# 1. Operacja RusticWeb: Złośliwe oprogramowanie oparte na rdzewie

Indyjskie podmioty rządowe i sektor obrony był celem kampanii phishingowej, która jest zaprojektowana w celu zrzucenia złośliwego oprogramowania do zbierania wywiadu.

Działalność, po raz pierwszy wykryta w październiku 2023 r., Została pokrewna operacja RusticWeb przez firmę zajmującą się ochroną Enterprise Seqrite.

„Nowe oparte na rdzy ładowności i zaszyfrowane polecenia PowerShell zostały wykorzystane do wykładania poufnych dokumentów do internetowego silnika serwisowego, zamiast dedykowanego serwera poleceń i kontroli (C2)”-powiedział badacz bezpieczeństwa Sathwik Ram Prakki.

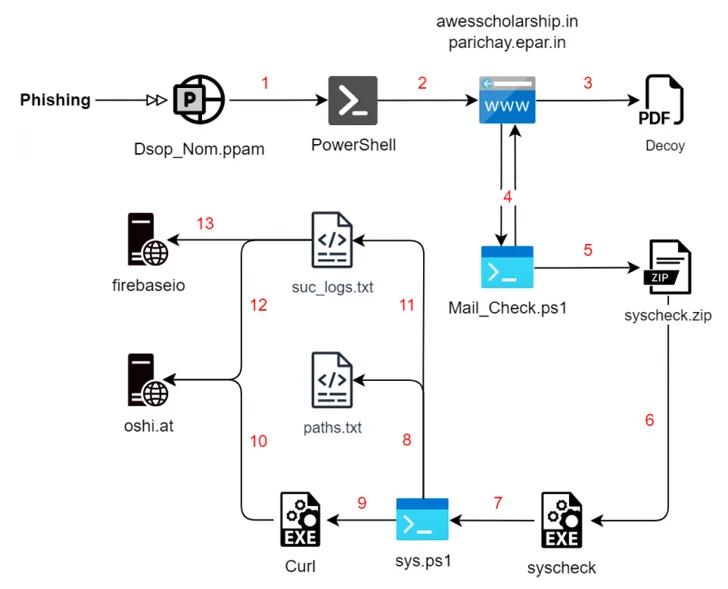
Zakładanie taktyczne zostały odkryte między klastrem a tymi szeroko śledzonymi pod pseudonimem przezroczystego plemienia i boczną, z których oba są oceniane jako powiązane z Pakistanem.

Sidecopia jest również podejrzanym elementem podrzędnym w przezroczystym plemieniu.W ubiegłym miesiącu Seqrite szczegółowo opisał wiele kampanii podjętych przez aktora zagrożenia skierowanego do organów rządowych indyjskich w celu dostarczenia licznych trojanów, takich jak Alakore Rat, Ares Rat i Drat.

Inne ostatnie łańcuchy ataku udokumentowane przez GroundMon wykorzystały pliki Microsoft Microsoft PowerPoint, a także specjalnie wykonane archiwa RAR podatne na CVE-2013-38831 w celu dostarczania złośliwego oprogramowania, umożliwiając nieokiełznany zdalny dostęp i kontrolę.

„Łańcuch infekcji grupy SideCopy APT obejmuje wiele kroków, z których każdy starannie zorganizował, aby zapewnić pomyślny kompromis” - zauważył Groundmon na początku tego roku.

Najnowszy zestaw ataków rozpoczyna się e-mailem phishingowym, wykorzystując techniki inżynierii społecznej w celu oszczędzania ofiar w interakcji ze złośliwymi plikami PDF, które zrzucają ładunki oparte na rdzy w celu wyliczenia systemu plików w tle, jednocześnie wyświetlając plik wabiki.



Oprócz gromadzenia interesujących plików, złośliwe oprogramowanie jest przygotowane do gromadzenia informacji o systemie i przesyłania ich na serwer C2, ale brakuje mu funkcji innych zaawansowanych złośliwych oprogramowania do złośliwego kradzieży dostępnych w podziemnym cyberprzestępczości.

Drugi łańcuch infekcji zidentyfikowany przez SEQRITE w grudniu wykorzystuje podobny wieloetapowy proces, ale zastępuje złośliwe oprogramowanie rdzy skryptem PowerShell, który zajmuje się etapami wyliczenia i exfiltracji.

