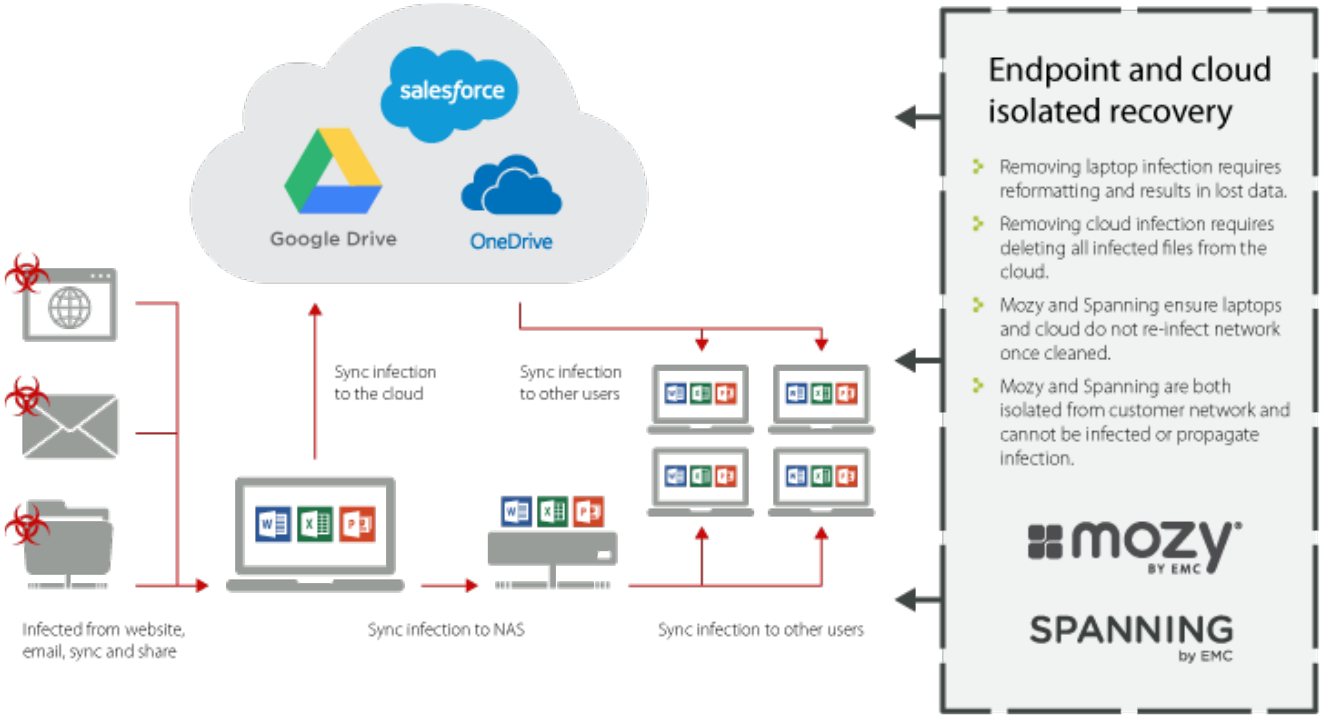
Sie können einen Datenverlust durch Ransomware vermeiden, indem Sie Ihre wertvollen Daten mit den renommierten Datensicherheitslösungen von EMC sichern.

Es beginnt am Endpunkt

Das Wiederherstellen der Server garantiert nicht, dass Sie die Infektion aus Ihrem Netzwerk entfernt haben, da diese wahrscheinlich von einem Endpunkt ausging, wie in der folgenden Abbildung dargestellt. Daten, die mit Mozy und Spanning gesichert werden – beide von EMC – sind vom Kundennetzwerk isoliert und können nicht infiziert werden oder eine Infektion weitergeben.

---

[13] HIPAA Security Rule, 45 CFR 164.308(7).
[14] National Exam Program Risk Alert, Volume IV, Issue 8; September 15, 2016.
[15] Emerging SEC guidance and enforcement regarding data privacy and breach disclosures, Joseph D. Masterson, Inside Counsel; June 25, 2015; and Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks, Paul Weiss; September 30, 2015.



Endpunktdatensicherheit mit Mozy von EMC

Ein Cloudbackup mit Mozy verhindert, dass Ihre wichtigen Endpunktdateien und Serverdaten durch Ransomware infiziert werden. Mit einer einzigartigen Back-end-Technologie verhindert Mozy jegliche Ausführung von Code in den gesicherten Dateien. Ein einfaches Backup an sich ist jedoch nicht ausreichend, um dafür zu sorgen, dass Ihre Dateien vor Ransomware geschützt sind.

