RANSOMWARE MEETS BLOCKCHAIN

Jörn Erbguth

PhD Candidate – Information Systems, Centre Universitaire d'Informatique, Université de Genève
Battelle bâtiment A, 7 route de Drize, 1227 Carouge, CH
Jorn.Erbguth@unige.ch; https://erbguth.ch/

Schlagworte: ***Ransomware, Blockchain, autonome Systeme, DAO***

Abstract: *Ransomware ist Software, die in der Regel Daten verschlüsselt um Lösegelder zu erpressen. Die Blockchain-Technologie ermöglicht dezentrale autonome Organisationen (DAO), die autark und unbeeinflussbar Verträge schließen und Finanztransaktionen tätigen. Die Kombination von Ransomware und Blockchain führt zu einem System, welches autonom alle Teile der Erpressung mit Ransomware verbindet: Dies sind die Erstellung von Ransomware, der Angriff über Phishingmails oder dem Ausnutzen von Schutzlücken und schließlich die Überwachung der Zahlung des Lösegeldes, die Überprüfung des Entschlüsselungscodes sowie die Aufteilung des Lösegeldes auf die beteiligten kriminellen Parteien. Der Vortrag entwickelt und bewertet das konkrete Bedrohungsszenario einer Ransomware DAO und leitet daraus die Notwendigkeit geeigneter Schutzmaßnahmen ab.*

1. Einleitung

In den letzten 12 Monaten waren 48% der Unternehmen in Deutschland, Frankreich, UK und USA von Ransomware betroffen.[1] Die Zahlung des Lösegeldes wird meistens in Bitcoin gefordert, da dort Konten Personen nicht direkt zuzuordnen sind. Ransomware geht inzwischen vermehrt arbeitsteilig vor. Unterschiedliche Personen kümmern sich um die verschlüsselnde Software, die Abwicklung der Lösegeldforderung und das Überwinden von Sicherheitsbarrieren z.B. via Phishing Mails. Daher liegt es nahe, nicht nur die Zahlung des Lösegeldes, sondern auch die Koordination dieser Aktivitäten auf einer Blockchain zu organisieren, damit sie ebenfalls keiner natürlichen Person mehr direkt zuzuordnen sind.

2. Ransomware

Ransomware ist eine Malware, die die Nutzung von Computersystemen verhindert und erst wieder freigibt, wenn Lösegeld gezahlt worden ist. Die aktuell grassierende Ransomware verschlüsselt dazu meistens die auf dem System abgelegten Daten des Nutzers.

Als nächste Evolutionsstufe der Ransomware wird die Ausweitung auf das Internet der Dinge gesehen. Von der Heizung, die erst nach Lösegeldzahlung wieder heizt, über das Auto, welches den Dienst komplett oder auch nur das Bremsen verweigert bis zur Wohnungstür, welche die Bewohner aussperrt oder Diebe hereinlässt, gibt es viele Bedrohungsszenarien.[2]

Einige Ransomware-Varianten bieten Partnerprogramme an. Dieser «Ransomware as a Service» (RaaS) verlagert das Formulieren von vertrauenserweckenden Phishing-Mails auf Partner, die dafür einen Anteil des erpressten Lösegeldes erhalten.[3]

---

1 SentinelOne, SentinelOne Reveals that Almost Half of Global Businesses Suffered a Ransomware Attack in Last Year.
2 Beuth, Ransomware – Wenn dich dein Thermostat erpresst.
3 Adams, Petya and Mischa Ransomware Affiliate System Publicly Released.

