Metryka dokumentu:

Data publikacji dokumentu: 21.05.2024
Wersja: 1.0

Spis treści

Wstęp

W obliczu stale rosnącej groźby ataków ransomware, które są jednym z najpoważniejszych wyzwań dla bezpieczeństwa systemów informatycznych współczesnych organizacji, konieczne jest podejmowanie skutecznych działań, aby zwiększać poziom bezpieczeństwa systemów teleinformatycznych. Ataki ransomware są nie tylko istotnym zagrożeniem dla bezpieczeństwa danych i stabilności systemów informatycznych, ale mogą także doprowadzić do poważnych strat finansowych, materializacji ryzyka wizerunkowego, a w efekcie tego utraty zaufania ze strony klientów lub innych zewnętrznych interesariuszy.

W atakach ransomware często wykorzystywane są poniższe techniki:

1. phishing – polegający na manipulacji użytkownikiem np. poprzez wysyłanie oszukańczych wiadomości e-mail, których celem jest nakłonienie odbiorcy do otwarcia przesłanego załącznika lub wejścia w link i pobrania pliku ze złośliwym oprogramowaniem,
2. podatne, nieaktualizowane usługi – wiele ataków ransomware wykorzystuje znane luki i podatności w oprogramowaniu, które nie zostały zaktualizowane do najnowszej, zalecanej przed producenta wersji,
3. niepoprawnie zabezpieczone dostępy zdalne – atakujący często wykorzystują publiczne usługi dostępu zdalnego i uzyskuje dostęp do tych usług poprzez łamanie haseł metodą „Brute Force”.

W tym dokumencie opisujemy dobre praktyki, które mogą pomóc zabezpieczyć organizację przed atakami ransomware. Przedstawiamy też propozycje reagowania na ewentualne wystąpienie tego typu incydentu w organizacji. Opisane propozycje środków technicznych oraz zabezpieczeń organizacyjnych mają na celu zwiększenie poziomu odporności na ataki ransomware oraz minimalizowanie skutków wystąpienia tego typu incydentu. Oprócz określenia „atak ransomware” w dokumencie zamiennie wykorzystywane są określenia takie jak „incydent” lub „zdarzenie”.

Mamy nadzieję, że przedstawione tutaj informacje w istotny sposób przyczynią się do zwiększenie poziomu odporności Państwa organizacji.

Schemat postępowania w przypadku ataku ransomware

W tym rozdziale opisujemy schemat postępowania w reagowaniu na incydenty, z uwzględnieniem etapu przygotowania organizacji. Poniższe zestawienie bazuje na doświadczeniach pracowników CSIRT KNF w obsłudze incydentów związanych z atakami ransomware, doświadczeniach i uwagach przekazanych przez przedstawicieli podmiotów rynku finansowego, rekomendacjach CISA [1], dostępnych w ramach projektu „Stop Ransomware”[2], a także niezależnych ekspertów bezpieczeństwa.

Ta część dokumentu poświęcona została opisowi procesu reagowania na incydent bezpieczeństwa jakim jest atak ransomware, w podziale na 7 etapów:

- przygotowanie,
- identyfikacja,
- ograniczanie,
- komunikacja zewnętrzna i raportowanie,
- środki naprawcze,
- odzyskiwanie,
- wnioski.

PRZYGOTOWANIE

To bardzo ważny etap, w którym nie doszło jeszcze do incydentu, a działania mają na celu zapobiegnięcie jego wystąpienia lub ograniczenia skutków w sytuacji, jeżeli jednak dojdzie do ataku ransomware. Na tym etapie warto również zadbać o kwestie organizacyjne. Zachęcamy do przechowywania dokumentu także w wersji papierowej na wypadek braku dostępności systemów informatycznych, do których dojść może w wyniku ataku ransomware. Warto również zadbać o rzetelne zapoznanie się z przedmiotowym dokumentem osób odpowiedzialnych za reagowanie na incydenty bezpieczeństwa, co może znacząco poprawić jakość działania w trakcie wystąpienia incydentu ransomware. Dodatkowo, zaleca się również ustalenie alternatywnych dróg kontaktu i komunikacji w ustalonej ścieżce eskalacyjnej, jak również wyznaczenie osób, które będą miały dostęp fizyczny do lokalizacji, w których przechowywane są urządzenia przetwarzające informacje organizacji (kolokacje, serwerownie itd.), w razie zaistnienia potrzeby fizycznej ingerencji w urządzenia informatyczne w przypadku wystąpienia ataku ransomware.

W ramach pierwszego etapu reagowania na możliwość wystąpienia ataku ransomware, opisane zostały rekomendowane przez CSIRT KNF mityganty do wdrożenia w organizacji. Mają one na celu próbę uchronienia środowiska przed tego typu działaniem przestępczym, podniesienie poziom bezpieczeństwa organizacji i/lub próbę ograniczenia skutków wystąpienia opisywanego incydentu. Należy jednak pamiętać, że nie są one zamkniętym katalogiem rozwiązań. W załączniku znajduje się szczegółowy opis poszczególnych elementów z poniższej listy.

[1] CISA – Cybersecurity and Infrastructure Security Agency, Amerykańska Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury, https://www.cisa.gov/
[2] https://www.cisa.gov/stopransomware

Zestawienie taktyk działania atakujących

Podział przygotowany został z wyodrębnieniem taktyk, opartych na opracowaniu MITRE ATT&CK[3]:

1. **Initial access** – zebrane w tej taktyce techniki i procedury (TTP), pozwalają wyodrębnić działania, procesy i mechanizmy poprzez które atakujący starają się dostać do sieci informatycznej organizacji. Występuje tutaj m.in szereg mechanizmów, które atakujący mogą wykorzystywać na etapie przygotowania się do ataku.
2. **Execution** – faza ta opiera się na procesie infekcji, czyli wykonaniu złośliwego kodu na systemie lub w sieci ofiary. Przeplata się również z innymi fazami ataku m.in. Defense Evasion, Lateral Movement, Credential Access, Privilege Escalation, Command and Control.
3. **Privilege Escalation –** w tej fazie, atakujący starają się pozyskać jak najwięcej danych umożliwiających im uzyskanie możliwie jak najwyższych uprawnień w systemie lub sieci informatycznej, aby uzyskać szeroki dostęp do zasobów organizacji.
4. **Defense Evasion** – atakujący w tej taktyce starają się omijać mechanizmy obronne organizacji, celem uniknięcia wykrycia.
5. **Credential Access** – faza ataku skupiająca się na pozyskaniu jak największej ilości danych autoryzujących. W fazie tej mogą wystąpić powielone techniki z fazy Privilege Escalation.
6. **Discovery** – techniki wykorzystywane przez atakujących do rozpoznania wnętrza infrastruktury teleinformatycznej, w celu przejścia do taktyk Lateral Movement.
7. **Lateral Movement** – faza, w której atakujący wykorzystują skradzione poświadczenia, celem zdobycia dostępu do dodatkowych systemów.
8. **Persistence** – techniki użyte w tej taktyce mają za zadanie zapewnić atakującym przetrwanie w skompromitowanym (przejętym) systemie i/lub zapewnić możliwość przeprowadzenia ponownej infekcji systemu w przypadku wykrycia ataku.
9. **Command and Control** – taktyka ta opisuje mechanizmy komunikacji zainfekowanej infrastruktury lub systemów z serwerami zarządzającymi atakujących.
10. **Exfiltration** – jest to jeden z ostatnich elementów ataku, polegający na wyprowadzeniu danych z zaatakowanej organizacji.
11. **Impact** – faza, w której atakujący mogą podjąć działania mające na celu zakłócenie, zniszczenie lub zmianę funkcjonowania systemów ofiary celem wywarcia wpływu na jakość, integralność i stabilność świadczonych przez organizację usług. Taktyka ta może zostać wykorzystana np. w przypadku odcięcia komunikacji zainfekowanych systemów z serwerami command&control atakującego w przypadku wykrycia ataku.

