Sophos setzt bei seinen KI-Entwicklungen auf branchenübergreifendes Teamwork

SophosAI setzt mit neuem Ansatz auf das öffentliche Teilen von Informationen und fördert damit die herstellerübergreifende Interaktion in der IT-Sicherheitsbranche

Wiesbaden, 14. Dezember 2020 – Sophos kündigt vier neue Entwicklungen im Bereich offener Künstliche Intelligenz (KI) an, die dazu beitragen, den Schutz gegen Cyberangriffe branchenweit zu optimieren. Hierzu gehören Datensätze, Tools und Methoden, die die Zusammenarbeit in der Security-Branche und gemeinsame Innovation fördern sollen. Damit erreicht Sophos einen weiteren Meilenstein in seinem Ziel, Errungenschaften in der Datenwissenschaft zugänglicher und den Einsatz von KI in der Cybersicherheit transparenter zu gestalten - alles mit dem Ziel, Unternehmen besser vor Cyberkriminalität zu schützen.

Während es in anderen Branchen gängige Praxis ist, KI-Methoden und -Erkenntnisse offen auszutauschen, hinkt die Cybersicherheit bei diesen Bemühungen hinterher. Die Folge ist ein eher unklares Verständnis darüber, wie KI zum Schutz vor Cyberbedrohungen beitragen kann. Sophos und sein Team von SophosAI-Datenexperten forcieren den offenen Ansatz, damit IT-Manager, Sicherheitsanalysten, CFOs, CEOs und andere Entscheidungsträger aus dem Bereich Security die KI-Vorteile auf einer möglichst einheitlichen Wissensbasis diskutieren und bewerten können.

„Mit der neuen Initiative von SophosAI und der Offenlegung von Forschungsergebnissen wollen wir unseren Beitrag dazu leisten, wie KI im Bereich der Cybersicherheit positioniert und diskutiert wird. Die heutige Uneinigkeit mit undurchsichtigen oder zurückhaltenden Aussagen über die Fähigkeiten oder die Wirksamkeit der KI macht es für Kunden schwierig bis unmöglich, diese zu verstehen oder zu validieren. Dies führt zu Skepsis und behindert künftige Fortschritte genau in dem Moment, in dem wir große Durchbrüche erleben“, sagt Joe Levy, Chief Technology Officer bei Sophos. „Diesen Zustand durch Standards oder Regulierung zu korrigieren, wird nicht schnell genug geschehen. Stattdessen erfordert es mehr Anstrengung an der Basis, um eine Reihe von Praktiken, ehrlichen Bewertungen sowie Formulierungen zu entwickeln, die die Branche in einer offenen und transparenten Art und Weise voranbringen.“

Angesichts des immensen Potenzials von KI in der Cybersicherheit kann dieser Wandel kaum überbewertet werden. Die Erkenntnisse von Sophos zeigen, dass Unternehmen zunehmend mit menschlichen Gegnern konfrontiert werden, die ihre Angriffe ständig verbessern. Sie starten hochgradig kontextbezogene Business E-Mail Compromise (BEC)-Kampagnen oder entwickeln neue Ransomware-Attacken. Eine skalierbare und effektive Verteidigung gegen Cyberattacken erfordert die Unterstützung der KI.

Sophos stellt Datensätze, Tools und Methoden in vier wichtigen Bereichen zur Verfügung:

SOREL-20M-Datensatz für schnellere Forschung bei der Malware-Erkennung
SOREL-20M ist ein Gemeinschaftsprojekt von SophosAI und ReversingLabs. Es handelt sich um einen produktionsreifen Datensatz mit Metadaten, Labels und Funktionen für 20 Millionen Windows Portable-Executable-Dateien (PE). Er steht zum Download zur Verfügung und enthält 10 Millionen entschärfte Malware-Samples, um Forschungsarbeiten über die Extraktion von Funktionen zur Beschleunigung branchenweiter Sicherheitsverbesserungen durchzuführen. Dieser Datensatz ist der erste öffentlich zugängliche Malware-

Forschungsdatensatz im Produktionsmaßstab inklusive eines kuratierten und gekennzeichneten Satzes von Samples und sicherheitsrelevanten Metadaten.

KI-gestützte Impersonation-Protection-Methode
SophosAI Impersonation Protection (Verfahren zum Schutz vor Nachahmung) wurde zum Schutz vor E-Mail-Spearphishing-Angriffen entwickelt, bei denen sich Personen als wichtige Ansprechpartner ausgeben, um Empfänger zu täuschen und schädliche Aktionen auszuführen. Der neue Schutz vergleicht den Absender eingehender E-Mails mit den Namen von Führungskräften und meldet potenziell verdächtige Nachrichten. Dazu gehören insbesondere die Namen, die bei einem Spearphishing-Angriff am häufigsten missbraucht werden, etwa von einem CEO, CFO oder Geschäftsführer. Sophos hat die zugrundeliegende KI mit Millionen bekannter Angriffs-E-Mails geschult und den neuen Ansatzauf der Defcon 28 sowie in einem Arxiv-Bericht öffentlich diskutiert.

Verfahren der digitalen Epidemiologie zur Bestimmung unentdeckter Malware
SophosAI hat eine Reihe epidemiologisch inspirierter, statistischer Modelle zur Schätzung der Verbreitung von Malware-Infektionen entwickelt, um die Menge der PE-Dateien besser abschätzen und im Gegenzug die berühmte Nadel im Heuhaufen besser finden zu können. Diese Modelle wurden öffentlich zugänglich gemacht, damit Malware, die möglicherweise übersehen oder falsch klassifiziert wurde, oder „zukünftige“ Malware, die von Angreifern aktuell entwickelt wird, besser ermittelt werden kann. Das Modell ist auf andere Dateiklassen und Informationssystem-Artefakte erweiterbar und wird auch im Sophos 2021 Threat Report besprochen.

Tools zur automatischen Signaturerstellung mit YaraML
Die Signaturerstellung für die Erkennung von Malware-Familien ist ein mühsamer manueller Prozess. Im Laufe der Jahre wurde eine Vielzahl von Methoden zur automatischen Signaturerstellung vorgestellt, von denen jedoch die meisten nicht angenommen wurden, weil sie den manuellen Prozessen nicht gerecht werden. SophosAI hat eine neue Methode zur automatischen Signaturerstellung namens, YaraML entwickelt, die sich durch einen KI-basierten Ansatz zur Lösung des Problems deutlich von früheren Optionen unterscheidet. SophosAI kompiliert vollwertige, industrietaugliche „Strength Machine Learning“-Modelle aus kommerziellen Sicherheitsprodukten direkt in Signatursprachen, wobei die KI im Wesentlichen das „Schreiben“ der Signaturen ermöglicht. Diese Methode erweist sich als weitaus effektiver als frühere Ansätze und stellt einen Durchbruch für die Cybersicherheit dar. SophosAI stellt YaraML als Open Source zur Verfügung.

Weitere Ressourcen
- Um mehr über AI in der Cybersicherheit zu erfahren, folgen Sie dem SophosAI’s blog und SophosAI auf Twitter
- Um mehr über SOREL 20M zu erfahren, lesen Sie Sophos-ReversingLabs (SOREL) 20 Million Sample Malware Dataset
- Um mehr über die digitale Epidemiologie zu erfahren, lesen Sie How Much Malware is Out There Anyway
- Um mehr über Cyber-Sicherheitstrends zu erfahren, lesen Sie den Sophos’ 2021 Threat Report
- Um mehr über die Abwehr von Ransomware zu erfahren, lesen Sie Five Early Indicators an Attacker is Present
- Lesen Sie die neuesten Nachrichten und Meinungen zum Thema Sicherheit auf Sophos Naked Security sowie auf Sophos News und SophosLabs Uncut
- Weitere Informationen von Sophos stehen auf Twitter, LinkedIn, Facebook, Spiceworks und YouTube

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de