JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

ID produktu: AA24-109A

18 kwietnia 2024 r.

Współautorstwo:

National Cyber Security Centre
Ministry of Security and Justice

#StopRansomware: Akira Ransomware

PODSUMOWANIE

Uwaga: *To wspólne doradztwo w zakresie cyberbezpieczeństwa (CSA) jest częścią trwających działań #StopRansomware mających na celu publikowanie porad dla obrońców sieci, które szczegółowo opisują różne warianty ransomware i podmioty zagrażające ransomware.*
Te porady #StopRansomware obejmują ostatnio i historycznie zaobserwowane taktyki, techniki i procedury (TTP) oraz wskaźniki kompromitacji (IOC), aby pomóc organizacjom chronić się przed oprogramowaniem ransomware. Odwiedź stronę stopransomware.gov, aby zobaczyć wszystkie porady #StopRansomware i dowiedzieć się więcej o innych zagrożeniach ransomware i bezpłatnych zasobach.

Federalne Biuro Śledcze Stanów Zjednoczonych (FBI), Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA), Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) Europolu i Holenderskie Narodowe Centrum Cyberbezpieczeństwa (NCSC-NL) publikują niniejszą wspólną ocenę bezpieczeństwa cybernetycznego w celu rozpowszechnienia znanych IOC i TTP oprogramowania ransomware Akira zidentyfikowanych w wyniku dochodzeń FBI przeprowadzonych w lutym 2024 r. oraz raportów zaufanych stron trzecich.

Działania, które należy podjąć już dziś, aby złagodzić cyberzagrożenia ze strony oprogramowania ransomware Akira:

- Priorytetowe usuwanie znanych wykorzystanych luk w zabezpieczeniach.
- Włącz uwierzytelnianie wieloskładnikowe (MFA) dla wszystkich usług w możliwym zakresie, w szczególności dla poczty internetowej, VPN i kont, które uzyskują dostęp do krytycznych systemów.
- Regularne łatanie i aktualizowanie oprogramowania i aplikacji do ich najnowszych wersji oraz przeprowadzanie regularnych ocen podatności na zagrożenia.

Od marca 2023 r. oprogramowanie ransomware Akira miało wpływ na wiele firm i podmiotów infrastruktury krytycznej w Ameryce Północnej, Europie i Australii. W kwietniu 2023 r., po początkowym skupieniu się na systemach Windows, aktorzy zagrożeń Akira wdrożyli wariant Linux atakujący maszyny wirtualne VMware ESXi. Od 1 stycznia 2024 r. grupa ransomware miała wpływ na ponad 250 organizacji i pochłonęła około 42 mln USD wpływów z ransomware.

Wczesne wersje wariantu ransomware Akira zostały napisane w języku C++ i szyfrowały pliki z rozszerzeniem `.akira`; jednak począwszy od sierpnia 2023 r. niektóre ataki Akira zaczęły wdrażać Megazord, wykorzystując kod oparty na Rust, który szyfruje pliki z rozszerzeniem `.powerranges`. Aktorzy zagrożeń Akira nadal używają zamiennie zarówno Megazord, jak i Akira, w tym Akira_v2 (zidentyfikowane przez zaufane dochodzenia stron trzecich).

informacji dotyczących incydentu: data, godzina i lokalizacja incydentu; rodzaj działania; liczba osób dotkniętych incydentem; rodzaj sprzętu użytego do działania; nazwa firmy lub organizacji zgłaszającej; oraz wyznaczony punkt kontaktowy.

FBI, CISA, EC3 i NCSC-NL zachęcają organizacje do wdrożenia zaleceń zawartych w sekcji "Środki zaradcze" niniejszego dokumentu CSA w celu zmniejszenia prawdopodobieństwa i wpływu incydentów związanych z oprogramowaniem ransomware.

SZCZEGÓŁY TECHNICZNE

Uwaga: W niniejszym poradniku wykorzystano platformę MITRE ATT&CK® for Enterprise, wersja 14. Zobacz MITRE ATT&CK for Enterprise dla wszystkich powiązanych taktyk i technik.

Dostęp początkowy

FBI i badacze zajmujący się cyberbezpieczeństwem zaobserwowali, że podmioty stanowiące zagrożenie Akira uzyskują początkowy dostęp do organizacji za pośrednictwem usługi wirtualnej sieci prywatnej (VPN) bez skonfigurowanego uwierzytelniania wieloskładnikowego (MFA)[1], głównie przy użyciu znanych luk w zabezpieczeniach Cisco [T1190] CVE-2020-3259 i CVE-2023-20269[2].[Dodatkowe metody początkowego dostępu obejmują korzystanie z usług zewnętrznych, takich jak Remote Desktop Protocol (RDP) [T1133], spear phishing [T1566.001][T1566.002] oraz nadużywanie ważnych danych uwierzytelniających [T1078][4].