[3] https://attack.mitre.org/

Zestawienie mitygantów możliwych do wdrożenia w organizacji

Do każdej z przedstawionych taktyk, przedstawiamy przypisane do nich możliwe do zastosowania mityganty. **Szczegółowe opisy mitygantów znajdują się w Załączniku 1 do dokumentu**. Należy pamiętać, że zakres wdrażanych i stosowanych mitygantów powinien zostać dostosowany do konkretnej organizacji w zależności od jej możliwości technicznych i organizacyjnych.

1.	**Initial access**
1.1	Blokowanie lub monitorowanie niestandardowych rozszerzeń załączników poczty
1.2	Dodanie ostrzeżeń dla wiadomości elektronicznych przychodzących spoza organizacji
1.3	Weryfikacja i detonacja linków oraz załączników w systemie typu Sandbox
1.4	Konfiguracja zabezpieczeń poczty elektronicznej SPF, DMARC, DKIM
1.5	Inwentaryzacja i weryfikacja usług wystawionych na interfejsach publicznych dostępnych z Internetu
1.6	Cykliczne skanowanie usług widocznych z sieci Internet
1.7	Zabezpieczenie interfejsów zdalnego dostępu
1.8	Monitorowanie informacji na temat nowych podatności
1.9	Monitorowanie integralności konfiguracji systemów, urządzeń oraz usług
1.10	Stosowanie rozwiązań klasy Web Application Firewall oraz IPS
1.11	Stosowanie wieloskładniowego procesu uwierzytelniania (MFA)
1.12	Cykliczne podnoszenie świadomości użytkowników z zakresu cyberzagrożeń
1.13	Monitorowanie i ograniczanie ataków typu „Password Spraying”
1.14	Monitorowanie i ograniczanie ataków typu „Brute Force”
1.15	Utrzymywanie aktualnej dokumentacji i schematów sieciowych
1.16	Stosowanie mechanizmów typu proxy
1.17	Wdrożenie ograniczeń dla usług RDP[4]
1.18	Analiza konfiguracji serwisów, usług, aplikacji pod kątem zgodności z politykami bezpieczeństwa
1.19	Regularna aktualizacja oprogramowania i nadzór nad poprawkami bezpieczeństwa
1.20	Prowadzenie testów i udział w ćwiczeniach cyberbezpieczeństwa
2.	**Execution**
2.1	Podwyższenie poziomu monitorowania wykonywania skryptów Powershell
2.2	Ograniczenie możliwości użycia narzędzia PsExec
2.3	Ograniczenie możliwości realizacji połączeń sieciowych przez skrypty PowerShell oraz narzędzia systemowe
2.4	Ograniczenia dla wykonywania makr w plikach dokumentów pakietów biurowych
2.5	Monitorowanie drzewa procesów pod kątem nietypowego zachowania
2.6	Podpisanie skryptów i narzędzi wytworzonych i wykorzystywanych w organizacji
2.7	Monitorowanie lub blokowanie wykonywania plików skryptów .bat, .js, .ps,
2.8	Wykrywanie zmiany ExecutionPolicy dla Powershell
2.9	Monitorowanie instalacji nowych usług poprzez PsExec
2.10	Monitorowanie procesów logowania oraz operacji czyszczenia logów
3.	**Privilege Escalation**

[4] RDP – Remote Desktop Protocol

3.1	Ograniczenie wykorzystywanie lokalnych kont administratorów i zastosowanie rozwiązań klasy PAM[5]
3.2	Monitorowanie i ograniczanie wykorzystywania LOLBin's[6]
3.3	Weryfikacja zapytań do LDAP[7]
3.4	Weryfikacja i monitorowanie pojawienia się i synchronizacji nowych kontrolerów domeny
3.5	Utworzenie kont użytkowników typu Canary
3.6	Wykrywanie enumeracji SMB[8]
4.	**Defense Evasion**
4.1	Stosowanie listy dozwolonych aplikacji
4.2	Monitorowanie dezaktywacji mechanizmów bezpieczeństwa
4.3	Wzajemne monitorowanie się agentów bezpieczeństwa
4.4	Wymuszanie aktualizacji sygnatur systemów bezpieczeństwa
4.5	Monitorowanie wywoływania polecenia net.exe stop
4.6	Monitorowanie kluczy rejestru odpowiedzialnych za rozwiązania bezpieczeństwa
4.7	Monitorowanie zmian w konfiguracji backupów stacji roboczej (VSSADMIN)
4.8	Monitorowanie wywołania polecenia kill.exe
4.9	Monitorowanie pojawiających się nieautoryzowanych hostów w sieci
4.10	Monitorowanie zmian w konfiguracji zaplanowanych zadań
4.11	Monitorowanie wykorzystania polecania sc.exe
5.	**Credential Access**
5.1	Wdrożenie wielowarstwowych zabezpieczeń
5.2	Higiena tożsamości
5.3	Monitorowanie aktywności użytkowników
5.4	Budowanie świadomości pracowników
5.5	Ochrona kont administratorów
5.7	Separacja uprawnień administratorów domeny - AD Tier model
5.7	Wykrywanie i blokowanie uruchomień programów realizujących zrzuty pamięci z procesu LSASS
5.8	Wdrożenie LAPS (Local Administratora Password Solution)
6.	**Discovery**
6.1	Monitorowanie prób rozpoznania połączeń sieciowych poprzez arp.exe
6.2	Monitorowanie prób rozpoznania poprzez nslookup.exe
6.3	Monitorowanie wykorzystania innych narzędzi i komend
7.	**Lateral Movement**
7.1	Segmentacja sieci
7.2	Monitorowanie wykorzystywania RDP
7.3	Zabezpieczenie kontrolerów domeny
8.	**Persistence**
8.1	Monitorowanie kluczy rejestru wykorzystywanych przez atakujących
8.2	Monitorowanie kluczy rejestru tworzonych dla nowych usług
8.3	Monitorowanie wykorzystania bcdedit.exe
9.	**Command and Control**

[5] PAM – Privilieged Access Management
[6] LOLBins – Living Off The Land Binaries, Scripts and Libraries
[7] LDAP – Lightweight Directory Access Protocol
[8] SMB – Samba Message Block

9.1	Monitorowanie połączeń do znanych serwerów Command&Control (C2)
9.2	Wdrożenie reguł i monitorowanie wykrytych prób beaconingu do serwerów C2
9.3	Wdrożenie reguł wykrywających komercyjne narzędzia typu Cobalt-Strike
10.	**Exfiltration**
10.1	Ograniczanie ruchu do węzłów wyjściowych sieci TOR
10.2	Organicznie ruchu DNS over HTTPs (DoH)
10.3	Monitorowanie lub blokowanie ruchu do serwisów kategorii File-share
10.4	Monitorowanie lub blokowanie ruchu TFTP/SMB/FTP/SFTP do Internetu
10.5	Monitorowanie anomalii sieciowych
11.	**Impact**
11.1	Utworzenie reguł monitorujących masowy nadpis plików
11.2	Utworzenie reguł wykrywających uruchomienie bibliotek typu pycrypto
11.3	Zapewnienie bezpiecznych dostępów do kopii zapasowych
11.4	Przygotowanie i utrzymanie backupów krytycznych danych

Proces reagowania na Incydent typu ransomware

Etap przygotowania to czas, kiedy nie mamy w organizacji podejrzenia wystąpienia ataku ransomware jednak mamy świadomość ryzyka takiego ataku. Istotnym elementem procesu reagowania na incydenty jest wyznaczenie koordynatora incydentów (stałego lub rotacyjnego), który będzie miał prawo do podejmowania kluczowych decyzji w zakresie, co najmniej, reagowania, zabezpieczenia i minimalizowania skutków ataku. Rola ta jest istotna przy obsłudze szerokiego spektrum incydentów bezpieczeństwa, nie tylko dla ataków ransomware. W dalszej części dokumentu przedstawiamy kolejne etapy reagowania na podejrzenie wystąpienia lub wystąpienie incydentu związanego z atakiem ransomware.