Wenn eine Malwareinfektion beteiligt ist, funktioniert die Wiederherstellung eines Endpunkts oder Servers von einem Backup am besten und einfachsten durch die Auswahl eines Wiederherstellungszeitpunkts. Mozy speichert Dateiversionen bis zu 90 Tage lang, d. h., wenn Sie den Infektionsherd (Benutzer und Datei) und den Zeitpunkt, zu dem die Schadsoftware in die Maschine eingeschleust wurde, ermittelt haben, kann Mozy alle Dateien für den angegebenen Benutzer ab dem Point-in-Time kurz vor Einschleusung der Schadsoftware wiederherstellen. Angenommen, die Schadsoftware wurde am 2. Juni eingeschleust, dann können Sie Dateien aus dem Backup vom 1. Juni wiederherstellen.

SaaS-Datensicherheit mit Spanning von EMC

SaaS-Office-Produktivitätsplattformen wie Google Apps oder Microsoft Office 365 sind ebenfalls anfällig für Angriffe durch Malware und Google oder Microsoft können Ihre Dateien möglicherweise nicht schnell genug auf einen Zustand vor der Infektion wiederherstellen. Infizierte Endpunktgeräte können sich mit diesen Plattformen synchronisieren. In einigen Fällen kann die Schadsoftware automatisch über freigegebene Laufwerke und Ordner verbreitet werden und die innerhalb oder sogar außerhalb Ihres Unternehmens freigegebenen Dateien verschlüsseln.

Ein Backup mit Spanning schützt in Google Apps und Office 365 gespeicherte und erzeugte Daten und ermöglicht es Ihnen, diese schnell auf einen früheren Point-in-Time vor der Verschlüsselung durch die Ransomware wiederherzustellen.

Indem Sie die geschäftskritischen Daten Ihres Unternehmens mit den Backuplösungen Mozy und Spanning sichern und schützen, erhalten Sie die Gewissheit, dass Sie Ihre Daten bei einem Datenverlustereignis schnell und einfach genau auf den Zustand wiederherstellen können, den diese zu einem beliebigen Point-in-Time hatten. Das bedeutet, dass Ihre Daten sicher, geschützt und immer verfügbar sind. Diese Lösungen sorgen dafür, dass Sie auf einen Angriff reagieren und sich davon wieder erholen können. Sie ermöglichen eine schnelle Wiederherstellung Ihrer Daten auf den ursprünglichen Zustand für Business Continuity und zur Erfüllung von Recovery Time bzw. Recovery Point Objectives (RTO und RPO).

FAZIT

ESET Irland zufolge wird Ransomware immer aggressiver, funktionsreicher und taucht wellenartig in immer mehr Varianten auf.[16] Auch wenn Prävention und Erkennung entscheidend sind, ist ein regelmäßig aktualisiertes Backup, das eine schnelle und präzise Wiederherstellung ermöglicht, die letzte Verteidigungslinie. „… [B]ackupdateien sind eine effektive Methode zur Minimierung der Auswirkung von Ransomware und … die Implementierung von Best Practices im Bereich Computersicherheit ist der effektivste Weg zur Vermeidung von Infektionen mit Ransomware. Personen oder Unternehmen, die ihre Dateien regelmäßig auf einem externen Server oder Gerät sichern, können ihre Festplatte von der Ransomware säubern und ihre Dateien von einem Backup wiederherstellen. Wenn alle Benutzer und Unternehmen ihre Dateien sichern würden, wäre Ransomware kein so einträgliches Geschäft für Cyberkriminelle.“[17]

Unternehmen verlassen sich auf digitale Daten mehr denn je. Aus diesem Grund müssen alle Unternehmen – vom kleinsten bis zum größten – die erforderlichen Maßnahmen ergreifen, die dafür sorgen, dass ihre Daten sicher geschützt und schnell auf den ursprünglichen Zustand wiederhergestellt werden können.

Für weitere Informationen dazu, wie Sie mithilfe von Endpunktdatensicherheit eine Ransomware-Katastrophe verhindern können, besuchen Sie Mozy. Und für Informationen dazu, wie Sie Ihre SaaS-Daten schützen können, besuchen Sie Spanning.

---

[16] Jigsaw and how ransomware is becoming more aggressive with new capabilities, Urban Schrott, ESET Ireland; May 4, 2016.
[17] U.S. Department of Justice, Federal Bureau of Investigation, Letter to Senator Ron Wyden, February 8, 2016.