Wytrwałość i odkrywanie

Po uzyskaniu początkowego dostępu aktorzy zagrożeń Akira próbują nadużywać funkcji kontrolerów domeny, tworząc nowe konta domeny [T1136.002] w celu ustanowienia trwałości. W niektórych przypadkach FBI zidentyfikowało aktorów zagrożeń Akira tworzących konto administracyjne o nazwie `itadm`.

Według doniesień FBI i open source, aktorzy zagrożeń Akira wykorzystują techniki ataku po eksploitacji, takie jak Kerberoasting[5], w celu wyodrębnienia danych uwierzytelniających przechowywanych w pamięci procesu usługi Local Security Authority Subsystem Service (LSASS) [T1003.001].[6] Aktorzy zagrożeń Akira używają również narzędzi do skrobania danych uwierzytelniających [T1003], takich jak Mimikatz i LaZagne, aby pomóc w eskalacji uprawnień. Narzędzia takie jak SoftPerfect i Advanced IP Scanner są często używane do wykrywania urządzeń sieciowych (rekonesansu) [T1016], a polecenia `Net` Windows są używane do identyfikacji kontrolerów domeny [T1018] i zbierania informacji o relacjach zaufania domeny [T1482].

Opisowa lista tych narzędzi znajduje się w tabeli 1.

Unikanie obrony

W oparciu o badania przeprowadzone przez zaufane strony trzecie, zaobserwowano, że podmioty zagrażające Akira wdrażają dwa różne warianty oprogramowania ransomware przeciwko różnym architekturom systemu w ramach tego samego zdarzenia naruszającego bezpieczeństwo. Oznacza to zmianę w stosunku do niedawno zgłoszonej aktywności podmiotów stowarzyszonych Akira. Aktorzy zagrożeń Akira po raz pierwszy zaobserwowali wdrażanie specyficznego dla systemu Windows oprogramowania ransomware "Megazord", a dalsza analiza ujawniła, że drugi ładunek został jednocześnie wdrożony w tym ataku (który został później zidentyfikowany jako nowy wariant szyfratora Akira ESXi, "Akira_v2").

Gdy aktorzy zagrożeń Akira przygotowują się do ruchu bocznego, zwykle wyłączają oprogramowanie zabezpieczające, aby uniknąć wykrycia. Badacze cyberbezpieczeństwa zaobserwowali, że aktorzy

zagrożeń Akira używają PowerTool do wykorzystania sterownika Zemana AntiMalware[4] i zakończenia procesów związanych z oprogramowaniem antywirusowym [T1562.001].

Eksfiltracja i wpływ

Aktorzy zagrożeń Akira wykorzystują narzędzia takie jak FileZilla, WinRAR [T1560.001], WinSCP i RClone do eksfiltracji danych [T1048]. Aby ustanowić kanały dowodzenia i kontroli, aktorzy zagrożeń wykorzystują łatwo dostępne narzędzia, takie jak AnyDesk, MobaXterm, RustDesk, Ngrok i Cloudflare Tunnel, umożliwiając eksfiltrację za pośrednictwem różnych protokołów, takich jak File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP) i usługi przechowywania w chmurze, takie jak Mega [T1537], aby połączyć się z serwerami eksfiltracji.

Aktorzy zagrożeń Akira wykorzystują model podwójnego wymuszenia [T1657] i szyfrują systemy [T1486] po eksfiltracji danych. Nota o okupie Akira zapewnia każdej firmie unikalny kod i instrukcje, aby skontaktować się z aktorami zagrożeń za pośrednictwem adresu URL `.onion`. Aktorzy zagrożeń Akira nie pozostawiają początkowego żądania okupu ani instrukcji dotyczących płatności w zaatakowanych sieciach i nie przekazują tych informacji, dopóki ofiara się z nimi nie skontaktuje. Okup jest płacony w Bitcoinach na adresy portfeli kryptowalutowych podane przez aktorów. Aby jeszcze bardziej wywrzeć presję, aktorzy zagrożeń Akira grożą opublikowaniem eksfiltrowanych danych w sieci Tor, a w niektórych przypadkach dzwonili do poszkodowanych firm, zgodnie z raportami FBI.