3. Decentralized Autonomous Organizations auf der Blockchain

Die Blockchain-Technologie bietet die Möglichkeit, Daten und Programme dezentral verteilt und von außen kaum beeinflussbar abzulegen und auszuführen. Wegen der Unveränderbarkeit der Informationen auf der Blockchain wird sie für digitale autonome Währungen wie z.B. Bitcoin verwendet.[4] «Smart Contracts» sind kleine Computerprogramme, die auf der Blockchain abgelegt sind und die Modifikation der Daten auf der Blockchain kontrollieren.[5] «Smart Contracts» sind daher ideal um Transaktionen digitaler Währungen oder Einträge und Modifikationen eines Registers zu kontrollieren. Damit wird sichergestellt, dass jeder nur die Änderungen vornehmen kann, zu denen er berechtigt ist. Mit «Smart Contracts» können auch dezentralisierte autonome Organisationen (DAO) modelliert werden. Die Gefahr krimineller DAOs wird diskutiert aber als Begleiterscheinung der neuen Technologie in Kauf genommen.[6] Das Projekt «The DAO» war ein Venture Capital Fond, der komplett auf der Blockchain verwaltet werden und einzelne DAOs abspalten sollte, die auf der Blockchain «lebend» bestimmte Geschäftsideen verfolgen. Alle Tätigkeiten der DAOs sollten über die Blockchain abgewickelt werden. Das ging von der Verwaltung und Ausübung des Stimmrechts der Anteilseigner über den «Vertragsschluss» mit Mitarbeitern und Vertragspartnern bis zu deren Bezahlung.[7]

4. Anforderungen an eine Ransomware DAO

Die Verwendung von DAOs zur Akquise und Vergütung von Partnern für kriminelle Ransomware erscheint ein naheliegendes Bedrohungsszenario. Die Partner steuern die Ransomware, Zero-day-exploits oder Phisingmails bei. Im Erfolgsfall erhalten diese über die DAO ihren Anteil der Beute. Auch können diese DAOs weitere DAOs mit ggf. modifizierten Parametern erstellen, die wiederum unabhängig voneinander in evolutionärer Konkurrenz ihr Unwesen treiben. Beim Schreiben des Codes der kriminellen DAO kann der Urheber dabei nach Belieben die DAO im Detail kontrollieren, sich nur den kriminellen Gewinn auszahlen lassen oder die DAO sich vollständig autark entwickeln lassen.

4.1. Markplatz

Eine Ransomware DAO stellt einen Marktplatz für Ransomware dar. Auf diesem Marktplatz kommen als Teilnehmer folgende Gruppen zusammen:

- **Anbieter** von Ransomware Software, die den Inhalt von Speichermedien möglichst unbemerkt im Hintergrund verschlüsselt. Die Software bietet darüber hinaus die Möglichkeit die Daten wieder zu entschlüsseln, wenn der richtige Schlüssel eingegeben wurde.
- **Vertriebspartner**, die die Verschlüsselungssoftware unter Überwindung von Sicherheitsbarrieren auf die Systeme der Opfer bringen. Dabei kann z.B. über regionalisierte oder gar personalisierte Angriffe das Vertrauen zur Überwindung von Sicherheitsbarrieren geschaffen werden. Dies geschieht etwa über Phishingmails, Smartphone-Apps oder verteilte Speichermedien. Daneben können auch Exploits zur technischen Überwindung von Sicherheitsbarrieren verwendet werden.
- Die **Opfer** der Ransomware-Angriffe, die über diesen Marktplatz den Schlüssel zur Entschlüsselung ihrer Daten erwerben.

4.2. Kontrolle durch Algorithmen statt Vertrauen

Da es sich um illegale Aktivitäten handelt, ist das Vertrauen in die anderen Parteien gering. Auch das Opfer wird alles versuchen, ohne Zahlung des Lösegeldes die Daten entschlüsseln zu können. Das System der kriminellen DAO muss daher die technische Sicherheit bieten, dass zum einen die Entschlüsselung nur gegen Zahlung

4 Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.
5 Gord, Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality.
6 Simonite, Bitcoin's Dark Side Could Get Darker.
7 Morris, Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting.

möglich ist. Zum anderen muss umgekehrt sichergestellt werden, dass der Anbieter nur dann die Zahlung erhält, wenn er auch einen passenden Entschlüsselungscode liefert.

Ebenso muss unter den kriminellen Partnern sichergestellt werden, dass der Anreiz sich gemäß den Regeln der Ransomware-DAO zu verhalten, lukrativer als der Bruch dieser Regeln ist. Insbesondere muss verhindert werden, dass eine der kriminellen Parteien das Geschäft alleine macht und dadurch den Lösegeldanteil der anderen Partei unterschlägt.

Schließlich müssen die Aktivitäten so abgesichert werden, dass die Strafverfolgungsbehörden keinen Ansatz finden, die kriminelle Tätigkeit zu unterbinden oder die kriminell handelnden Parteien zu identifizieren.

5. Konzept für eine Ransomware DAO

Im Folgenden wird das Konzept einer Ransomware DAO soweit konkretisiert, dass die Realisierbarkeit plausibel wird. Eine DAO ermöglicht die Interaktion pseudonymer Parteien auf Basis transparenter Regeln.

5.1. Ablauf

Der Ablauf eines Ransomware-Angriffs könnte dabei wie folgt implementiert werden:

1. Ein Anbieter einer Ransomware stellt ein Angebot auf der Ransomware-DAO ein. Teil des Angebots sind Parameter wie die Höhe des Lösegeldes, der Gewinnanteil der beteiligten kriminellen Parteien sowie ggf. eine Anzahlung des Vertriebspartners.
2. Ein Vertriebspartner nimmt das Angebot an und bezahlt eine ggf. geforderte Anzahlung.
3. Der Anbieter der Ransomware generiert ein Public Key Encryption Schlüsselpaar für die Verschlüsselung der Daten des Opfers. Er integriert den öffentlichen Schlüsselteil in seine Software, signiert diese mit dem privaten Schlüssel seines verwendeten Blockchain-Accounts und verschlüsselt sie mit dem öffentlichen Schlüssel des vom Vertriebspartner verwendeten Blockchain-Account. Anschließend erstellt der Anbieter ein Konto für einen Ablageort auf einer beliebigen Plattform und legt die Software dort ab. Die Zugangsdaten zu dieser Ablage-Plattform verschlüsselt der Anbieter mit dem öffentlichen Schlüssel des Blockchain Accounts des Vertriebspartners. Er übergibt die verschlüsselten Zugangsdaten sowie den öffentlichen Teil des Public Key Encryption Schlüsselpaar an die Ransomware DAO.
4. Der Vertriebspartner kann die Software in einer «Sandbox» oder auf einem Testsystem testen und dabei verifizieren, dass die Verschlüsselung mit dem angegebenen Schlüssel durchgeführt wird.
5. Die Ransomware wird an das Opfer übermittelt und dort unter Umgehung oder Bruch der Sicherheitsmechanismen ausgeführt. Das Opfer erhält die Mitteilung, das Lösegeld an die Ransomware DAO zu zahlen.
6. Nach der Zahlung stellt der Anbieter der Ransomware den privaten Teil des Schlüsselpaars auf die Blockchain. Die Ransomware-DAO überprüft dabei, ob der private Teil zum bereits registrierten öffentlichen Teil passt. Nur nach positiver Prüfung wird die Zahlung des Opfers nach dem festgelegten Aufteilungsschlüssel auf den Anbieter, den Vertriebspartner und ggf. auch die Plattform aufgeteilt.
7. Sollte der Ransomware Anbieter keinen passenden Schlüssel einstellen, kann das Opfer nach Ablauf einer Frist das gezahlte Lösegeld von der Ransomware DAO zurückerhalten. Eine Entschlüsselung seiner Dateien, erfolgt dann jedoch nicht.

