Opmerking vooraf: Dit onderzoeksrapport blijft actief tot 31 juli 2018 en sommige kerncijfers, inclusief het totaal verzamelde ransomware-aantallen, kunnen nog veranderen. Wij houden u op de hoogte in het geval een verandering plaatsvindt en u kunt contact met ons opnemen voor vragen en het controleren van feiten en cijfers, indien nodig.

Interviews met de SophosLabs researchers en Threat experts en grafieken van het report zijn beschikbaar op aanvraag.

De verwijzing naar de finale versie met Sophos commentaar is terug te vinden via volgende websites:

**SophosLabs Uncut:** <http://news.sophos.com/en-us/samsam-guide-to-coverage>

**Naked Security:** <https://nakedsecurity.sophos.com/samsam>

**Full report:** <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf>

# SamSam: De (bijna) zes miljoen dollar ransomware

## Management/pers briefing en highlights van ons onderzoek naar de ransomware campagne

### Managementsamenvatting

Sophos heeft op de lange termijn onderzoek uitgevoerd naar de SamSam ransomware-campagne, na de introductie aan het einde van 2015. Dit rapport vat de resultaten samen van de attacker’s tools, technieken en protocollen met als doel een beter begrip te krijgen over deze relatief unieke gevaren.

De aanvalsmethode is verassend genoeg handmatig, waarbij de aanvaller zorgvuldig en onopgemerkt te werk gaat. Vervolgens kan de aanvaller tegenmaatregelen nemen (indien nodig) en is verassend goed in het ontwijken van allerlei verschillende beveiligingstechnieken. Als het proces van dataversleuteling is verstoord, verwijdert de malware direct zelf alle sporen om verder onderzoek te hinderen.

SamSam is een bijzonder grondige versleutelingstool die niet alleen databestanden ontoegankelijk maakt, maar het versleutelt ook alle programma’s die niet essentieel zijn voor de werking van een Windows computer, waarvan de meeste niet regelmatig worden voorzien van een back-up. Het herstel kan wellicht een herinstallatie van software vereisen en het herstellen van backups. De aanvaller is enorm goed in het verborgen houden van zijn sporen en lijkt na verloop van tijd steeds meer paranoïde te worden (of meer ervaren) en voegt geleidelijk meer beveiligingsfuncties toe aan zijn tools en websites.

# Belangrijkste resultaten

## De basis

* De introductie van de SamSam ransomware verscheen onverwacht in december 2015.
* Sommige slachtoffers hebben een wijdverspreide ransomware aanval gemeld die grote organisaties, zoals ziekenhuizen, scholen en steden heeft geraakt.
* Het kostte aanzienlijk wat tijd om de details van de aanvallers te krijgen, omdat de aanvallers met veel zorgvuldigheid hun methodes hebben geprobeerd te verdoezelen en daarbovenop het bewijs dat hen kon verhullen, verwijderd.
* Veel slachtoffers vonden dat ze niet voldoende of snel genoeg konden herstellen om de bedrijfscontinuïteit alleen te waarborgen en betaalden met tegenzin het losgeld.

## De statistieken

* Door het volgen van Bitcoin-adressen op losgeld, details en voorbeeldbestanden en door samen te werken met de firma Neutrino, heeft Sophos berekend dat SamSam sinds eind 2015 meer dan $5,9 miljoen Amerikaanse dollar aan schepper(s) heeft verdiend.
* Sophos heeft vastgesteld dat 74% van de bekende slachtoffers zijn gevestigd in de Verenigde Staten. Het Verenigd Koninkrijk neemt de tweede plek in met 8%. België sluit de top-3 af met 6% van de bekende slachtoffers, voor Canada (5%).
* De SamSam-aanvaller heeft losgeld ontvangen ter waarde van $64.000, op basis van analyse van losgeldbetalingen aan de Bitcoin-wallets.
* In tegenstelling tot de meeste andere ransomware, codeert SamSam niet alleen documentbestanden, afbeeldingen en andere persoonlijke- of werkgegevens, maar ook configuratie- en gegevensbestanden die nodig zijn om toepassingen uit te voeren (bijvoorbeeld Microsoft Office). Slachtoffers wiens back-upstrategie alleen de documenten en bestanden van de gebruiker beschermt, zullen niet in staat zijn om een ​​machine te herstellen zonder deze eerst opnieuw te imiteren.
* Elke volgende aanval toont een vooruitgang in verfijning en een toenemend bewustzijn van hoe men de operationele veiligheid kan omzeilen.
* De kosten voor de slachtoffers zijn drastisch gestegen en het tempo van de aanvallen zijn tot nu toe nog niet verlaagd.