Szyfrowanie

Aktorzy zagrożeń Akira wykorzystują wyrafinowany hybrydowy schemat szyfrowania do blokowania danych. Obejmuje to połączenie szyfru strumieniowego ChaCha20 z kryptosystemem klucza publicznego RSA w celu zapewnienia szybkości i bezpiecznej wymiany kluczy [T1486]. To wielowarstwowe podejście dostosowuje metody szyfrowania w oparciu o typ i rozmiar pliku i jest zdolne do pełnego lub częściowego szyfrowania. Zaszyfrowane pliki są dołączane z rozszerzeniem `.akira` lub `.powerranges`. Aby jeszcze bardziej utrudnić odzyskanie systemu, szyfrator Akiry (`w.exe`) wykorzystuje polecenia PowerShell do usuwania kopii w tle woluminów (VSS) w systemach Windows [T1490]. Dodatkowo, nota okupu o nazwie `fn.txt` pojawia się zarówno w katalogu głównym (`C:`), jak i katalogu domowym każdego użytkownika (`C:\Users`).

Analiza przeprowadzona przez zaufaną stronę trzecią wykazała, że szyfrator Akira_v2 jest aktualizacją poprzedniej wersji, która zawiera dodatkowe funkcje ze względu na język, w którym została napisana (Rust). Poprzednie wersje szyfratora zapewniały opcje dołączania argumentów w czasie wykonywania, które obejmowały:

- `-p --encryption_path (docelowa ścieżka pliku/folderu)`
- `-s --share_file (ścieżka docelowego dysku sieciowego)`
- `-n --encryption_percent (procent szyfrowania)`
- `--fork (utworzenie procesu potomnego dla szyfrowania)`

Dodatkowe włączenie wątków pozwala aktorowi na bardziej szczegółową kontrolę nad liczbą używanych rdzeni procesora, zwiększając szybkość i wydajność procesu szyfrowania. Nowa wersja dodaje również warstwę ochrony, wykorzystując identyfikator kompilacji jako warunek uruchomienia, aby utrudnić dynamiczną analizę.
Enkoder nie jest w stanie pomyślnie uruchomić się bez określonego unikalnego identyfikatora kompilacji. Zaobserwowano również możliwość wdrożenia tylko na maszynach wirtualnych przy użyciu funkcji "`vmonly`" oraz możliwość zatrzymania uruchomionych maszyn wirtualnych za

pomocą funkcji "stopvm" dla Akira_v2. Po zaszyfrowaniu wariant Linux ESXi może zawierać rozszerzenie pliku "akiranew" lub dodany plik o nazwie "akiranew.txt" jako notatkę o okupie w katalogach, w których pliki zostały zaszyfrowane przy użyciu nowej nomenklatury.

Narzędzia lewarowane

Tabela 1 zawiera listę publicznie dostępnych narzędzi i aplikacji, z których korzystali aktorzy zagrożeń Akira, w tym legalnych narzędzi zmienionych na potrzeby ich operacji. Korzystanie z tych narzędzi i aplikacji nie powinno być przypisywane jako złośliwe bez dowodów analitycznych potwierdzających wykorzystanie i/lub kontrolę przez podmioty stanowiące zagrożenie.

Tabela 1: Narzędzia wykorzystywane przez aktorów Akira Ransomware

Nazwa	Opis
AdFind	`AdFind.exe` służy do odpytywania i pobierania informacji z Active Directory.
Zaawansowany skaner IP	Skaner sieciowy służy do lokalizowania wszystkich komputerów w sieci i skanowania ich portów. Program pokazuje wszystkie urządzenia sieciowe, zapewnia dostęp do folderów współdzielonych i umożliwia zdalne sterowanie komputerami (przez RDP i Radmin).
AnyDesk	Powszechne oprogramowanie, które może być złośliwie wykorzystywane przez podmioty stanowiące zagrożenie w celu uzyskania zdalnego dostępu i utrzymania trwałości [T1219]. AnyDesk obsługuje również zdalny transfer plików.
LaZagne	Umożliwia użytkownikom odzyskiwanie zapisanych haseł w systemach Windows, Linux i OSX.
PCHunter64	Narzędzie służące do pozyskiwania szczegółowych informacji o procesach i systemach [T1082].[7]
PowerShell	Wieloplatformowe rozwiązanie do automatyzacji zadań składające się z powłoki wiersza poleceń, języka skryptowego i struktury zarządzania konfiguracją, które działa w systemach Windows, Linux i macOS.
Mimikatz	Umożliwia użytkownikom przeglądanie i zapisywanie danych uwierzytelniających, takich jak bilety Kerberos.
Ngrok	Narzędzie reverse proxy [T1090] używane do tworzenia bezpiecznego tunelu do serwerów za zaporami ogniowymi lub lokalnych maszyn bez publicznego adresu IP.
RClone	Program wiersza poleceń służący do synchronizacji plików z usługami przechowywania w chmurze [T1567.002], takimi jak Mega.
SoftPerfect	Skaner sieciowy (`netscan.exe`) służący do pingowania komputerów, skanowania portów, wykrywania udostępnionych folderów i pobierania informacji o urządzeniach sieciowych za pośrednictwem Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) i PowerShell. Skanuje również w poszukiwaniu zdalnych usług, rejestru, plików i liczników wydajności.
WinRAR	Służy do dzielenia zainfekowanych danych na segmenty i kompresji plików [T1560.001] do formatu `.RAR` w celu eksfiltracji.

