Eksperci Cisco Talos zidentyfikowali nowe cyberzagrożenie o nazwie "Greatness" oparte na phishingu jako usłudze

Najważniejsze informacje:

- Greatness wykorzystuje funkcje spotykane w najbardziej zaawansowanych ofertach PaaS (Phishing as a Service), takie jak obejście uwierzytelniania wieloskładnikowego (MFA), filtrowanie IP oraz integrację z botami na Telegramie;
- Greatness, wyspecjalizowany jest w atakach phishingowych na zainfekowane elementy Microsoft 365, dostarczając przestępcom kreator załączników i linków, który tworzy przekonujące strony-przynęty służące do logowania. Zawiera on takie funkcje, jak wstępnie wypełniony adres e-mail ofiary oraz wyświetlanie odpowiedniego logo i tła firmy, pobranego z prawdziwej strony logowania Microsoft 365 organizacji docelowej. Dzięki temu Greatness szczególnie dobrze nadaje się do ataków na użytkowników biznesowych;
- Analiza domen będących celem kilku bieżących i przeszłych kampanii ujawniła, że najczęściej atakowane sektory to produkcja, opieka zdrowotna i technologia. Dokładny rozkład ofiar w każdym kraju i sektorze różni się nieznacznie w zależności od celów przestępców;
- Aby korzystać z Greatness, złośliwe podmioty muszą wdrożyć i skonfigurować dostarczony zestaw phishingowy z kluczem API, który pozwala nawet niewykwalifikowanym cyberprzestępcom na łatwe korzystanie z zaawansowanych funkcji usługi. Zestaw phishingowy i API działają jako proxy do systemu uwierzytelniania Microsoft 365, przeprowadzając atak typu "man-in-the-middle" i kradnąc dane uwierzytelniające ofiary lub pliki cookie.

Warszawa, 18 maja 2023 - Nowa usługa phishing-as-a-service (PaaS) o nazwie Greatness została wykryta przez ekspertów Cisco Talos. Wykorzystuje ona funkcje spotykane w najbardziej zaawansowanych ofertach PaaS, takie jak obejście wieloskładnikowego uwierzytelniania (MFA), filtrowanie IP oraz integracja z botami na Telegramie. Zdaniem Cisco Talos, Greatness rozpoczął działalność w połowie 2022 roku.

Ataki z użyciem Greatnessa najczęściej celują w firmy z USA

Greatness był szczególnie popularny w grudniu 2022 roku i marcu 2023 roku. Chociaż każda kampania miała nieco inną lokalizację, zbiorczo ponad 50 proc. wszystkich celów miało siedzibę w USA. Kolejne najczęściej atakowane regiony to Wielka Brytania, Australia, RPA i Kanada.

Greatness został zaprojektowany w celu kompromitowania użytkowników Microsoft 365 i może sprawić, że strony phishingowe będą szczególnie przekonujące i skuteczne we wsparciu ataków na firmy. W oparciu o dane uzyskane przez Cisco Talos, udało się ustalić, że cyberprzestępcy wykorzystujący Greatness celują niemal wyłącznie w przedsiębiorstwa. Analiza organizacji będących celem ataków w kilku kampaniach pokazuje, że najczęściej atakowanym sektorem była produkcja, a następnie opieka zdrowotna, technologia i nieruchomości.

Przebieg ataku

Ofiara otrzymuje złośliwy e-mail, który zazwyczaj zawiera plik HTML jako załącznik. Gdy ofiara otworzy plik HTML, przeglądarka internetowa wykonuje krótki fragment zamaskowanego kodu JavaScript, który nawiązuje połączenie z serwerem atakującego w celu uzyskania kodu HTML strony phishingowej

i wyświetlenia go użytkownikowi w tym samym oknie przeglądarki. Kod ten zawiera zamazany obraz, który przedstawia wirujące koło, udając, że ładuje dokument.

Następnie strona przekierowuje ofiarę na stronę logowania Microsoft 365, zwykle wstępnie wypełnioną adresem e-mail ofiary oraz tłem i logo używanym przez jej firmę. Gdy ofiara podaje swoje hasło, PaaS łączy się z Microsoft 365, podszywa się pod ofiarę i podejmuje próbę logowania. Jeśli używane jest MFA, usługa wyświetli ofierze monit o uwierzytelnienie przy użyciu metody MFA wymaganej przez prawdziwą stronę Microsoft 365 (np. kod SMS, kod połączenia głosowego, powiadomienie push).

Gdy usługa otrzyma autoryzację, będzie nadal podszywać się pod ofiarę za kulisami i dokończy proces logowania, aby zebrać uwierzytelnione pliki cookie sesji. Następnie zostaną one dostarczone do partnera usługi na jego kanale Telegram lub bezpośrednio przez panel internetowy.

Jak organizacje mogą zabezpieczyć się przed Greatness:

- Cisco Secure Endpoint (dawniej AMP for Endpoints) idealnie zapobiega opisanej formie ataków. Secure Endpoint można wypróbować za darmo tutaj.
- Skanowanie stron internetowych Cisco Secure Web Appliance zabezpiecza przed połączeniem się ze złośliwych stron internetowych i wykrywa złośliwe oprogramowanie wykorzystywane w tych atakach.
- Cisco Secure Email (dawniej Cisco Email Security) może blokować złośliwe wiadomości e-mail wysyłane przez cyberprzestępców w trakcie ataków. Secure Email można wypróbować za darmo tutaj.
- Urządzenia Cisco Secure Firewall (dawniej Next-Generation Firewall i Firepower NGFW), takie jak Threat Defense Virtual, Adaptive Security Appliance i Meraki MX mogą wykrywać złośliwą aktywność związaną z tym zagrożeniem.
- Cisco Secure Malware Analytics (Threat Grid) identyfikuje złośliwe kody binarne i wbudowuje ochronę we wszystkie produkty Cisco Secure.
- Umbrella, bezpieczna brama internetowa (SIG) firmy Cisco, blokuje użytkowników przed łączeniem się ze złośliwymi domenami, adresami IP i URL, niezależnie od tego, czy użytkownicy znajdują się w sieci firmowej, czy poza nią. Bezpłatna wersja próbna dostępna jest tutaj.
- Cisco Secure Web Appliance (dawniej Web Security Appliance) automatycznie blokuje potencjalnie niebezpieczne witryny i testuje podejrzane strony, zanim użytkownicy uzyskają do nich dostęp.
- Dodatkowe zabezpieczenia w kontekście konkretnego środowiska i danych o zagrożeniach są dostępne w Firewall Management Center.
- Klienci korzystający z open-source Snort Subscriber Rule Set mogą być na bieżąco, pobierając najnowszy pakiet reguł dostępny do nabycia na stronie Snort.org.

Więcej informacji na temat struktury Greatness oraz szczegóły przykładowego ataku można przeczytać we wpisie na blogu Cisco Talos.

.:|:.:|:.

O Cisco: