Paweł Zawadzki

Akademia Sztuki Wojennej

Mustang Panda – modus operandi

Wstęp

Mustang Panda, znana również jako Red Delta, TA416 czy Bronze President, to chińska grupa cyberzagrożeń klasyfikowana jako zaawansowane trwałe zagrożenie (APT). Mustang Panda został po raz pierwszy zaobserwowany w 2017 roku, ale prawdopodobnie prowadzi działania szpiegowskie co najmniej od 2014 roku. Mustang Panda atakował podmioty rządowe, organizacje non-profit, religijne i inne organizacje pozarządowe w UE, USA, Niemczech, Mongolii, Mjanmie, Pakistanie i Wietnamie, od końca 2021 r., do początku 2022 r. Mustang Panda wykorzystuje zarówno zastrzeżone, jak i publicznie dostępne narzędzia hackerskie. Mustang Panda wykorzystuje kilka różnych metod początkowego dostępu, w tym spear-phishing z użyciem złośliwych załączników lub linków, ataki typu watering hole i zainfekowane dyski USB[1].

Operacje realizowane przez Mustang Panda poprzedzone są wysyłką e-maili, celem wzbudzenia zainteresowania i otwarcia pliku przez pracowników ambasady i konsulatów. Otwarcie pliku powoduje przeniesienie do fikcyjnej strony internetowej. W tym celu atrybucja adresów email stwarza przeświadczenie o źródle budzącym zaufanie. Ponadto używa się skrzynek email należących do osób związanych z dyplomacją. Treść takiej wiadomości niejednokrotnie zawiera zaproszenie na raut, prośbę o spotkanie z ambasadorem lub ofertą sprzedaży ze zniżką tylko dla dyplomatów. Znane są również przypadki dystrybucji wiadomości ze sprzedażą auta ambasadora z powodu zmiany placówki dyplomatycznej. Po otwarciu takiego ogłoszenia przeglądarka automatycznie

[1] JP-23-01 - Sustained activity by specific threat actors, tructured Cooperation between CERT-EU and ENISA TLP:CLEAR, 15/02/2023, JP-23-01, v1.0.

Zadanie publiczne współfinansowane ze środków otrzymanych w 2024 r. od Ministra Nauki w ramach konkursu „Organizowanie i animowanie działań na rzecz środowiska akademickiego”

pobiera zainfekowany plik. Następnie powyższy plik pobiera wszystkie dane z komputera[2].

Główne metody działania

Ataki spear-phishingowe

Mustang Panda znana jest z używania ukierunkowanych ataków phishingowych jako głównego wektora początkowego dostępu do systemów.

- **Jak działa:** Grupa wysyła e-maile zawierające załączniki złośliwego oprogramowania lub linki do zainfekowanych stron internetowych.
- **Przykład:** Podczas jednej z kampanii wykorzystano dokumenty związane z COVID-19 jako przynęty, co miało na celu zainteresowanie atakowanych aktualnymi wydarzeniami.
- **Cel:** Zdobycie danych logowania, wprowadzenie złośliwego oprogramowania i przejęcie kontroli nad systemem docelowym.

Wykorzystanie narzędzi złośliwego oprogramowania

Grupa stosuje zaawansowane złośliwe oprogramowanie, takie jak PlugX, MQsTTang czy Poison Ivy.

- **PlugX:** Narzędzie umożliwiające zdalny dostęp, wykradanie danych i trwałą obecność w systemie.
- **MQsTTang:** Nowoczesne oprogramowanie pozwalające na komunikację z serwerami dowodzenia i kontroli (C2).
- **Cel:** Eksfiltracja wrażliwych danych, takich jak dokumenty rządowe, dane uwierzytelniające i informacje o infrastrukturze IT.

[2] Analiza zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych RP oraz innych państw NATO w kontekście wybranych ataków hakerskich, Agencja Wywiadu, Ministerstwo Cyfryzacji.

Zadanie publiczne współfinansowane ze środków otrzymanych w 2024 r. od Ministra Nauki w ramach konkursu „Organizowanie i animowanie działań na rzecz środowiska akademickiego”

Maskowanie

Mustang Panda stosuje wybrane techniki, aby uniknąć wykrycia przez systemy zabezpieczające.

- **Ukrywanie plików:** Używanie zaszyfrowanych kanałów do komunikacji i ukrywanie złośliwego kodu w legalnych plikach.
- **Zmiana narzędzi:** Grupa regularnie dostosowuje swoje metody, na przykład używając plików SCR (screensaver) zamiast standardowych archiwów ZIP czy RAR[3].

Podsumowanie

Mustang Panda, chińska grupa cyberzagrożeń (APT), jest uznawana za jedną z najbardziej efektywnych w zakresie cyberszpiegostwa. Jej działania obejmują zaawansowane techniki infiltracji, utrzymywania trwałości w systemach oraz eksfiltracji danych. Grupa celuje w kluczowe organizacje, takie jak ministerstwa obrony, organizacje pozarządowe, placówki edukacyjne, a także firmy prywatne. Jej celem jest zdobywanie wrażliwych informacji o znaczeniu geopolitycznym i gospodarczym. Zdolność do szybkiej adaptacji do nowych środków bezpieczeństwa, takich jak zmiana formatu plików infekujących (np. SCR zamiast ZIP) i stosowanie unikalnych „przynęt", pozwala grupie na utrzymywanie wysokiej skuteczności poprzez złośliwe oprogramowanie, takie jak PlugX, MQsTTang i Poison Ivy, umożliwiające zdalny dostęp, kradzież danych i przejmowanie kontroli nad systemami. Jednym z głównych wektorów ataku są spear-phishingowe e-maile, które często używają tematyki związanej z aktualnymi wydarzeniami, np. COVID-19 czy spotkaniami politycznymi. Dane są wykradane przy użyciu zaszyfrowanych kanałów komunikacyjnych, co utrudnia ich wykrycie przez zespoły bezpieczeństwa. Ponadto Mustang Panda jest wysoce skuteczna w utrzymywaniu długotrwałego dostępu do zainfekowanych systemów. Grupa wykorzystuje mechanizmy maskowania, takie jak ukryte pliki i

[3] Strona internetowa, https://attack.mitre.org/, dostęp dnia: 30.11.2024.

szyfrowanie, aby uniknąć wykrycia. Ponadto korzysta z mechanizmów autostartu i kluczy rejestru systemowego, które zapewniają grupie nieprzerwaną obecność w sieciach docelowych. Mustang Panda jest postrzegana jako organizacja wspierana przez chiński rząd. Dzięki temu grupa ma dostęp do zasobów i ochrony, co dodatkowo zwiększa jej skuteczność operacyjną.

Zadanie publiczne współfinansowane ze środków otrzymanych w 2024 r. od Ministra Nauki w ramach konkursu „Organizowanie i animowanie działań na rzecz środowiska akademickiego”