WinSCP	Windows Secure Copy to darmowy i otwarty klient protokołu transferu plików SSH, protokołu transferu plików, WebDAV, Amazon S3 i protokołu bezpiecznego kopiowania. Aktorzy zagrożeń Akira używali go do przesyłania danych [T1048] z zainfekowanej sieci na konta kontrolowane przez aktorów.

Wskaźniki kompromisu

Zastrzeżenie: Przed podjęciem działań, takich jak blokowanie, zaleca się zbadanie lub weryfikację tych wskaźników.

Tabela 2: Złośliwe pliki powiązane z Akira Ransomware

Nazwa pliku	Hash (SHA-256)	Opis
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca	Oprogramowanie ransomware Akira
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e	Szyfrator ransomware Akira
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138	Aplikacja pulpitu zdalnego
Gcapi.dll	73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf	Plik DLL, który pomaga w wykonaniu AnyDesk.exe
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386	Narzędzie Ngrok dla trwałości
Config.yml	Zależy od zastosowania	Plik konfiguracyjny Ngrok
Rclone.exe	aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9	Narzędzie do eksfiltracji
Winscp.rnd	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4	Program do przesyłania plików w sieci
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c	Program do przesyłania plików w sieci
Akira_v2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f750ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c	Akira_v2 ransomware
Megazord	ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fcdfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07	Oprogramowanie ransomware Akira "Megazord"

Nazwa pliku	Hash (SHA-256)	Opis
	9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d0652f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c837f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0	
VeeamHax.exe	aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d	Narzędzie do wycieku danych uwierzytelniających w postaci zwykłego tekstu
Veeam-Get-Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88	Skrypt PowerShell do uzyskiwania i odszyfrowywania kont Veeam serwery
PowershellKerberos TicketDumper	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32	Narzędzie do zrzucania biletów Kerberos z pamięci podręcznej LSA
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694	Backdoor OpenSSH
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694	Backdoor OpenSSH
ipscan-3.9.1-setup.exe	892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0	Skaner sieciowy skanujący adres IP adresy i porty
Nazwa pliku	**Hash (MD5)**	**Opis**
winrar-x64-623.exe	7a647af3c112ad805296a22b2a276e7c	Program do przesyłania plików w sieci

Tabela 3: Polecenia powiązane z oprogramowaniem Akira Ransomware

Wytrwałość i odkrywanie
nltest /dclist: [T1018]
nltest /DOMAIN_TRUSTS [T1482]
net group "Domain admins" /dom [T1069.002]
net localgroup "Administrators" /dom [T1069.001]
lista zadań [T1057]
rundll32.exe c:\Windows\System32\comsvcs.dll, MiniDump ((Get-Process lsass).Id) C:\windows\temp\lsass.dmp full [T1003.001].
Dostęp do poświadczeń
cmd.exe /Q /c esentutl.exe /y "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.default-release\key4.db" /d "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.default-release\key4.db.tmp" **Uwaga:** Służy do uzyskiwania dostępu do danych Firefox.
cmd.exe /Q /c esentutl.exe /y "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data" /d "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data.tmp" **Uwaga:** Służy do uzyskiwania dostępu do danych Google Chrome.
Wpływ
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject" [T1490].

TAKTYKI I TECHNIKI ATAKÓW MITRE

W tabelach 4-12 znajdują się wszystkie przywołane w tym poradniku taktyki i techniki aktorów zagrożeń Akira dla środowisk korporacyjnych. Aby uzyskać pomoc w mapowaniu złośliwej aktywności cybernetycznej do ram MITRE ATT&CK, zobacz Najlepsze praktyki CISA i MITRE ATT&CK dotyczące mapowania MITRE ATT&CK oraz narzędzie CISA Decider Tool.