IDENTYFIKACJA

Na tym etapie dochodzi do wykrycia i potwierdzenia (lub zaprzeczenia) wystąpienia ataku ransomware. Zalecamy, aby organizacja miała przygotowane procedury i instrukcje wewnętrzne, pozwalające na optymalne działanie osób przyjmujących początkowe zgłoszenie o wystąpieniu ataku ransomware. Osoby obsługujące takie zdarzenie powinny mieć odpowiednie przeszkolenie i wiedzę m.in w zakresie pozyskiwania próbki malware w celu ekstrakcji z niej IOC[9] i wykorzystaniu go np. w systemie EDR/XDR[10]. Niezbędna jest również pioryteryzacja zadań i świadomość osób przyjmujących zgłoszenie o konieczności potraktowania takiego zgłoszenie priorytetowo. Sprawne i usystematyzowane działanie pozwoli uniknąć zbędnych pomyłek oraz skróci czas identyfikacji incydentu. W tym celu należy przeprowadzić wstępną analizę zdarzenia i podjąć dalsze kroki zgodne ze stwierdzonym stanem faktyczny.

1. Identyfikacja i potwierdzenie wystąpienia incydentu:
    - wstępna analiza logów systemu bezpieczeństwa, celem potwierdzenia incydentu,
    - określenie aktualnego stanu infekcji: czy zostały zainfekowane serwery, wirtualizatory i/lub kopie zapasowe, czy atakujący mają dostęp do struktury AD z wykorzystaniem kont uprzywilejowanych.
2. Przegląd logów systemowych:
    - weryfikacja potencjalnych alertów wskazujących na obecność złośliwego oprogramowania lub działalności atakujących,
    - zabezpieczenie logów z ActiveDirectory, systemów bezpieczeństwa i urządzeń brzegowych (antivirus, EDR/XDR, IDS, IPS, FW, WebFB itd.),
    - zabezpieczenie logów z proxy oraz DNS celem próby oceny czy nastąpiła eksfiltracja danych organizacji z zainfekowanych stacji roboczych i/lub serwerów.
3. Wstępna ocena zdarzenia, nadanie priorytetu.
4. Weryfikacja, czy do organizacji została dostarczona wiadomość od atakujących np. informacja o możliwości zapłacenia okupu.
5. Uruchomienie wewnętrznej ścieżki eskalacyjnej:
    - potencjalne skutki incydentu ransomware mogą w istotny sposób wypłynąć na stabilność funkcjonowania organizacji, w przypadku wystąpienia incydentu tej klasy zaleca się poinformowanie o zdarzeniu bezpośrednich przełożonych oraz kierownictwa organizacji,

[9] IOC – Indicator of Compromise – wskaźniki kompromitacji systemu
[10] EDR – Endpoint Detection and Response
XDR – Extended Detection and Response

- mając dostęp do infrastruktury teleinformatycznej zaatakowanej organizacji (np. systemów pocztowych, ticketowych czy wewnętrznych systemów komunikacji bezpośredniej) atakujący mogą śledzić działania podejmowane przez organizację, aby kontrolować czy atak został zauważony i zidentyfikowany – zaleca się korzystanie z zewnętrznych kanałów komunikacji, takich jak np. rozmowy telefoniczne, by nie informować intruzów o wykryciu i podjętych przez organizację działaniach,
- listy kontaktowe wraz z numerami telefonów warto przygotować wcześniej i trzymać w gotowości na wypadek ataku również w formie papierowej (należy pamiętać, że atakujący mogą monitorować sieć teleinformatyczną organizacji).

6. Rozpoczęcie prac zespołu reagowania na incydent.

OGRANICZANIE

Po wstępnej analizie zdarzenia i klasyfikacji go jako incydent bezpieczeństwa związany z atakiem ransomware, należy zadbać o zminimalizowanie skutków ataku oraz zapobiec dalszej eskalacji incydentu, mając jedocześnie na uwadze konieczność zabezpieczenia materiału niezbędnego do prowadzenia dalszych analiz.

W tym celu zalecamy:

1. Bezzwłoczną izolację potencjalnie skompromitowanych systemów:
   - określenie aktualnego stanu infekcji i zakresu dostępów atakujących do zainfekowanych systemów,
   - w przypadku infekcji kilku systemów lub podsieci rozważenie izolacji całych podsieci na poziomie urządzeń sieciowych, odcięcie pojedynczych hostów w przypadku infekcji ransomware może okazać się nieskuteczne,
   - w trakcie izolowania elementów sieci skupienie się w pierwszej kolejności na systemach krytycznych dla funkcjonowania organizacji,
   - w przypadku braku możliwości izolacji sieci z poziomu urządzeń sieciowych rozważenie fizycznego odłączenia połączeń sieciowych z zainfekowanych urządzeń lub sieci,
   - przeprowadzenie izolacji w sieci w sposób możliwie niezauważalny dla atakujących, gdyż atakujący mogą obserwować organizację w trakcie ataku,
   - należy mieć na uwadze, że odłączenie potencjalnie skompromitowanych urządzeń od zasilania może spowodować utratę dostępu do istotnych informacji i artefaktów związanych z atakiem. Wyłączenie systemów należy rozpatrzyć w przypadku braku możliwości odseparowania potencjalnie zainfekowanych urządzeń, pamiętając o konieczność zebrania materiału dowodowego.
2. Monitorowanie nieskompromitowanej części sieci pod kątem potencjalnych śladów infekcji.

KOMUNIKACJA ZEWNĘTRZNA I RAPORTOWANIE

Na tym etapie konieczna jest współpraca osób zaangażowanych w obsługę incydentu z osobami odpowiedzialnymi w organizacji za komunikację wewnętrzną i zewnętrzną. Zalecamy aby formułowany przekaz był wyważony i nie budził niepotrzebnego chaosu i poczucia niepokoju. Przekazywane informacje powinny być rzetelne i zostać zweryfikowane przed ich publikacją. Na tym etapie działań organizacji potrzebne jest również zaangażowanie osób odpowiedzialnych za raportowanie, celem wypełnienia obowiązków formalnych oraz operacyjnych.

Warto rozważyć również powołanie sztabu kryzysowego (chyba, że wynika on z wewnętrznych procedur reagowania na incydenty bezpieczeństwa), w skład którego wchodzić powinny, co najmniej osoby odpowiedzialne za koordynowanie incydentu, przedstawiciele działu komunikacji, przedstawiciele działu prawnego, osoby odpowiedzialne za raportowanie oraz członkowie kierownictwa organizacji.

W tym celu zalecamy:

1. Przygotowanie planu komunikacji zewnętrznej:
    - w proces obsługi incydentu należy zaangażować departamenty odpowiedzialne za komunikację (w etapie Identyfikacji, ustalając zespół reagowania na incydenty),
    - organizacja powinna mieć opracowany plan komunikacji kryzysowej na wypadek ataku ransomware, w przypadku braku planu komunikacji należy bezzwłocznie go opracować,
    - jeżeli ustalono, że w pierwszej fazie obsługi incydentu informacja nie będzie ujawniana poza organizację, należy przygotować się do poinformowania i poinstruowania pracowników, aby informacji o ataku nie ujawniali, a osoby które mają kontakt z interesariuszami zewnętrznymi powinny być przygotowane do odpowiedniej komunikacji; informację o ataku mogą ujawnić sami atakujący.
2. Zgłoszenie informacji o Incydencie do zespołu CSIRT poziomu krajowego lub sektorowego [11] . Ze względu na potencjalną sensytywność przekazywanych informacji, wiadomości należy zabezpieczyć. Zalecamy wykorzystanie szyfrowania komunikacji z wykorzystaniem np. kluczy PGP. Na tym etapie komunikacji z zespołem/zespołami CSIRT organizacja może nie mieć pełnej wiedzy o skali i zakresie ataku, co jednak nie może być podstawą do braku lub opóźnień w zgłoszeniu wystąpienia incydentu. Zaleca się, aby zgłoszenia były realizowane w sposób niezwłoczny, ale też niewprowadzający istotnych opóźnień w proces obsługi incydentu. W proces zgłoszenia powinny być zaangażowane inne osoby niż odpowiadające bezpośrednio za realizację zadań technicznych w procesie obsługi incydentu. Należy pamiętać, że pierwsze zgłoszenie incydentu może być uzupełnione w razie pojawienia się nowych informacji. W zgłoszeniu do CSIRT warto uwzględnić:

    Na pierwszym etapie, bezpośrednio po wykryciu i identyfikacji incydentu:
    - określenie aktualnego stanu infekcji i podejmowanych aktualnie działań,
    - informację o ewentualnym otrzymaniu wiadomości od atakujących z żądaniem okupu oraz treść tej wiadomości (może pozwolić to na szybszą identyfikację grupy przestępczej odpowiedzialnej za atak).

    W kolejnych etapach obsługi incydentu zgłoszenie należy uzupełnić o następujące informacje:
    - zidentyfikowany lub prawdopodobny wektor inicjalny ataku wraz z informacją o statusie mitygacji lub likwidacji zagrożenia,
    - określenie wpływu zdarzenia na funkcjonowanie i dostępność usług organizacji,
    - status realizacji eskalacji wewnętrznych,
    - informację czy planowana jest komunikacja zewnętrzna o incydencie, w tym szczególnie do zewnętrznych interesariuszy (jeżeli tak, to uwzględniając informację o formie przekazu),
    - określenie statusu dostępnych backupów oraz planu przywracania infrastruktury i usług biznesowych,
    - status zgłoszeń do innych podmiotów, w tym czy zostało złożone zawiadomienie o popełnieniu przestępstwa i/lub zgłoszenie incydentu do UODO,

[11] Jeżeli dla danego sektora został powołany zespół CSIRT.

- zidentyfikowane ryzyka związane z potencjalnym rozprzestrzenianiem się infekcji ransomware na powiązane systemy innych organizacji lub dostawców usług ICT,
- potencjalne zidentyfikowane ryzyka, które mogą stanowić zagrożenia dla innych podmiotów współpracujących z organizacją,
- przesłanie następujących plików[12]:
    - minimum 2 zaszyfrowane pliki,
    - notatka z żądaniem okupu od przestępców (jeżeli została pozostawiona przez atakujących),
    - próbka oprogramowania, które zainfekowało stacje robocze lub serwery,
    - logi z zainfekowanej maszyny/maszyn oraz systemów bezpieczeństwa z czasu infekcji,
    - oryginały plików, które zostały zaszyfrowane, jeżeli się zachowały lub zostały odtworzone z backupu (przykładowe pliki po zaszyfrowaniu oraz ich oryginalne wersje),
- inne, podjęte do tej pory kroki.

3. W przypadku stwierdzenia naruszenia danych osobowych należy zgłosić incydent do Urzędu Ochrony Danych Osobowych w terminach wskazanych w odpowiednich przepisach prawa.
4. Zgłoszenie zawiadomienia o popełnieniu przestępstwa do organów ścigania. Zgodnie z informacjami pozyskanymi z Centralnego Biura Zwalczania Cyberprzestępczości oraz Prokuratury, w trakcie składania zawiadomienia organizacja może zostać poproszona m.in o następujące informacje:
    - kiedy i jak stwierdzono atak,
    - jakie czynności podjął pokrzywdzony w związku z incydentem,
    - wektor ataku/sposób infekcji wraz z dostępnymi szczegółami,
    - liczbę zaatakowanych urządzeń i skutki wystąpienia incydentu, w tym zidentyfikowane straty dla firmy/klientów,
    - czy podczas ataku wykradzione zostały dane (w tym ich rodzaj) oraz czy pokrzywdzony jest szantażowany możliwością upublicznienia lub sprzedaży wykradzionych danych,
    - czy znana jest lokalizacja serwera, na którym sprawcy upublicznili bądź mają zamiar upublicznić wykradzione dane,
    - czy określono sposób i szczegóły dotyczące żądania okupu w zamian za przywrócenie dostępności lub odstąpienie od ujawnienia wykradzionych danych, jeżeli tak to w zakresie organów ścigania istotna będzie również informacja jaka została określona przez atakujących forma płatności,
    - komunikat pojawiający się po zaszyfrowaniu, a co za tym idzie nazwy cryptolockera, formy płatności okupu czy metody komunikacji ze sprawcami,
    - czy organizacja nawiązała kontakt z przestępcami.

Jeżeli zawiadomienie składane jest na piśmie, warto na etapie przygotowywania pisma z zawiadomieniem o popełnieniu przestępstwa uwzględnić ten zakres informacji.
Dodatkowo, w trakcie prowadzenia sprawy, organy ścigania mogą chcieć również zabezpieczyć niezbędne urządzenia, logi z systemów oraz zwiększyć zakres potrzebnych informacji ponad te wymienione.

[12] Zgodnie z poradami opisanymi w poradniku CERT Polska
https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

ANALIZA INCYDENTU

Na tym etapie należy ustalić jakie działania zostaną podjęte oraz jakie narzędzia należy wykorzystać, aby usunięć źródła zagrożenia oraz naprawić szkody w organizacji. To również moment na przeprowadzenie szczegółowej analizy przyczyn incydentu, aby zrozumieć, jak doszło do ataku ransomware i jak im zapobiec w przyszłości. Możliwość przeprowadzenia szczegółowej analizy wymaga jednak niezbędnych informacji, w tym przede wszystkim logów z systemów. Zaleca się, aby organizacja była przygotowana na konieczność sprawdzenia informacji do 3 miesięcy przed datą wystąpienia incydentu i miała proces, którego celem jest bezpieczne przechowywanie chronologicznego zapisu zawierającego informacje o zdarzeniach i działaniach w infrastrukturze teleinformatycznej organizacji.

Na tym etapie zalecamy:

1. Rozpoczęcie procesu Threat Huntingu, w trakcie którego należy skupić się w szczególności na:
    - identyfikacji wektora inicjalnego ataku oraz identyfikacji potencjalnych dostępów, do których mają dostęp atakujący. Kluczowy aspektem jest zidentyfikowanie kont i systemów, które były wykorzystane przez atakujących w pierwszych fazach ataku,
    - identyfikacji innych systemów i ich zabezpieczeniu, do których mogą mieć dostęp atakujący z wykorzystaniem skompromitowanych poświadczeń i posiadanych dostępów,
    - nowo utworzonych kontach w Active Directory, w szczególności posiadających podwyższony poziom uprawnień (np. administratora domeny),
    - weryfikacji logów z połączeń zdalnych do organizacji (np. VPN) w celu identyfikacji potencjalnych niepożądanych logowań lub nieuprawnionych urządzeń mających zdalny dostęp do infrastruktury organizacji,
    - zidentyfikowaniu modyfikacji ustawień backupów na stacjach roboczych (np. shadow copy). Najczęściej w tym celu wykorzystywane są wbudowane w system Windows narzędzia takie jak fsutil.exe (deletejournal), vssadmin.exe, wbadmin.exe, wmic.exe (shadowcopy),
    - śladach komunikacji z systemami takimi jak Cobalt Strike beacon/client. Cobalt Strike jest oprogramowaniem komercyjnym używanym przy testach penetracyjnych, często jednak również wykorzystywanym przez przestępców w realnych atakach. Procesy oprogramowania często ukrywane są pod standardowymi nazwami procesów systemu Windows,
    - śladach niestandardowego wykorzystania oprogramowania do zdalnego monitorowania i zarządzania (RMM),
    - niestandardowych komendach Powershell lub operacjach z wykorzystaniem narzędzi z pakietu PSTools,
    - śladach po próbach enumeracji zasobów Active Directory,
    - śladach po próbach realizacji zrzutów pamięci z procesu LSASS np. z wykorzystaniem narzędzi takich jaki Mimikatz, Sysinternals ProcDump, PPLdump, HandleKatz, nanodump,
    - śladach niestandardowej komunikacji wewnątrz sieci lub komunikacji zewnętrznej z serwerami Command&Control (C2),
    - śladach wskazujących na wyprowadzenie danych z organizacji takich jak:
        - niestandardowy wzmożony ruch sieciowy wychodzący z organizacji w okresie poprzedzającym incydent, ruch może być tunelowany na różnych portach i usługach,
        - komunikacji z serwisami do przechowywania plików FTP/SFTP czy też wykorzystywaniu narzędzi Rclone, Rsync,
    - w przypadku danych na serwerze zaszyfrowanych poprzez zainfekowaną stację roboczą:

- przegląd logów Review Computer Management > Sessions and Open Files lists pod kątem określenia użytkowników lub systemów uzyskujących dostęp do plików,
- przegląd właściwości zaszyfrowanych plików lub plików z treścią okupu, w celu identyfikacji powiązanych kont użytkowników,
- przegląd logów TerminalServices-RemoteConnectionManager, w celu weryfikacji potencjalnych połączeń RDP,
- przegląd logów Windows Security log, SMB event logs i innych mogących identyfikować próby uzyskania dostępów do zasobów serwera,
- uruchomienie na serwerze oprogramowania do nasłuchiwania ruchu np. Wireshark w celu identyfikacji adresów IP powiązanych z procesami zapisywania lub zmiany nazw plików na serwerze np. z wykorzystaniem komendy smb2.filename contains *nazwaransomware,*

- nowo utworzonych usługach, dodanych wpisach w harmonogramach zadań, niestandardowym oprogramowaniu, tworzeniu nietypowych plików czy też standardowego oprogramowania wywołującego nietypowe procesy,
- śladach po modyfikacjach procesów logowania oraz operacjach czyszczenia logów.

2. Rozszerzona analiza pod kątem dostępów atakujących i wektora inicjalnego ataku:
   - pełna identyfikacja i zabezpieczenie wektorów ataków wykorzystywanych przez przestępców,
   - trwałe usunięcie wszystkich potencjalnych dostępów i mechanizmów wykorzystywanych przez atakujących.

ODZYSKIWANIE

Na tym etapie organizacja prowadzi działania w celu przywrócenia standardowego funkcjonowania systemów i usług. Ze względu na możliwość zainfekowania systemów przed wykonaniem backupu zaleca się testowanie odtworzonych z backupów systemów i aplikacji, aby upewnić się, że są one wolne od zagrożeń, głównie tych, które zidentyfikowane zostały jako wektor wejścia atakujących.

Odbudowa systemów zgodnie z priorytetyzacją usług krytycznych w organizacji:

- przeprowadzenie analizy pod kątem odtwarzania, identyfikacja systemów krytycznych dla działania organizacji, które powinny być odtworzone w pierwszej kolejności;
- reset haseł we wszystkich powiązanych z incydentem systemach, przegląd zabezpieczeń i wdrożenia aktualizacji i poprawek bezpieczeństwa w infrastrukturze, które wcześniej nie zostały zrealizowane,
- odbudowa systemów i elementów infrastruktury zgodnie z priorytetyzacja usług krytycznych,
- ponowne podłączenie przywróconych systemów i odtworzenie funkcjonowania procesów biznesowych.

WNIOSKI

Po zakończeniu procesu obsługi incydentu i przywróceniu organizacji do pełnego funkcjonowania procesów biznesowych i operacyjnych zaleca się przeprowadzenie dodatkowej analizy, w ramach której oceniony zostanie również proces reagowania na incydenty.

Na tym etapie zalecamy:

1. Udokumentowanie szczegółów incydentu oraz wyciagnięcie wniosków na podstawie przeprowadzonego procesu obsługi incydentu ransomware.
2. Przygotowanie raportu po incydencie, który powinien zawierać m.in szczegółowy opis zdarzenia, podjętych działań i rekomendacji na przyszłość
3. Uzupełnienie danych w rejestrze incydentów.
4. Przeprowadzenie procesu „Lessons learned” z obsługi incydentu i powiązanych zdarzeń.
5. Przesłanie raportów końcowych z obsługi incydentów do właściwego zespołu CSIRT.

Podsumowanie

Ryzyko ataku typu ransmoware to zagrożenie, z którym musi się zmierzyć każda organizacja. Wdrożenie odpowiednich procedur i mechanizmów bezpieczeństwa pozwala w znaczący sposób obniżyć prawdopodobieństwo realizacji udanego ataku. Równie ważna jest także umiejętność reagowania na incydenty tego typu, jeżeli już przyjdzie nam się z nimi zmierzyć. Szybkie, ale przemyślane i odpowiednio skoordynowane działania pozwalają niejednokrotnie wyjść z opresji i istotnie zminimalizować konsekwencje incydentu. Z tego też powodu mamy nadzieje, że zebrane w dokumencie dobre praktyki w zakresie zapobiegania i reagowania na ataki ransomware będą dla Państwa materiałem pomocnym zarówno w przygotowaniu na ataki tego typu, jak i w sytuacji wystąpienia incydentu ransomware. Należy jednak pamiętać, że zakres działań i kształt procedur wewnętrznych powinien być przygotowany zgodnie ze specyfiką działania Państwa organizacji.

Materiał ten powstał we współpracy z podmiotami z polskiego rynku finansowego oraz zewnętrznymi konsultantami, którzy podzielili się z nami swoją wiedza i doświadczeniem w przedmiotowym zakresie. Za pracę nad materiał i wszelkie przesłane do nas uwagi, serdecznie dziękujemy!

ZAŁĄCZNIK 1: Szczegółowy opis poszczególnych mitygantów

1. Initial Access

1.1. **Blokowanie lub monitorowanie niestandardowych rozszerzeń załączników poczty** – wdrożenie reguł, na podstawie których wiadomości poczty elektronicznej zawierające załączniki o określonych rozszerzeniach będą blokowane lub dodatkowo weryfikowane; przykładami takich rozszerzeń są .iso, .dmg, .img, .exe, .vbs, .lnk, .bat, cmd, .ps1.

1.2. **Dodanie ostrzeżeń dla wiadomości elektronicznych przychodzących spoza organizacji –** zabieg ten ma za zadanie zwiększenie świadomości użytkowników poczty elektronicznej i zwrócić uwagę na konieczność zachowanie ostrożności w przypadku otwierania wiadomości mailowych pochodzących spoza organizacji. Dobrą praktyką jest zmienianie komunikatów, tak by użytkownicy nie przyzwyczaili się do wyświetlanego komunikatu.

1.3. **Weryfikacja i detonacja linków oraz załączników w systemie typu Sandbox** – wdrożenie mechanizmów umożliwiających weryfikacje potencjalnie niebezpiecznych linków oraz załączników zawartych w wiadomościach elektronicznych. W rozwiązaniu warto uwzględnić:
- sprawdzanie w serwisach reputacyjnych linków zawartych w wiadomościach e mail przychodzących do organizacji,
- sprawdzanie sum kontrolnych załączników lub próba ich uruchomienia w systemie typu sandbox, następnie zależnie od werdyktu mechanizmu dostarczenie wiadomości lub jej przeniesienie do odpowiedniej kwarantanny.

1.4. **Konfiguracja zabezpieczeń poczty elektronicznej SPF, DMARC, DKIM** – weryfikacja oraz konfiguracja mechanizmów SPF, DMARC oraz DKIM w celu wykluczenia podszycia się pod innego niż faktyczny nadawcę. Korzystanie z list reputacyjnych w celu filtrowania wiadomości ze znanych adresów rozsyłających spam lub inną złośliwą zawartość, w trakcie konfiguracji zabezpieczeń warto skorzystać z poradników CERT Polska oraz mechanizmów testowania poprawności konfiguracji:
https://cert.pl/posts/2021/10/mechanizmy-weryfikacji-nadawcy-wiadomosci/
https://bezpiecznapoczta.cert.pl/

1.5. **Inwentaryzacja i weryfikacja usług wystawionych na interfejsach publicznych dostępnych z Internetu** – przeprowadzanie cyklicznego skanowania własnych adresów IP w celu zidentyfikowania usług udostępnionych do sieci Internet oraz weryfikacja czy widoczność i dostępność zidentyfikowanych usług jest zasadna. Skonfigurowanie interfejsów zarządzających dla różnego rodzaju usług tak, by dostęp do nich był możliwy tylko z infrastruktury lokalnej lub z wykorzystaniem whitelistingu.

1.6. **Cykliczne skanowanie usług pojawiających się i widocznych z sieci Internet** – wdrożenie mechanizmów skanowania zewnętrznych adresów IP należących do organizacji, w celu wykrycia nieautoryzowanych usług i serwisów.

1.7. **Zabezpieczenie interfejsów zdalnego dostępu** – Organizacja powinna rozważyć ograniczenie dostępów do interfejsów zdalnych w taki sposób, by były dostępne tylko dla użytkowników zalogowanych za pomocą VPN, minimalnym rozwiązaniem jest ograniczenie listy adresów IP, które mogą się logować do tych usług.