## Het slachtofferprofiel

* Een aantal middelgrote tot grote overheidsorganisaties in de gezondheidszorg, het onderwijs en de overheid hebben bekendmakingsverklaringen gepubliceerd met betrekking tot SamSam.
* 100% van de bekende slachtoffers van overheidsorganisaties hebben de aanvallen publiekelijk bekend gemaakt. 79% van de organisaties in de gezondheidszorg hebben het nieuws naar buiten gebracht, evenals 38% van de onderwijsinstellingen welke slachtoffer waren.
* De organisaties die de aanslagen publiekelijk bekend gemaakt hebben, omvatten slechts 37% van de SamSam slachtoffers die Sophos heeft vastgesteld. We geloven dat er wellicht nog honderden slachtoffers zijn die geen openbare verklaring hebben afgelegd, waarvan niet bekend is wie het zijn.
* Tot op heden heeft geen enkel ander bedrijf uit de industrie of de privésector enige publieke verklaring afgelegd waarin een SamSam aanval wordt bevestigd (die we hebben kunnen vinden). Meer dan de helft van het totale aantal slachtoffers hebben tot op de dag van vandaag geen woord gezegd over de aanvallen.

## De aanval in detail

* Sophos heeft sterke vermoedens dat veel aanvallen beginnen met een besmette Remote Desktop van een machine binnen het netwerk. Van de aanvaller is ook bekend dat hij exploits op kwetsbare machines implementeert om een externe code toe te passen.
* De aanvaller selecteert het doelwit en bereidt zijn aanval met veel nauwkeurigheid voor.
* De aanvaller behoudt zijn aanwezigheid op de besmette computer tijdens het scannen van het interne netwerk.
* De aanvaller gebruikt conventionele open-source en commerciële programma’s die normaal worden gebruikt voor systeembeheer of penetratietesten om wachtwoorden te achterhalen, ransomware-installatieprogramma’s naar domeinbeheerders te verplaatsen en de ransomware naar verbonden werkstations te pushen.
* In tegenstelling tot veel ransomware aanvallen, zijn deze niet afkomstig van een conventionele aanval met schadelijke spam of aanvallen via downloads. Elke aanval is een handmatige inbraak van een vooraf geselecteerd netwerk.
* De aanvallen verzetten zich actief tegen pogingen om het SamSam installatieprogramma te blokkeren en gebruikt routinematige technieken die bepaalde typen eindpuntbeveiliging op bepaalde systemen omzeilen, waardoor ze kwetsbaar worden voor de ransomware.
* Zodra de malware het interne netwerk kan scannen en een lijst met mogelijke slachtoffers kan maken, wachten de SamSam aanvallers tot het midden in de nacht in de tijdzone van het slachtoffer, voordat de aanval wordt uitgevoerd: een opdracht om de malware te distribueren en de geïnfecteerde machines te coderen. Timing is voor deze fase uiterst belangrijk, wanneer de meeste gebruikers en beheerders slapen, worden de kansen op succes van de aanval stapsgewijs verbeterd.

## De balans opgemaakt

* Sophos schat dat de SamSam aanvaller ongeveer $300,000\* Amerikaanse dollar per maand heeft verdiend in 2018.
* Van het volgen van Bitcoin betalingen naar Wallet adressen die eigendom zijn van de aanvaller, heeft Sophos de SamSam berekend op meer dan $5,9 miljoen Amerikaanse dollar\*.
* Het meeste losgeld dat de SamSam aanvaller ontving, werd geschat op $64.478 Amerikaanse dollar\* (op het moment van betaling).
* De betaling gebeurt door slachtoffers in Bitcoins via een aangepaste ‘betaalsite’ op het Darkweb dat zich op een uniek adres voor elke slachtoffersorganisatie bevindt.
* De betaalsite laat de SamSam aanvaller direct communiceren met de directe slachtoffers, welke een interface gebruikt die op een message omgeving lijkt.
* De hoogte van het losgeld varieert sterk per organisatie, maar is gestaag toegenomen in de tijd dat de ransomware actief is gebruikt.
* Nadat de volledige betaling is ontvangen, verplaatst de SamSam aanvaller de cryptocurrency naar een systeem van Tumblers en Mixers die proberen de bron van de Bitcoin wit te wassen via ontelbare microtransacties.

\* Opmerking: Om de kosten nauwkeurig in te schatten, als gevolg van de sterk fluctuerende wisselkoersen, berekenen we de waarde van een bepaalde hoeveelheid Bitcoin als zijn waarde op de dag dat het ontvangen wordt bij de aanvaller, en hij die onmiddellijk zou verzilveren.

## Gedragsnieuws en andere unieke kenmerken

* Recente ransom notes hebben een verontschuldigende, bijna gekwetste toon omgezet in een bestand genaamd SORRY-FOR-FILES.html en een bestandsextensie van .weapologize op elk versleuteld bestand.
* De eerste twee versies van de SamSam malware hebben meer dan 50 verschillende bestandsextensies toegevoegd aan gecodeerde gebruikersbestanden met slechts 1 variant per aanval, waardoor deze extensies om de paar aanvallen worden gewijzigd. Maar sinds versie 3 hebben ze vastgehouden aan - “.weapologize”.
* SamSam bevat binnen de programmacode een hardgecodeerde lijst met bestandsextensies om daarop als eerste te gaan richten voor encryptie. De bestanden op die lijst zullen voor alle andere worden gecodeerd.
* De ransomware codeert niet alleen de bestanden op de hardgecodeerde lijst met extensies. Nadat het de bestanden in de lijst heeft gecodeerd, versleutelt het elk ander bestand dat niet nodig is om Windows te laten werken en die IE- of Edge-browser te laten werken. De meeste back-upregimes worden niet gebruikt voor het onderhouden van back-ups van programmamappen of configuratiebestanden.
* Tijdens de gehele levensduur van de SamSam aanvallen worden bepaalde gedragskenmerken, in de vorm van kleine spelling- of interpunctiefouten, herhaald. Deze fouten kunnen leerzaam zijn bij het bepalen vanuit welke regio de aanvaller te werk gaat.
* De SamSam-payloads bevatten in het verleden tekenreeksen die de bouwpaden bevatten op de computer die wordt gebruikt om de uitvoerbare bestanden van malware te compileren. Deze bouwpaden kunnen een aanwijzing zijn om te wijzen op het gebruik van een specifieke machine bij het bouwen van malware.
* De compileertijd voor SamSam malware geeft aan dat de overgrote meerderheid van de samples wordt gebouwd tijdens een venster van 20.00 uur tot 23.00 uur in de lokale tijd van de aanvaller.
* De aanvaller verzamelt de hele week nieuwe exemplaren van de uitvoerbare malware payloads, maar gaat het minste te werk op maandag en het meeste op dinsdag. Zelfs slechteriken houden niet van maandagen.
* Als iemand het encryptie proces midden in de stream onderbreekt, detecteert een intern proces in de SamSam malware dit en voert het een veilig verwijderingsprogramma uit dat de SamSam code wist en forensisch herstel belemmert.

## Aanbevolen security toepassingen

* Er is geen gouden oplossing voor security; een actief en goed werkend beveilingsmodel is de beste methode.
* Als u de methodologie bestudeert, zijn er verschillende punten waarop basisbeveilingsmaatregelen de SamSam aanvaller kunnen stoppen.
* Sophos beveelt nu aan om deze top 4 security toepassingen te implementeren:

1. Beperkte toegang tot poort 3389 (RDP) door alleen personeel toe te staan die een VPN gebruiken om op afstand toegang te krijgen tot alle systemen. Gebruik multi-factor authenticatie voor VPN-toegang.
2. Complete, regelmatige kwetsbaarheidsscans en penetratietesten op het netwerk. Als u de recente testrapporten nog niet heeft doorgenomen, doe het dan nu.
3. Multi-factor authenticatie voor gevoelige interne systemen, zelfs voor medewerkers op het LAN of VPN.
4. Maak back-ups die offline en offsite zijn en ontwikkel een noodherstelplan dat het herstel van gegevens en systemen dekt.

* Bijkomende security toepassingen die Sophos aanbeveelt zijn:
  + Goed werkende security die aanvallers blokkeert van alle mogelijke manieren om binnen te komen en die hem toegang verlenen als hij eenmaal binnen een netwerk is.
  + Rigoureus en ijverig herstellen.
  + Server-specifieke security met Lockdown functies en Anti-Exploit beveiliging, met name voor niet-gepatchte systemen.
  + Security die synchroniseert en informatie deelt om vergrendelingen te activeren.
  + Endpoint en server security met beveiliging tegen diefstal.
  + Moeilijk te kraken en unieke IT-admin wachtwoorden met multi-factor authenticatie.
  + Wachtwoordbeleid verbeteren: moedig medewerkers aan om veilige wachtwoordbeheerders en langere zinnen te gebruiken en het niet-hergebruiken van wachtwoorden voor meerdere accounts.
  + Periodieke beoordelingen, met behulp van tools van derde partijen zoals Censys of Shodan, om voor het publiek toegankelijke diensten en poorten in uw openbare IP-adresruimte te identificeren en vervolgens te sluiten.
  + Verbeterde toegangscontrole voor accounts: volg verstandig beleid om niet-actieve accounts te beveiligen; automatisch accounts vergrendelen en IT-personeel te waarschuwen na een aantal mislukte inlogpogingen.
  + Regelmatige phishing testen en voorlichting aan het personeel over de gevaren van phishing.