Tabela 4: Dostęp początkowy

Tytuł techniki	ID	Użycie
Ważne konta	T1078	Aktorzy zagrożeń Akira uzyskują i nadużywają poświadczenia istniejących kont jako sposób na uzyskanie początkowego dostępu.

Tytuł techniki	ID	Użycie
Wykorzystaj aplikację publiczną	T1190	Aktorzy zagrożeń Akira wykorzystują luki w systemach internetowych w celu uzyskania dostępu do systemów.
Zewnętrzne usługi zdalne	T1133	Aktorzy zagrożeń Akira wykorzystali zdalne usługi dostępu, takie jak połączenie RDP/VPN w celu uzyskania początkowego dostępu.
Phishing: Załącznik wyłudzający informacje	T1566.001	Aktorzy zagrożeń Akira wykorzystują phishing wiadomości e-mail ze złośliwymi załącznikami w celu uzyskania dostępu do sieci.
Phishing: Łącze spearphishingowe	T1566.002	Aktorzy zagrożeń Akira wykorzystują phishing wiadomości e-mail ze złośliwymi linkami w celu uzyskania dostępu do sieci.

Tabela 5: Dostęp do poświadczeń

Tytuł techniki	ID	Użycie
Zrzucanie poświadczeń systemu operacyjnego	T1003	Aktorzy zagrożeń Akira używają narzędzi takich jak Mimikatz i LaZagne do wyrzucenia poświadczeń.
Zrzucanie danych uwierzytelniających systemu operacyjnego: Pamięć LSASS	T1003.001	Aktorzy zagrożeń Akira próbują uzyskać dostęp do materiał uwierzytelniający przechowywany w pamięci procesowej systemu LSASS.

Tabela 6: Odkrycie

Tytuł techniki	ID	Użycie
Wykrywanie konfiguracji sieci systemowej	T1016	Aktorzy zagrożeń Akira używają narzędzi do skanowania systemów i identyfikowania usług działających na zdalnych hostach i w sieci lokalnej. infrastruktura.
Wykrywanie informacji o systemie	T1082	Aktorzy zagrożeń Akira używają narzędzi takich jak PCHunter64 do uzyskiwania szczegółowych informacji o procesach i systemie.

Wykrywanie zaufania do domeny	T1482	Aktorzy zagrożeń Akira używają polecenia net Windows do wyliczania informacje o domenie.
Odkrywanie procesów	T1057	Aktorzy zagrożeń Akira korzystają z listy zadań aby uzyskać szczegółowe informacje na temat uruchomionych procesów za pośrednictwem PowerShell.

Tytuł techniki	ID	Użycie
Wykrywanie grup uprawnień: Grupy lokalne	T1069.001	Aktorzy zagrożeń Akira używają `net localgroup /dom`, aby znaleźć system lokalny grupy i ustawienia uprawnień.
Wykrywanie grup uprawnień: Grupy domen	T1069.002	Aktorzy zagrożeń Akira korzystają z `grupy sieciowej` polecenie `/domain`, aby spróbować znaleźć grupy na poziomie domeny i ustawienia uprawnień.
Zdalne wykrywanie systemu	T1018	Aktorzy zagrożeń Akira używają `nltest /dclist` do gromadzenia listy innych systemów według adresu IP, nazwy hosta lub inne identyfikatory logiczne w sieci.

Tabela 7: Trwałość

Tytuł techniki	ID	Użycie
Utwórz konto: Konto domeny	T1136.002	Aktorzy zagrożeń Akira próbują nadużywać funkcji kontrolerów domeny, tworząc nowe konta domeny w celu ustanowić wytrwałość.

Tabela 8: Unikanie obrony

Tytuł techniki	ID	Użycie
Uszkodzenie obrony: Wyłączenie lub Modyfikacja narzędzi	T1562.001	Aktorzy zagrożeń Akira używają BYOVD ataków w celu wyłączenia oprogramowania antywirusowego.

Tabela 9: Dowodzenie i kontrola

Tytuł techniki	ID	Użycie
Oprogramowanie do zdalnego dostępu	T1219	Aktorzy zagrożeń Akira używają legalnego oprogramowania do obsługi pulpitu, takiego jak AnyDesk, aby uzyskać zdalny dostęp do systemy ofiar.
Pełnomocnik	T1090	Aktorzy zagrożeń Akira wykorzystali Ngrok do utworzenie bezpiecznego tunelu do serwerów, który pomagał w eksfiltracji

		danych.