1.8. **Monitorowanie publikowanych podatności** – bieżące monitorowanie informacji na temat podatności i zagrożeń dla systemów, aplikacji, elementów infrastruktury, urządzeń i usług sieciowych będących na styku sieci Internet i infrastruktury lokalnej, cykliczne skanowania bezpieczeństwa zewnętrznych elementów infrastruktury pod kątem podatności i zagrożeń.

1.9. **Monitorowanie integralności konfiguracji systemów, urządzeń oraz usług** – bieżące monitorowanie zewnętrznych elementów infrastruktury, w celu weryfikacji potencjalnych nieautoryzowanych zmian w konfiguracji.

1.10. **Stosowanie rozwiązań klasy Web Application Firewall oraz IPS** – dla elementów infrastruktury widocznej z sieci Internet, w celu automatycznej detekcji i blokowania prób ataków. Aktualizacja sygnatur i reguł w tych rozwiązaniach (z uwzględnieniem testów w celu wykluczenia False-Positive) w celu zapewnienia ciągłej jakości ochrony.
1.11. **Stosowanie wieloskładnikowego procesu uwierzytelniania (MFA)** w logowaniu do usług dostępnych z sieci Internet; wymuszenie stosowania złożonych i bezpiecznych haseł zgodnych z polityką haseł w organizacji
1.12. **Cykliczne podnoszenie świadomości użytkowników w zakresu cyberzagrożeń** – prowadzenie działań edukacyjnych mających na celu zwiększenie poziomu świadomości użytkowników w obszarze cyberzagrożeń z praktycznymi przykładami technik stosowanych przez atakujących, zakładających różne scenariusze.
1.13. **Monitorowanie i ograniczanie ataków typu „Password Spraying”** – wdrożenie mechanizmów pozwalających na wykrywanie i blokowanie ataków typu „Password Spraying”.
1.14. **Monitorowanie i ograniczanie ataków typu „Brute Force”** – wdrożenie mechanizmów pozwalających na wykrywanie i blokowanie (np. captcha) ataków typu „Brute Force”.
1.15. **Utrzymywanie aktualnej dokumentacji i schematów sieciowych** identyfikujących elementy infrastruktury teleinformatycznej uczestniczących w dostępie do wewnętrznej sieci organizacji z sieci Internet (w obu kierunkach), wraz z dokumentacją kierunków i przepływu danych. Dokumentacja powinna być utrzymywana w stanie aktualnym.
1.16. **Stosowanie mechanizmów typu proxy** – zaleca się wdrożenie w organizacji komunikacji za pośrednictwem mechanizmów proxy. Zaleca się także sprzężenie mechanizmów proxy z listami niebezpiecznych domen np. tymi prowadzonymi przez CERT Polska https://cert.pl/lista-ostrzezen/
1.17. **Zwiększenie restrykcji dla usług RDP** dostępnych z zewnątrz sieci. Jeżeli usługi te nie powinny być dostępne, rekomenduje się blokowanie ich na urządzeniach brzegowych. Jeżeli usługi RDP są niezbędne ze względów biznesowych, organizacyjnych itp. zaleca się zabezpieczenie dostępu do nich mechanizmami VPN. W celu dostępu do usług RDP należy stosować silne, bezpieczne hasła zgodnie z polityką bezpieczeństwa i procedurami organizacji. Dla Interfejsów zdalnego dostępu organizacja powinna wdrożyć ochronę przy użyciu MFA
1.18. **Analiza konfiguracji serwisów, usług, aplikacji** w celu eliminacji domyślnych lub niespełniających norm wewnętrznych ustawień, haseł, nadmiarowych usług i informacji.
1.19. **Regularna aktualizacja oprogramowania i nadzór nad poprawkami bezpieczeństwa** – brak aktualizacji poprawek bezpieczeństwa w sposób znaczący zwiększą ryzyko przeprowadzenia udanego ataku ransomware na organizację. Zaleca się wdrożenie mechanizmów nadzoru nad procesem zarządzania podatnościami w organizacji, z ustaleniem wysokiego priorytetu dla systemów dostępnych z sieci zewnętrznych w tym przede wszystkim z sieci Internet.
1.20. **Prowadzenie testów i udział w ćwiczeniach cyberbezpieczeństwa** – w momencie realnego incydentu osoby odpowiedzialne za jego obsługę mają ograniczony czas na podejmowanie kluczowych decyzji. Wstępne przygotowanie organizacji realizowane poprzez regularny udział w testowaniu zabezpieczeń oraz procedur jest istotnym elementem w obsłudze incydentu ransomware.

2. Execution

2.1. **Podwyższenie poziomu monitorowania wykonywania skryptów Powershell** – stosowanie dwóch poziomów logowania dostępnych w Windows: PowerShell

Windows Event Log oraz PowerShell Operational Log. Analiza sytuacji uruchamiania skryptów PowerShell nieautoryzowanych przez organizację.

2.2. **Ograniczenie możliwości użycia narzędzia PsExec** – zaleca się ograniczenie wykorzystania narzędzia PsExec poprzez wymaganie mechanizmu UAC, ograniczenie narzędzia tylko do wybranych kont administracyjnych, logowanie i weryfikacja każdego wywołania narzędzia PsExec. Przykładowe reguła SNORT wykrywająca użycie PSEXEC dostępna jest tutaj: https://medium.com/@DatBoyBlu3/sigma-rule-psexec-command-execution-684bbc036cbe

2.3. **Ograniczenie możliwości realizacji połączeń sieciowych przez skrypty PowerShell oraz narzędzia systemowe** – konfiguracja ograniczeń dla połączeń sieciowych, realizowanych przez skrypty PowerShell, w tym ze szczególnym uwzględnieniem połączeń do sieci Internet np. *cmd /c powershell.exe iwr oraz innych narzędzi systemowych („LOLBINs") np. Bitsadmin, certutil, netuse, netcat, tftp, wget, debug i inne.* Ograniczy to ryzyko pobrania złośliwej treści (payload) i przejście do kolejnych etapów ataków. Analogiczne ograniczenia można wdrożyć dla innych silników skryptowych, wscript, cscript, python. W przypadku środowisk developerskich zaleca się indywidualne podejście do wprowadzenia ograniczenia.

2.4. **Ograniczenia dla wykonywania makr w plikach dokumentów pakietów biurowych** – utwardzenie konfiguracji pakietów biurowych, ograniczenie możliwości uruchamiania makr, które nie są podpisane. Blokowanie makr może być wykonane poprzez mechanizmy GPO: *Administrative templates > Microsoft Word > Word options > Security Trust Center>Block macros from running in Office files from the Internet lub Disable all macros except digitally signed macros*.

2.5. **Monitorowanie drzewa procesów pod kątem nietypowych zachowania** – monitorowanie pod kątem nietypowego zachowania takiego jak wywołanie przez edytor dokumentów biurowych programów typu *conhost.exe, cmd.exe, cscript.exe*, itp. Utworzenie reguł, które mogą wskazywać na wykonanie się złośliwego oprogramowania z poziomu makr w dokumentach biurowych.

2.6. **Podpisywanie skryptów i narzędzi wytworzonych i wykorzystywanych w organizacji** – blokowanie możliwości uruchomienia niepodpisanych skryptów , a dla dojrzałych środowisk: niepodpisanych wewnętrznym certyfikatem wygenerowanym dla organizacji.

2.7. **Monitorowanie lub blokowanie wykonywania plików skryptów .bat, .cmd, .js, .ps1, .py** – wdrożenie mechanizmów monitorowania wykonywania skryptów przez użytkowników bez uprawnień administratora. Zaleca się utworzenie odpowiedniej roli dla użytkowników, dla których wykonywanie plików skryptów jest niezbędne w pracy. Bardziej restrykcyjne uprawnienia mogą również dotyczyć plików wykonywalnych pochodzących spoza listy oprogramowania dozwolonego w organizacji.