Eine Automatisierung dieser Schritte auf Seitens des Anbieters oder des Vertriebspartners ist möglich, erfolgt jedoch ggf. außerhalb der Blockchain. Anbieter können gegenüber den Vertriebspartnern über den Nachweis erfolgreicher Angriffe Reputation erwerben. Diese Reputation dient dazu, das Vertrauen von potentiellen Vertriebspartnern zu gewinnen.

5.2. Bewertung des Konzeptes

Eine DAO kann nicht selbständig auf unerwartetes Verhalten der Marktteilnehmer reagieren. Daher ist es wichtig, dass die DAO bei diesem Konzept gegen alle möglichen Angriffspunkte geschützt werden kann.

5.2.1. Entschlüsselung nur gegen Zahlung des Lösegeldes durch das Opfer

Für jeden Angriff wird ein eigenes Public Key Encryption Paar verwendet. Eine Entschlüsselung ist daher nur mit dem passenden privaten Schlüssel möglich, über den nur der Anbieter der Ransomware verfügt. Da die Blockchain für alle offen lesbar ist, kann der Code zur Entschlüsselung nicht auf der Blockchain abgelegt werden. Vielmehr wird er im Rahmen des unter geschilderten 5.1. Ablaufes Punkt 6 erst nach Zahlung auf die Blockchain gelegt.

5.2.2. Rückerstattung des Lösegeldes, wenn kein Entschlüsselungscode nicht geliefert wird

Die DAO prüft über die Blockchain ob der gelieferte Schlüssel zum öffentlich hinterlegten Verschlüsselungscode passt. Natürlich könnte der hinterlegte und der tatsächlich zur Verschlüsselung verwendete Schlüssel voneinander abweichen. Dann wäre der Entschlüsselungscode wirkungslos, obwohl er zum hinterlegten Verschlüsselungscode passt. Da jedoch der Vertriebspartner die Verschlüsselungssoftware prüfen kann, kann eine solche Abweichung festgestellt werden.

5.2.3. Anderweitige Verwendung der Ransomware durch den Vertriebspartner

Der Vertriebspartner könnte die Ransomware beziehen, ohne damit Angriffe zu starten. Er könnte die Software analysieren, um entweder selbst eine Variante dieser Software bereit zu stellen oder das Wissen für die Verbesserung von Anti-Ransomware zu verwenden.

Diese beiden Möglichkeiten können technisch nicht einfach ausgeschlossen werden. Eine Teilnahmegebühr, die der Vertriebspartner vorstrecken muss, kann diese Problematik verringern. Zwar wird auch dann bei ausbleibendem Angriff der Anbieter keinen Anteil an einem Lösegeld erhalten. Er wird durch diese Teilnahmegebühr jedoch soweit entschädigt, dass es sich für ihn lohnt, weitere Versionen der Ransomware anzubieten. Schließlich wird auch bei jedem Angriff die Ransomware offenbart, so dass es immer wieder neue Variationen bedarf um angepasste Abwehrmaßnahmen auf Opferseite zu unterlaufen.

5.2.4. Bereitstellung defekter Ransomware durch den Anbieter

Auch nach einer Prüfung durch den Vertriebspartner kann dieser nicht sicher ausschließen, dass die Ransomware überhaupt verschlüsselt und dann auch auf die Ransomware-DAO für die Lösegeldzahlung verweist. Da auf der Blockchain die Angriffshistorie der Anbieter von Ransomware offen zugänglich ist, werden Anbieter nicht funktionierender Ransomware erkennbar und auf dem Marktplatz gemieden.

5.2.5. Ergebnis

Zwischen Anbieter, Vertriebspartner und Opfer kann das Konzept so abgesichert werden, dass eine Umgehung für die Marktteilnehmer nicht lohnend erscheint.

5.3. Möglichkeiten der Strafverfolgung

Strafverfolgungsbehörden werden versuchen, den Betrieb der Ransomware-DAO zu stoppen und die kriminellen Marktteilnehmer zur Strafverfolgung zu identifizieren.