Tabela 10: Kolekcja

Tytuł techniki	ID	Użycie
Zebrane dane archiwalne: Archiwum za pośrednictwem Utility	T1560.001	Aktorzy zagrożeń Akira używają narzędzi takich jak WinRAR do kompresji plików.

Tabela 11: Eksfiltracja

Tytuł techniki	ID	Użycie
Eksfiltracja przez alternatywę Protokół	T1048	Aktorzy zagrożeń Akira wykorzystują transfer plików narzędzia takie jak WinSCP do przesyłania danych.
Przesyłanie danych na konto w chmurze	T1537	Aktorzy zagrożeń Akira używają narzędzi takich jak CloudZilla do eksfiltracji danych na konto w chmurze i łączenia się z serwerami eksfiltracji kontrolują.
Eksfiltracja przez usługę sieciową: Eksfiltracja do pamięci masowej w chmurze	T1567.002	Aktorzy zagrożenia Akira wykorzystali RClone do synchronizacji plików z pamięcią masową w chmurze usługi eksfiltracji danych.

Tabela 12: Wpływ

Tytuł techniki	ID	Użycie
Data zaszyfrowana dla wpływu	T1486	Aktorzy zagrożeń Akira szyfrują dane na systemy docelowe, aby przerwać dostępność do zasobów systemowych i sieciowych.
Hamowanie odzyskiwania systemu	T1490	Aktorzy zagrożenia Akira usuwają wolumin shadow copies w systemach Windows.
Kradzież finansowa	T1657	Aktorzy zagrożenia Akira używają podwójnego model wymuszeń w celu uzyskania korzyści finansowych.

ŚRODKI ZARADCZE

Obrońcy sieci

FBI, CISA, EC3 i NCSC-NL zalecają organizacjom zastosowanie następujących środków zaradczych w celu ograniczenia potencjalnego wykorzystania przez przeciwników powszechnych technik wykrywania systemów i sieci oraz zmniejszenia ryzyka kompromitacji przez oprogramowanie ransomware Akira. Te środki zaradcze są zgodne z międzysektorowymi celami w zakresie cyberbezpieczeństwa (CPG) opracowanymi przez CISA i National Institute of Standards and Technology (NIST). CPG zapewniają minimalny zestaw praktyk i zabezpieczeń, które CISA i NIST zalecają wszystkim organizacjom. CISA i NIST oparły CPG na istniejących ramach cyberbezpieczeństwa i wytycznych w celu ochrony przed najczęstszymi i najbardziej wpływowymi zagrożeniami i TTP. Odwiedź stronę CISA's Cross-Sector Cybersecurity Performance Goals, aby uzyskać więcej informacji na temat CPGs, w tym dodatkowe zalecane zabezpieczenia podstawowe.

- **Wdrożenie planu odzyskiwania danych** w celu utrzymania i przechowywania wielu kopii wrażliwych lub zastrzeżonych danych i serwerów w fizycznie oddzielonej, podzielonej na segmenty i bezpiecznej lokalizacji (np. dysk twardy, urządzenie pamięci masowej, chmura) [CPG 2.F, 2.R, 2.S].
- **Wymaganie,** aby **wszystkie konta** z loginami na hasło (np. konta usług, konta administratorów i konta administratorów domeny) były zgodne ze standardami NIST. W szczególności należy wymagać od pracowników

używać długich haseł i rozważyć niewymaganie powtarzających się zmian haseł, ponieważ może to osłabić bezpieczeństwo [CPG 2.C].