2.8. **Wykrywanie zmiany ExecutionPolicy dla Powershell** – zaleca się monitorowanie i weryfikacje wykonywania skryptów, które próbują zdegradować poziom Policy Execution np.: *jsRun.Run("cmd.exe /c PowerShell -ExecutionPolicy Bypass).*

2.9. **Monitorowanie instalacji nowych usług poprzez PsExec** – zaleca się monitorowanie instalacji nowych usług za pośrednictwem narzędzia PSEXEC np. poprzez „Auditing Windows Services" event ID 7045 i słowa kluczowe psexec w treści.

2.10. **Monitorowanie procesów logowania oraz operacji czyszczenia logów** – w trakcie realizacji ataku częstym działaniem przestępców jest modyfikacja procesów logowania i czyszczenie logów na zainfekowanych urządzeniach. Zaleca się wdrożenie mechanizmów monitorujących tego typu zdarzenia.

3. Privilege Escalation

3.1. **Ograniczenie wykorzystywanie lokalnych kont administratorów i zastosowanie rozwiązań klasy PAM (Privilieged Access Management)** – w celu ograniczenia bezpośrednio wykorzystywania kont administratorów zaleca się wdrożenie w organizacji rozwiązań klasy PAM (Privilieged Access Management). Rozwiązania umożliwiają zabezpieczenia dostępu do kont administracyjnych oraz monitorowania ich wykorzystania. Należy również rozpatrzeć osobne mechanizmy logowania lub nagrywania sesji administracyjnych.

3.2. **Monitorowanie i ograniczenie wykorzystywania LOLBins**[13] oraz ich obecności w drzewach procesów, mogą tu być pomocne rozwiązania klasy EDR/XDR. Rozważenie wykluczenia możliwości ich użycia.

3.3. **Weryfikacja zapytań do LDAP** – wdrożenie mechanizmów monitorujących zapytania do LDAP pod kątem możliwości ataków „Password Spraying", „BruteForce", wykrywanie próby enumeracji LDAP. Przykładowa reguła SIGMA: *https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/ldap/win_ldap_recon.yml*

3.4. **Weryfikacja i monitorowanie pojawienia się nowych kontrolerów domeny oraz synchronizacji pomiędzy nimi** – wdrożenie mechanizmów monitorowania pojawienia się nowych kontrolerów domeny.

3.5. **Utworzenie kont użytkowników typu „Canary"** – utworzenie w organizacji kont typu „Canary", które nie będą przez nikogo wykorzystywane; Aktywność i próby logowania na wskazane konta powinna być monitorowana i alertowana, ponieważ może świadczyć o ewentualnych próbach przełamania zabezpieczeń lub eskalacji uprawnień.

3.6. **Wykrywanie enumeracji SMB** – wdrożenie reguł monitorowania prób enumeracji udziałów SMB, przykładowe wywołanie:
smbmap -u "" -p "" -P 445 -H <DC IP> && smbmap -u "guest" -p "" -P 445 -H <DC IP>, smbclient -U '%' -L //<DC IP> && smbclient -U 'guest%' -L //

4. Defense Evasion

4.1. **Stosowanie listy dozwolonych aplikacji** – użytkownicy nie powinni mieć możliwości instalacji oraz używania (portable) aplikacji, które nie zostały sprawdzone pod kątem bezpieczeństwa i dopuszczone w organizacji do użytkowania. Lista aplikacji powinna być aktualizowana i utrzymywana. Kolejnym działaniem powinno być utrzymywanie centralnego repozytorium aplikacji, z którego użytkownicy mogą pobierać aplikacje dopuszczone do użytkowania w organizacji.

4.2. **Monitorowanie dezaktywacji mechanizmów bezpieczeństwa** – wdrożenie mechanizmów wykrywania i alertowania odnośnie wyłączenia usług/procesów antywirusa/EDR/XDR/HIPS. Monitorowanie Event ID 7040 w „Auditing Windows Services" pod kątem zmian w uruchamianych usługach bezpieczeństwa.

4.3. **Wzajemne monitorowanie się agentów bezpieczeństwa** – raportowanie w momencie, gdy którykolwiek z mechanizmów bezpieczeństwa zostaje wyłączony, a pozostałe działają; jeżeli to możliwe wykrywanie procesu reinstalacji np. antywirusa.

4.4. **Wymuszanie aktualizacji sygnatur systemów bezpieczeństwa** i reguł bezpieczeństwa w systemach bezpieczeństwa.

4.5. **Monitorowanie wywoływania polecenia net.exe stop oraz net.exe start** – Przykładowe wykorzystanie *net.exe stop „nazwa_usługi"*, w celu zatrzymania usługi.

[13] Więcej informacji na temat LOLBins: https://socprime.com/blog/what-are-lolbins/

4.6. **Monitorowanie kluczy rejestru odpowiedzialnych za rozwiązania bezpieczeństwa** – wdrożenie mechanizmów monitorowania i alertowania w przypadku modyfikacji kluczy rejestru odpowiedzialnych za rozwiązania bezpieczeństwa oraz Security System np. *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*

4.7. **Monitorowanie zmian w konfiguracji backupów stacji roboczej (VSSADMIN)** – wdrożenie mechanizmów wykrywania i alterowania zmian w konfiguracji backupu stacji roboczej np. poprzez wykorzystanie wbudowanych narzędzi vssadmin.exe do modyfikacji ustawień „*shadow copy*".

4.8. **Monitorowanie polecenia taskkill.exe, Pskill.exe** – polecenia te mogą być wykorzystywane do wyłączenia mechanizmów i agentów bezpieczeństwa zainstalowanych na hoście. Przykładowe wywołanie wyłączające oprogramowanie antywirusowe Sophos: *cmd.exe /C taskkill /F /IM SavService.exe*

4.9. **Monitorowanie pojawiających się hostów w sieci** – wdrożenie mechanizmów wykrywania nowych niezautoryzowanych urządzeń w sieci wewnętrznej.

4.10. **Monitorowanie zmian w konfiguracji zaplanowanych zadań** – wdrożenie mechanizmów monitorowania modyfikacji konfiguracji zaplanowanych zadań w systemie.

4.11. **Monitorowanie wykorzystania polecania sc.exe** – zaleca się monitorowania wykorzystywania wbudowanego oprogramowania *sc.exe*. Ransomware może wykorzystać je do instalacji, modyfikacji lub wyłączenia usług. Może być również wykorzystywana do wyłączenia mechanizmów bezpieczeństwa.

5. Credential Access

5.1. **Wdrożenie wielowarstwowych zabezpieczeń –** celem lepszego zabezpieczenia organizacji, w tym przede wszystkim systemów krytycznych, warto rozważyć zastosowanie podejścia „Defense in Depth", w zakres którego wchodzi m.in. wdrożenie wielowarstwowych zabezpieczeń (ochrona styku sieci organizacji z Internetem, systemy wykrywania włamań, segmentacja sieci, ochrona stacji roboczych) oraz implementacja mechanizmów ograniczających dostęp na różnych poziomach infrastruktury sieciowej (np. poziomy uprawnień, segmentacja sieci). Warto rozważyć również wdrożenie list kontrolnych dostępu (ACL), aby ograniczyć dostęp do zasobów tylko do uprawnionych użytkowników i urządzeń.

5.2. **Higiena tożsamości** – wdrożenie w organizacji wymogu korzystania z uwierzytelnienia wieloskładnikowego (MFA). Stworzenie procesu zarządzania tożsamościami i dostępami (IAM) m.in. poprzez regularne przeglądy uprawnień celem zminimalizowania sytuacji, w której pracownicy posiadają uprawnienia niebędące im potrzebne do wykonywania obowiązków służbowych oraz usuwanie nieużywanych lub nieaktywnych kont użytkowników.

5.3. **Monitorowanie aktywności użytkowników** – wdrożenie systemów monitorujących logowania i aktywność użytkowników oraz zapewnienie obsługi alertów na możliwe najwyższym akceptowalnym poziomie.

5.4. **Budowanie świadomości pracowników** – prowadzenie regularnych szkoleń dotyczących cyberzagrożeń i ochrony zasobów informacyjnych, umiejętności rozpoznawania prób ataku i sposobów oraz procedur zgłaszania incydentów.