5.3.1. Identifizierung des Anbieters von Ransomware oder der Vertriebspartner bei der Kommunikation mit der Blockchain

Der Anbieter von Ransomware und der Vertriebspartner kommunizieren bis auf eine Ausnahme nur über die Ransomware-DAO. Es ist möglich über Heuristiken den Einträgen auf einer Blockchain mit einer gewissen

Wahrscheinlichkeit IP-Adressen zuzuordnen.[8] Durch geeignete Maßnahmen wie z.B. der Verwendung von Onion Routing[9] wie etwa «TOR»[10] kann die Herkunft der Requests an die Ransomware-DAO jedoch zusätzlich verschleiert werden.

5.3.2. Identifizierung des Anbieters von Ransomware beim Ablegen der Ransomware

Der Anbieter entscheidet selbst und ohne Vorankündigung wo die Software abgelegt wird. Daher sind gezielte Überwachungsmaßnahmen nicht möglich. Wird die eigene IP-Adresse beim Ablegen der Software wirksam verschleiert, wird sich im Nachhinein kaum feststellen lassen, wer die Ransomware dort abgelegt hat.

5.3.3. Identifizierung des Vertriebspartners beim Kontakt mit der Ransomware

Der Vertriebspartner muss die Ransomware zum Test und zur Verteilung von einem Server herunterladen. Dabei kann der Rechner des Vertriebspartners angegriffen werden. Verwendet der Vertriebspartner hierzu jedoch jeweils neu zurückgesetzte virtuelle Maschinen und verschleiert die Herkunft der Requests, so dürfte die Identifizierung des Vertriebspartners schwierig sein.

5.3.4. Identifizierung der Geldströme

Nach erfolgter Lösegeldzahlung wird das Lösegeld auf den Anbieter der Ransomware, den Vertriebspartner und die Ransomware-DAO verteilt. Die darauffolgenden Transaktionen des Blockchain-Geldes sind zwar pseudonym aber offen auf der Blockchain einsehbar. «Mixer»[11] versuchen Geldtransaktionen so zu vermengen, dass die konkrete Herkunft nicht mehr zuzuordnen ist. Analyseprogramme[12] versuchen jedoch mit aufwändigen statistischen Analysen eine Zuordnung dennoch herzustellen.

5.3.5. Unterbinden des Betriebs der Ransomware DAO

Eine DAO ist – einmal auf der Blockchain – nicht mehr vom Zutun des Erstellers abhängig. Sie benötigt auch keinen adressierbaren Webserver oder einen Webhoster. Solange die Blockchain ungepatched in Betrieb ist, wird die DAO weiter gemäß dem vorgegebenen Algorithmus agieren. Die Ransomware-DAO kann daher nur gestoppt werden, wenn alle Knoten der Blockchain außer Betrieb gesetzt werden oder die Betreiber der Blockchain entscheiden, ein Softwareupdate einzuspielen, der die kritische Ransomware-DAO deaktiviert. Ist die Ransomware-DAO deaktiviert, kann der gleiche – oder leicht modifizierte Code – jederzeit wieder eingespielt werden.

5.3.6. Ergebnis

Die Strafverfolgungsmöglichkeiten sind begrenzt. Die Blockade einer Ransomware-DAO ist nur mit massiven Eingriffen in die Blockchain möglich und tangiert alle dort laufenden Anwendungen.

6. Bewertung

Ransomware-DAOs stellen eine realistische Bedrohung dar. Sie bieten gegenüber einfacher Ransomware eine «bessere» Arbeitsteilung sowie auf Grund der Entschlüsselungsgarantie eine höhere Zahlungsbereitschaft. Strafverfolgungsbehörden können solche DAOs nur schwer bekämpfen.