- **Wymagaj uwierzytelniania wieloskładnikowego** dla wszystkich usług w możliwym zakresie, w szczególności dla poczty internetowej, wirtualnych sieci prywatnych i kont, które uzyskują dostęp do krytycznych systemów [CPG 2.H].
- **Aktualizuj wszystkie systemy operacyjne, oprogramowanie i firmware.** Terminowe łatanie jest jednym z najbardziej wydajnych i opłacalnych kroków, jakie organizacja może podjąć w celu zminimalizowania narażenia na zagrożenia cybernetyczne. Priorytetowo traktuj łatanie znanych luk w zabezpieczeniach w systemach mających dostęp do Internetu. [CPG 1.E].
- **Segmentacja sieci** w celu zapobiegania rozprzestrzenianiu się oprogramowania ransomware. Segmentacja sieci może pomóc w zapobieganiu rozprzestrzenianiu się oprogramowania ransomware poprzez kontrolowanie przepływów ruchu między różnymi podsieciami i dostępu do nich oraz poprzez ograniczanie bocznego ruchu przeciwnika [CPG 2.F].
- **Zidentyfikować, wykryć i zbadać nietypową aktywność i potencjalne przejście wskazanego oprogramowania ransomware za pomocą narzędzia do monitorowania sieci.** Aby pomóc w wykryciu oprogramowania ransomware, należy wdrożyć narzędzie, które rejestruje i raportuje cały ruch sieciowy, w tym aktywność ruchów bocznych w sieci. Narzędzia do wykrywania i reagowania w punktach końcowych (EDR) są szczególnie przydatne do wykrywania połączeń bocznych, ponieważ mają wgląd w typowe i nietypowe połączenia sieciowe dla każdego hosta [CPG 3.A].
- **Filtrowanie ruchu sieciowego** poprzez uniemożliwienie nieznanym lub niezaufanym źródłom dostępu do usług zdalnych w systemach wewnętrznych. Uniemożliwia to podmiotom stanowiącym zagrożenie bezpośrednie łączenie się z usługami zdalnego dostępu, które ustanowili w celu zapewnienia trwałości.
- **Zainstaluj, regularnie aktualizuj i włącz wykrywanie w czasie rzeczywistym oprogramowania antywirusowego** na wszystkich hostach.
- **Przegląd kontrolerów domeny, serwerów, stacji roboczych i aktywnych katalogów pod** kątem nowych i/lub nierozpoznanych kont [CPG 1.A, 2.O].
- **Kontrola kont użytkowników** z uprawnieniami administracyjnymi i konfiguracja kontroli dostępu zgodnie z zasadą najmniejszych uprawnień [CPG 2.E].
- **Wyłączenie nieużywanych portów** [CPG 2.V].
- **Rozważ dodanie banera do wiadomości e-mail** otrzymywanych spoza organizacji [CPG 2.M].
- **Wyłącz hiperłącza** w otrzymywanych wiadomościach e-mail.
- **Wdrożenie dostępu opartego na czasie dla kont ustawionych na poziomie administratora i wyższym. Na** przykład metoda dostępu Just-in-Time (JIT) zapewnia uprzywilejowany dostęp w razie potrzeby i może wspierać egzekwowanie zasady najmniejszych uprawnień (a także modelu Zero Trust). Jest to proces, w którym w całej sieci obowiązują zasady automatycznego wyłączania kont administratorów na poziomie Active Directory, gdy konto nie jest bezpośrednio potrzebne. Poszczególni użytkownicy mogą składać wnioski za pośrednictwem zautomatyzowanego procesu, który przyznaje im dostęp do określonego systemu na określony czas, gdy muszą wesprzeć wykonanie określonego zadania.

- **Wyłączenie działań i uprawnień wiersza poleceń i skryptów.** Eskalacja uprawnień i ruchy boczne często zależą od oprogramowania narzędziowego uruchamianego z wiersza poleceń. Jeśli podmioty stanowiące zagrożenie nie są w stanie uruchomić tych narzędzi, będą miały trudności z eskalacją uprawnień i/lub przemieszczaniem się na boki [CPG 2.E, 2.N].

- **Utrzymywanie kopii zapasowych danych w trybie offline** oraz regularne tworzenie i przywracanie kopii zapasowych [CPG 2.R]. Wprowadzając tę praktykę, organizacja pomaga zapewnić, że nie zostanie poważnie zakłócona i / lub będzie miała tylko nieodwracalne dane.
- **Upewnij się, że wszystkie dane kopii zapasowych są zaszyfrowane, niezmienne** (tj. nie można ich zmienić ani usunąć) i obejmują całą infrastrukturę danych organizacji [CPG 2.K, 2.L, 2.R].

WALIDACJA KONTROLI BEZPIECZEŃSTWA

Oprócz stosowania środków zaradczych, FBI, CISA, EC3 i NCSC-NL zalecają ćwiczenie, testowanie i walidację programu bezpieczeństwa organizacji w odniesieniu do zachowań zagrożeń zmapowanych w ramach MITRE ATT&CK for Enterprise w tym poradniku. FBI, CISA, EC3 i NCSC-NL zalecają przetestowanie istniejącego wykazu kontroli bezpieczeństwa w celu oceny ich skuteczności w odniesieniu do technik ATT&CK opisanych w niniejszym poradniku.