Ale w ciekawym akcentie końcowy ładunek jest uruchamiany za pomocą wykonywalny rdzy, który ma nazwę „Cisco AnyConnect Web Helper”.Zebrane informacje są ostatecznie przesyłane do Oshi [.] W Domain, anonimowy publiczny silnik udostępniania plików o nazwie OSHIUPLOOD.

„Operacja Rusticweb może być powiązana z APT zagrożeniem, ponieważ dzieli podobieństwa z różnymi grupami powiązanymi z Pakistanem”-powiedział Ram Prakki.

Ujawnienie pojawia się prawie dwa miesiące po tym, jak Cyble odkrył złośliwą aplikację na Androida wykorzystywaną przez zespół Donot skierowany do osób w regionie Kaszmiru w Indiach.

Uważa się, że aktor państwa narodowego, znany również pod nazwami APT-C-35, słonia origami i sektor02 i ma historię wykorzystywania złośliwego oprogramowania Androida do infiltracji urządzeń należących do ludzi w Kaszmirze i Pakistanie.

Wariant zbadany przez Cyble to trojanizowana wersja projektu Github o nazwie „Quranapp: Read and Explore”, który jest wyposażony w szeroką gamę funkcji oprogramowania szpiegowskim do rejestrowania połączeń audio i VOIP, przechwytywania zrzutów ekranu, gromadzenia danych z różnych aplikacji,Pobierz dodatkowe pliki APK i śledź lokalizację ofiary.

„Nieustanne wysiłki grupy Donot, aby udoskonalić swoje narzędzia i techniki, podkreślają ciągłe zagrożenie, jakie stwarzają, szczególnie w zakresie celowania osób w wrażliwym regionie Kaszmiru w Indiach” - powiedział Cyble.

Link: <https://thehackernews.com/2023/12/operation-rusticweb-rust-based-malware.html>

# 2. Członkowie nastolatków British Lapsus $ skazani za głośne ataki

Dwa nastolatki brytyjskie w Lapsus $ Cyberprzestępczości i gangu wymuszenia zostały skazane za swoje role w organizowaniu szeregu głośnych ataków na wiele firm.

ARION KURTAJ, 18-latek z Oksfordu, został skazany na nieokreślony nakaz szpitala ze względu na zamiar powrotu do cyberprzestępczości „jak najszybciej”, donosi BBC.Kurtaj, który jest autystyczny, został uznany za niezdolnego do postawienia procesu.

Inny członek Lapsus $, 17-letni nienazwany nieletni, został skazany na 18-miesięczny nakaz rehabilitacji młodzieży, w tym trzymiesięcznego intensywnego nadzoru i wymogu nadzoru.Został uznany za winnego dwóch przypadków oszustwa, dwóch przestępstw związanych z niewłaściwym użyciem komputera i jednego szantażu.

Obaj oskarżeni zostali początkowo aresztowani w styczniu 2022 r., A następnie zwolnieni w badaniu.Zostali ponownie aresztowani w marcu 2022 r. Podczas gdy Kurtaj otrzymał kaucję, kontynuował atak na różne firmy, dopóki nie został ponownie aresztowany we wrześniu.

Szaleństwo ataku, które odbyło się między sierpniem 2020 r. Do września 2022 r., Kierowane BT, EE, Globant, LG, Microsoft, Nvidia, Okta, Revolut, Rockstar Games, Samsung, Ubisoft, Uber i Vodafone.

Mówi się, że Lapsus $ obejmuje członków z Wielkiej Brytanii i Brazylii.Trzeci członek grupy, również podejrzany o nastolatkę, został aresztowany w kraju Ameryki Południowej w październiku 2022 r.

Raport opublikowany przez Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) Cyber Safety Review Rad (CSRB) w tym roku ujawnił wykorzystanie przez aktora zagrożonego ataków w celu przejęcia rachunków ofiar i infiltruj sieci docelowe.Wykorzystał również kanał telegramowy do opublikowania jego działalności i wymuszenia ofiar.

W ciągu ostatniego roku rozgłos przyciągany przez Lapsus $ doprowadził również do pojawienia się innej grupy o nazwie Scrested Spider.Obie grupy są częścią większej jednostki, która nazywa się komunikatem.

Według Federalnego Biura Śledczego Comm składa się z „zróżnicowanej geograficznie grupy osób, zorganizowanych w różnych podgrupach, z których wszystkie koordynują poprzez wnioski o komunikację online, takie jak Discord i Telegram”, aby zaangażować się w włamy, prawdziwa przemoc i swatowanie.