7. Konsequenzen und Ausblick

Für Smart Contracts gibt es aktuell keine Kontrollinstanz. Ob Ransomware, Erpressungsnetzwerk, Auftragsmord oder Geldwäsche – ein einmal angelegter «Smart Contract» ist generell unabänderbar, es sei denn eine

---

8 Koshy/Koshy/McDaniel, An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, S. 469–485.

9 Goldschlag/Reed/Syverson, Onion Routing for Anonymous and Private Internet Connections.

10 https://www.torproject.org (alle Websites zuletzt überprüft am 13. Dezember 2016).

11 Möser/Böhme/Breuker, An inquiry into money laundering tools in the Bitcoin ecosystem.

12 Z.B. Elliptic, https://www.elliptic.co.

Änderung wäre im «Smart Contract» selbst vorgesehen. Für alle anderen Änderungen müsste sich die Mehrheit der weltweit verteilten Mineure einer Blockchain auf ein Softwareupdate einigen, welches diese dann einspielen. Wenn man diese Entscheidung nicht den Mineuren überlassen will, stellt sich die Frage, ob es nicht doch eine Art Generalschlüssel für Blockchains geben muss. Wie dieser Generalschlüssel jedoch kontrolliert werden kann und wer in einer globalisierten Welt den Schlüssel für die Blockade oder Modifikation einer kriminell agierenden DAO haben soll, bleibt zu diskutieren.

Ohne Regulierung droht eine weitere Steigerung des Bedrohungspotentials durch die Kombination von Kampfrobotern und DAOs. Diese finanziell autarken Kampfmaschinen könnten «Schutzgeld» erpressen und mit dem ergaunerten Geld autark Munition, Ersatzteile und weitere Kampfroboter kaufen. Bei diesen Szenarien gibt es glücklicherweise noch Hürden bei der Konstruktion der Kampfroboter, sowie der Kontrolle der Übergabe der Munition und Ersatzteile durch die DAO. Bei Weiterentwicklung der physischen Autonomie von Robotersystemen erscheinen solche Szenarien jedoch leider zunehmend realistisch.

8. Literatur

Adams, Lawrence, Petya and Mischa Ransomware Affiliate System Publicly Released, BleepingComputer, 26. Juli 2016, https://www.bleepingcomputer.com/news/security/petya-and-mischa-ransomware-affiliate-system-publicly-released/.

Beuth, Patrick, Ransomware – Wenn dich dein Thermostat erpresst, Zeit Online, 8. August 2016, http://www.zeit.de/digital/datenschutz/2016-08/ransomware-thermostat-gehackt-def-con.

Goldschlag, David/Reed, Michael/Syverson, Paul, Onion Routing for Anonymous and Private Internet Connections, Communications of the ACM Februar 1999, Vol 42, 2, S. 39–41.

Gord, Michael, Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality, Bitcoin Magazine, 26. April 2016, https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751.

Koshy, Philip/Koshy, Diana/McDaniel, Patrick, An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, in: Christin, Nicolas/Safavi-Naini, Reihaneh (Hrsg.), Financial Cryptography and Data Security, Volume 8437 of the series Lecture Notes in Computer Science, S. 469–485.

Möser, Malte/Böhme, Rainer/Breuker, Dominik, An inquiry into money laundering tools in the Bitcoin ecosystem, 2013 APWG eCrime Researchers Summit, S. 1–14.

Morris, David Z., Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting, FORTUNE, 15. Mai 2016, http://fortune.com/2016/05/15/leaderless-blockchain-vc-fund/.

Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

SentinelOne, SentinelOne Reveals that Almost Half of Global Businesses Suffered a Ransomware Attack in Last Year, Palo Alto CA, USA, 18. November 2016, https://sentinelone.com/article/sentinelone-reveals-half-global-businesses-suffered-ransomware-attack-last-year/.

Simonite, Tom, Bitcoin's Dark Side Could Get Darker, MIT Techonology Review, 13. August 2015, https://www.technologyreview.com/s/540151/bitcoins-dark-side-could-get-darker/.