Aby rozpocząć:

1. Wybierz technikę ATT&CK opisaną w niniejszym poradniku (patrz tabele 4-12).
2. Dostosuj technologie zabezpieczeń do tej techniki.
3. Przetestuj swoje technologie pod kątem tej techniki.
4. Przeanalizuj wydajność swoich technologii wykrywania i zapobiegania.
5. Powtórz ten proces dla wszystkich technologii zabezpieczeń, aby uzyskać zestaw kompleksowych danych dotyczących wydajności.
6. Dostosuj swój program bezpieczeństwa, w tym ludzi, procesy i technologie, w oparciu o dane wygenerowane przez ten proces.

FBI, CISA, EC3 i NCSC-NL zalecają ciągłe testowanie programu bezpieczeństwa, na dużą skalę, w środowisku produkcyjnym, aby zapewnić optymalną wydajność w stosunku do technik MITRE ATT&CK określonych w tym poradniku.

ZASOBY

- Stopransomware.gov to podejście obejmujące cały rząd, które zapewnia jedną centralną lokalizację zasobów i alertów dotyczących oprogramowania ransomware.
- Zasoby do złagodzenia ataku ransomware: #StopRansomware Guide.
- Bezpłatne usługi higieny cybernetycznej: Usługi cyberhigieny, Ocena gotowości na ransomware.

ODNIESIENIA

[1] Fortinet: Ransomware Roundup - Akira

[2] Cisco: Ransomware Akira atakuje sieci VPN bez MFA

[3] Truesec: Wskazania grupy Akira Ransomware aktywnie wykorzystującej Cisco AnyConnect CVE- 2020-3259

[4] TrendMicro: Akira Ransomware w centrum uwagi

[5] CrowdStrike: Czym jest atak kerberoastingowy?

[6] Sophos: Akira po raz kolejny: Ransomware, które nie przestaje brać

[7] Sophos: Akira Ransomware "przywraca rok 1988"

RAPORTOWANIE

Organizacja użytkownika nie ma obowiązku udzielania odpowiedzi ani przekazywania informacji zwrotnych do FBI w odpowiedzi na niniejszą wspólną CSA. Jeśli po zapoznaniu się z dostarczonymi informacjami organizacja zdecyduje się przekazać informacje FBI, raportowanie musi być zgodne z obowiązującymi przepisami stanowymi i federalnymi.

FBI jest zainteresowane wszelkimi informacjami, które można udostępnić, w tym dziennikami granicznymi pokazującymi komunikację z i do zagranicznych adresów IP, przykładową notą okupu, komunikacją z aktorami zagrożeń Akira, informacjami o portfelu Bitcoin, plikami deszyfratora i / lub łagodną próbką zaszyfrowanego pliku.

Dodatkowe interesujące szczegóły obejmują: docelowy punkt kontaktowy firmy, status i zakres infekcji, szacowane straty, wpływ operacyjny, identyfikatory transakcji, datę infekcji, datę wykrycia, początkowy wektor ataku oraz wskaźniki oparte na hoście i sieci.

FBI, CISA, EC3 i NCSC-NL nie zachęcają do płacenia okupu, ponieważ płatność nie gwarantuje odzyskania plików ofiary. Co więcej, płatność może również ośmielić przeciwników do atakowania kolejnych organizacji, zachęcić inne podmioty przestępcze do zaangażowania się w dystrybucję oprogramowania ransomware i/lub sfinansować nielegalne działania. Niezależnie od tego, czy Ty lub Twoja organizacja zdecydowaliście się zapłacić okup, FBI i CISA wzywają do niezwłocznego zgłaszania incydentów związanych z oprogramowaniem ransomware do Internet Crime Complain Center (IC3) FBI, lokalnego biura terenowego FBI lub CISA za pośrednictwem systemu zgłaszania incydentów agencji lub jej całodobowego centrum operacyjnego (report@cisa.gov lub (888) 282-0870).

ZASTRZEŻENIE ODPOWIEDZIALNOŚCI

Informacje zawarte w niniejszym raporcie są dostarczane "tak jak są" wyłącznie w celach informacyjnych. FBI, CISA, EC3 i NCSC-NL nie popierają żadnego komercyjnego podmiotu, produktu, firmy lub usługi, w tym żadnych podmiotów, produktów lub usług powiązanych w tym dokumencie. Wszelkie odniesienia do określonych komercyjnych produktów, procesów lub usług za pomocą znaku usługowego, znaku towarowego, producenta lub w inny sposób nie stanowią ani nie sugerują poparcia, rekomendacji lub faworyzowania przez FBI lub CISA.

PODZIĘKOWANIA

Cisco i Sophos przyczyniły się do powstania tej porady.

HISTORIA WERSJI

18 kwietnia 2024: Wersja początkowa.