Eksperci łączą atak na firmę SolarWinds z backdoorem Kazuar

ID artykułu: 60977 / 2264

URL: http://www.publikuj.org/60977

W połowie grudnia 2020 r. firmy FireEye, Microsoft oraz SolarWinds poinformowały o wykryciu dużego, wyrafinowanego ataku na łańcuch dostaw, w którym wykorzystano nieznane wcześniej szkodliwe oprogramowanie Sunburst i którego ofiarą padli klienci oprogramowania Orion firmy SolarWinds. Eksperci z firmy Kaspersky zidentyfikowali różne podobieństwa w kodzie pomiędzy szkodnikiem Sunburst oraz znanymi wersjami backdoora Kazuar, zapewniającego atakującym zdalny dostęp do urządzeń ofiar. Nowe ustalenia ujawniają szczegóły, które mogą pomóc badaczom w dochodzeniach związanych z tym atakiem. Badając backdoora wykorzystanego przez szkodnika Sunburst, eksperci z firmy Kaspersky odkryli wiele cech wspólnych ze szkodnikiem Kazuar, który został wcześniej zidentyfikowany jako backdoor napisany przy użyciu platformy .NET Framework. Po raz pierwszy poinformowała o nim firma Palo Alto w 2017 r., a sam szkodnik był wykorzystywany w atakach cyberszpiegowskich na całym świecie. Liczne podobieństwa w kodzie sugerują związek pomiędzy Kazuarem oraz Sunburstem, aczkolwiek charakter powiązania nie został jeszcze określony.

Szkodniki łączy m.in. algorytm generowania identyfikatorów użytkownika (UID) odnoszących się do ofiar, podobieństwa w kodzie odpowiadającym za pozostawanie szkodnika w uśpieniu w pierwszej fazie ataku oraz intensywne wykorzystywanie funkcji skrótu FNV1a. Po pojawieniu się szkodnika Sunburst w lutym 2020 r. Kazuar ciągle ewoluował i podobieństwa obserwowane w jego wersjach z późniejszej części ubiegłego są jeszcze większe.

Eksperci z firmy Kaspersky zaobserwowali ciągły rozwój szkodnika Kazuar w okresie jego ewolucji, łącznie z pojawianiem się nowych, istotnych funkcji wskazujących na podobieństwo ze szkodnikiem Sunburst. Chociaż podobieństwa te są godne uwagi, mogą one wynikać z kilku przyczyn: Sunburst mógł zostać stworzony przez to samo ugrupowanie co Kazuar; twórcy Sunbursta mogli wykorzystać Kazuara jako inspirację; twórca Kazuara mógł dołączyć do zespołu, który stworzył Sunbursta; lub też ugrupowania stojące za Sunburstem i Kazuarem mogły uzyskać kod źródłowy szkodnika z tego samego źródła.

Zidentyfikowany związek nie wystarczy, aby wskazać sprawcę ataku na firmę SolarWinds, jednak dzięki temu, że rzuca nieco więcej światła, może pomóc badaczom osiągnąć postępy w prowadzonych dochodzeniach. Uważamy, że badacze powinni przyjrzeć się tym podobieństwom i spróbować odkryć nowe fakty dotyczące backdoora Kazuar oraz pochodzenia Sunbursta szkodnika wykorzystanego w ataku na firmę SolarWinds. Pamiętajmy, że w przypadku ataku Wannacry na początku istniało niewiele faktów pozwalających powiązać go z ugrupowaniem Lazarus. Z czasem jednak pojawiło się więcej dowodów. Konieczne są zatem dalsze badania w tym zakresie. Dzięki nim będzie można połączyć wszystkie puzzle powiedział Costin Raiu, dyrektor Globalnego Zespołu ds. Badań i Analiz (GReAT) w firmie Kaspersky.

Dalsze szczegóły techniczne dotyczące podobieństw między szkodnikami Sunburst oraz Kazuar zawiera raport dostępny na stronie https://r.kaspersky.pl/54hZf. Więcej informacji na temat badań firmy Kaspersky dotyczących Sunbursta można znaleźć w tym miejscu, z kolei tutaj można dowiedzieć się, w jaki sposób firma Kaspersky chroni swoich klientów przed tym backdoorem.

Firma Kaspersky zaleca następujące działania pozwalające zapobiec infekcji szkodliwym oprogramowaniem, takim jak backdoor zastosowany w ataku na SolarWinds:

Zapewnij swojemu zespołowi z centrum operacji bezpieczeństwa dostęp do najnowszej analizy zagrożeń. Kaspersky Threat Intelligence Portal zapewnia dostęp do eksperckiej wiedzy firmy Kaspersky, oferując zgromadzone na przestrzeni ponad 20 lat szczegółowe dane dotyczące cyberataków. Darmowy dostęp do wybranych funkcji portalu, które umożliwiają sprawdzenie plików, adresów URL oraz IP, można uzyskać na stronie https://opentip.kaspersky.com.

Organizacje, które chcą prowadzić własne dochodzenia, mogą skorzystać z Kaspersky Threat Attribution Engine. Rozwiązanie to pozwala porównać wykryty szkodliwy kod z bazami szkodliwego oprogramowania i na podstawie podobieństw w kodzie połączyć go ze znanymi cybergangami.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 11/01/21 12:03, odsłony: 53