„Ta sprawa stanowi przykład niebezpieczeństw, w których młodzi ludzie mogą być przyciągnięci w Internecie i poważne konsekwencje, jakie może mieć w czyjejś szerszej przyszłości” - powiedziała Amanda Horsburgh, kurator detektywu z policji w Londynie.

„Wielu młodych ludzi chce zbadać, jak działa technologia i jakie istnieją luki. Może to obejmować naukę kodowania, interakcję z podobnie myślącymi osobami online i eksperymentowanie z narzędziami. Niestety świat cyfrowy może również kusić młodych ludzi z niewłaściwych powodów. "

Link: <https://thehackernews.com/2023/12/british-lapsus-teen-members-sentenced.html>

# 3. 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”.

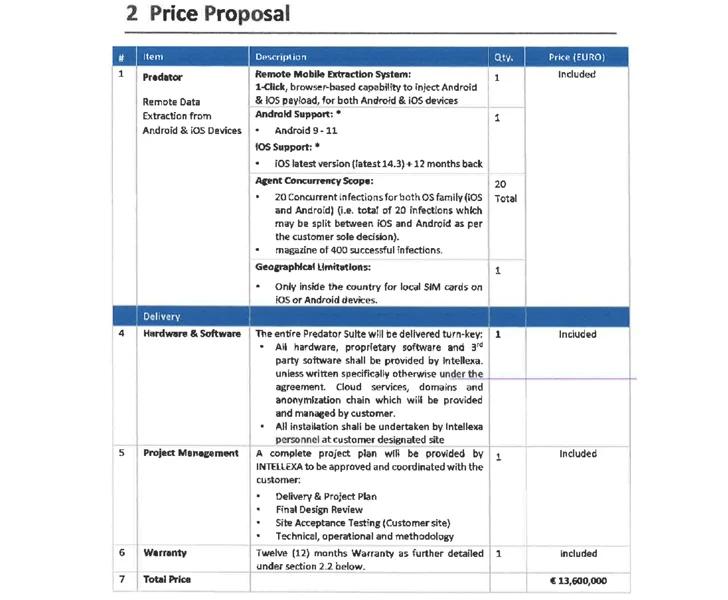
Predator jest produktem konsorcjum o nazwie Intellexa Alliance, które obejmuje Cytrox (następnie nabyty przez Wispear), NEXA Technologies i SenPai Technologies.Zarówno CYTROX, jak i Intellexa zostały dodane do listy jednostek przez USA w lipcu 2023 r. W celu „Handlu w cyberprzestrzeni używanych do uzyskania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

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.

„Potrzebne jest publiczne ujawnienie analiz technicznych mobilnych oprogramowania szpiegowskim i namacalnych próbek umożliwiających publiczne badanie złośliwego oprogramowania. Takie publiczne ujawnienia nie tylko umożliwią większe analizy i napędzają wysiłki wykrywania, ale także nakładać koszty rozwoju dla dostawców, aby stale rozwijać ich implanty. "

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

# 4. 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.

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

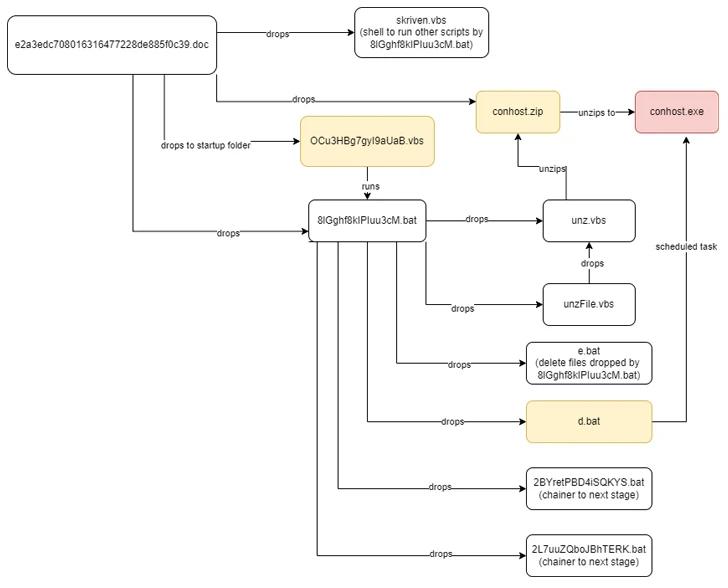
nitc [.] Govnp [.] org

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>