Spiele ohne Grenzen:
Cyberkriminelle Forschungswettbewerbe

Sophos X-Ops deckt in einem neuen Report Forschungswettbewerbe auf kriminellen Online-Foren für Innovationen und die Überwindung von Sicherheitshürden auf

.

Die Wettbewerbe konzentrieren sich auf neue Angriffs- und Ausweichmethoden und spiegeln Trends im Bereich Cyberkriminalität wider, wie etwa das Ausschalten von AV/EDR, Kryptowährungsbetrug und das Einrichten von Command-and-Control-Infrastrukturen.

Sophos X-Ops beschreibt in seinem neuen Report "For the win? Offensive Research Contests on Criminal Forums" Forschungswettbewerbe, die von Cyberkriminalitäts-Foren durchgeführt werden, um neue Angriffsinnovationen voranzutreiben.

Die Wettbewerbe ähneln dabei dem „Call for Papers“ legitimer Sicherheitskonferenzen und bieten den Gewinnern erhebliche finanzielle Belohnungen, Anerkennung von Kollegen und Kolleginnen sowie potenzielle Arbeitsmöglichkeiten. Die aufgedeckten, eingereichten Beiträge liefern Cybersecurity-Experten wertvolle Einblicke in die Vorgehensweisen von Cyberkriminellen und die Art und Weise, wie sie versuchen, Sicherheitshürden zu überwinden.

„Die Tatsache, dass Cyberkriminelle diese Wettbewerbe veranstalten, daran teilnehmen und sie sogar sponsern, legt nahe, dass es ein gemeinschaftliches Ziel gibt, ihre Taktiken und Techniken weiterzuentwickeln. Es gibt sogar Hinweise darauf, dass diese Wettbewerbe als Rekrutierungsinstrument bei prominenten Cyberkriminellen-Gruppen dienen“, sagt Christopher Budd, Direktor für Bedrohungsforschung bei Sophos.

Früher eher harmlos, heute geht es ums große Geld

Dass auf kriminellen Foren Wettbewerbe ausgerichtet werden, ist nichts Neues, die Praxis existiert schon seit Jahren. Interessant ist jedoch, wie sie sich im Laufe der Zeit weiterentwickelt haben. Frühe Aktionen umfassten Quizfragen, Grafikdesign-Wettbewerbe und Ratespiele. Jetzt laden kriminelle Foren dazu ein, Artikel zu technischen Themen einzureichen, inklusive Quellcode, Videos und/oder Screenshots. Die gesammelten Werke werden anschließend von den Forennutzern bewertet und so der Sieger ermittelt. Die Bewertung ist jedoch nicht völlig transparent, da die Forenbesitzer und Wettbewerbssponsoren scheinbar spezielle Stimmrechte haben.

„Während unsere Forschungen eine verstärkte Konzentration der Cyberkriminalität auf Web-3-bezogene Themen wie Kryptowährungen oder NFTs zeigt, hatten viele der siegreichen Einreichungen im Rahmen der Contests dagegen eine breitere Anwendung. Sie zeichneten sich dadurch aus, dass sie quasi umgehend einsetzbar sein würden und zudem oftmals nicht besonders innovativ waren. Dies könnte entweder die Prioritäten der Gemeinschaft offenlegen, oder auch Beleg dafür sein, dass Angreifer ihre besten Forschungsergebnisse für sich behalten wollen, um sich nicht in die Karten schauen zu lassen und ihre neuen Taktiken dann in realen Angriffen profitabel einzusetzen,“ so Christopher Budd weiter.

Sophos hat zwei Wettbewerbe genauer untersucht
Sophos X-Ops hat zwei prominente, jährliche Wettbewerbe untersucht: zum einen eine Veranstaltungsreihe auf dem russischsprachigen Cyberkriminalitätsforum Exploit mit einer Preissumme von 80.000 US-Dollar aus dem Jahr 2021, sowie einer weiteren Serie im sogenannten XSS-Forum. Hier stand 2022 ein Preisgeld von 40.000 Dollar zur Verfügung. Seit mehreren Jahren haben prominente Mitglieder der Cyberkriminalitätsgemeinschaft diese Veranstaltungen gesponsert, darunter All World Cards und Lockbit.

In den jüngsten Wettbewerben konzentrierte Exploit seinen Ausschreibungen auf Kryptowährungen, während XSS sich auf verschiedene Themen von sozialer Manipulation und Angriffsvektoren bis hin zu Ausweichmethoden und Betrugsangeboten konzentriert hat. Viele der Gewinnerbeiträge konzentrierten sich darauf, legitime Tools wie Cobalt Strike zu missbrauchen. Ein Zweitplatzierter teilte ein Tutorial zur Ausrichtung von Initial Coin Offerings (ICOs), um Mittel für eine neue Kryptowährung zu sammeln, und ein weiteres zur Manipulation von Privilegien, um den Windows Defender zu deaktivieren.

Die ganze Untersuchung können Sie unter folgendem Link nachlesen: https://news.sophos.com/en-us/2023/08/29/for-the-win-offensive-research-contests-on-criminal-forums/

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

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