5.5. **Ochrona kont administratorów** – wdrożenie dodatkowych zabezpieczeń dla kont użytkowników uprzywilejowanych, w tym posiadających uprawnienia administracyjne. Konta tego typu nie powinny być wykorzystywane do codziennej pracy niewymagającej podwyższonych uprawnień. Ograniczenie do niezbędnego minimum liczby kont mających uprawnienia Enterprise Administrator lub Domain Administrator.

5.6. **Separacja uprawnień administratorów domeny - AD Tier model** – zaleca się wprowadzenie separacji uprawnień administratorów np. wdrożenie AD Tier model

– rozdzielenie uprawnień kont administracyjnych na trzy poziomy, zgodnie zaleceniami Microsoft[14].

5.7. **Wykrywanie i blokowanie uruchomień programów realizujących zrzuty pamięci z procesu LSASS** – w celu pozyskania poświadczeń z tego procesu cyberprzestępcy często wykorzystują narzędzia takie jak Mimikatz, Sysinternals ProcDump, PPLdump, HandleKatz, nanodump. Zaleca się wdrożenie mechanizmów wykrywających działanie tego typu narzędzi oraz próby realizacji zrzutów pamięci, a także wdrożenie mechanizmów zabezpieczających przed takim działaniem np. ASR for LSASS.

5.8. **Wdrożenie LAPS (Local Administratora Password Solution)** – tam gdzie jest to możliwe zaleca się wdrożenie mechanizmów LAPS dla lokalnych kont administracyjnych.

6. Discovery

6.1. **Monitorowanie prób rozpoznania połączeń sieciowych poprzez arp.exe** – wdrożenie mechanizmów **wykrywanie** wywoływania komendy *arp.exe -a*, która może być wywoływana przez złośliwe oprogramowanie w celu rozpoznania infrastruktury.

6.2. **Monitorowanie prób rozpoznania poprzez nslookup.exe** – wdrożenie mechanizmów wykrywania prób rozpoznania poprzez niestandardowe wywołanie komendy nslookup.

6.3. **Monitorowanie wykorzystania innych narzędzi i komend** – wdrożenie mechanizmów wykrywania wykorzystania narzędzi i komend**,** które mogą być użyte przez atakujących, a są wykorzystywane tylko w szczególnych przypadkach przez wykwalifikowany i uprawniony personel np. komendy net: *net view / GetIPNetTable*

7. Lateral Movement

7.1. **Segmentacja sieci** – zaleca się odseparowanie poszczególnych sieci i podsieci w organizacji. Wdrożenie odpowiedniej segmentacji sieci w znaczący sposób utrudnią atakującym rozprzestrzenienie ataku ransomware.

[14]https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model
https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/tier-model-for-partitioning-administrative-privileges

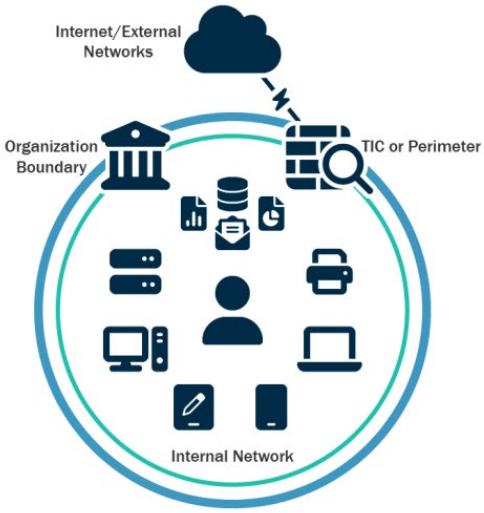

Figure 2: Flat (Unsegmented) Network

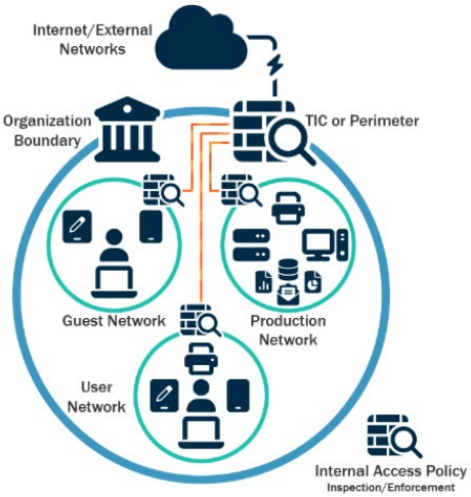

Figure 3: Segmented Network

Rysunek 1 Przykładowy schemat segmentacji sieci[15]

7.2. **Monitorowanie wykorzystywania RDP** – wdrożenie mechanizmów monitorowania prób połączeń z wykorzystaniem protokołu RDP w miejscach gdzie hostami źródłowymi nie są stacje przesiadkowe.

7.3. **Monitorowanie wykorzystywania RDP** – wdrożenie mechanizmów monitorowania prób połączeń z wykorzystaniem protokołu RDP w miejscach gdzie hostami źródłowymi nie są stacje przesiadkowe.

7.4. **Zabezpieczenie kontrolerów domeny** – kontrolery domeny są częstym celem w trakcie ataku ransomware ze względu na potencjał do uzyskania szerszych dostępów do pozostałych elementów infrastruktury. Należy w szczególny sposób zadbać o ich bezpieczeństwo. W tym celu zaleca się wdrożenie zabezpieczeń zgodnie z zaleceniami Microsoft[16] a także prowadzenie testów bezpieczeństwa kontrolerów domeny w celu weryfikacji ich poziomu bezpieczeństwa z wykorzystaniem narzędzi takich jak np. BloodHound, Adalanche lub PingCastle.

8. Persistence:

8.1. **Monitorowanie kluczy rejestru wykorzystywanych przez atakujących** – wdrożenie mechanizmów monitorowania i alertowania modyfikacji w kluczach rejestru wykorzystywanych przez atakujących do utrzymania dostępów do infrastruktury (persystencja) np.:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

8.2. **Monitorowanie kluczy rejestru tworzonych dla nowych usług** – wdrożenie mechanizmów monitorowania dodawania nowych usług poprzez modyfikację kluczy rejestru *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*

[15] https://www.cisa.gov/resources-tools/resources/stopransomware-guide

[16] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

9. Command and Control:

9.1. **Monitorowanie połączeń do znanych serwerów Command&Control (C2)** – wdrożenie mechanizmów monitorowania ruchu sieciowego pod kątem komunikacji z serwerami Command&Control (C2). Zaleca się także sprzężenie mechanizmów proxy z listami niebezpiecznych stron np. prowadzoną przez CERT Polska[17].

9.2. **Wdrożenie reguł i monitorowanie wykrytych prób beaconingu do serwerów C2** – zaleca się uruchomienie analityki ruchu sieciowego w mechanizmach klasy, proxy, IDS/IPS lub firewallach, w celu odnalezienia wzorców połączeń świadczących o beaconingu[18] cyklicznych połączeniach do C2 z podobnym interwałem czasowym). Lub uruchomienie odpowiednich reguł w systemach SIEM jeżeli analizują one flowy sieciowe.[19].

9.3. **Wdrożenie reguł wykrywających komercyjne narzędzia typu Cobalt-Strike** – Przestępcy w swoich atakach często wykorzystują popularne komercyjne narzędzia wykorzystywane w trakcie testów penetracyjnych jak np. Cobalt-Strike. Zaleca się utworzenie lub uruchomienie wbudowanych w rozwiązania bezpieczeństwa reguł, umożliwiających wykrywania wykorzystanie takich narzędzi w infrastrukturze organizacji.

10. Exfiltration

10.1. **Ograniczanie ruchu do węzłów wyjściowych sieci TOR** – zaleca się monitorowanie i ograniczenie ruchu sieciowego wychodzącego pod kątem prób połączeń z sieci wewnętrznej do sieci TOR np. poprzez blokowanie na urządzeniach brzegowych znanych węzłów sieci TOR lub ograniczenia na portach 9001,9030,9090. Zaleca się również ograniczenie możliwości instalacji i wykorzystania przez użytkownika oprogramowania do komunikacji z siecią TOR takiego jak np. torify, Tor browser, torsocks.

10.2. **Organicznie ruchu DNS over HTTPs (DoH)** – atakujący w celu zamaskowania swojej komunikacji wykorzystują mechanizmy komunikacji oparte o DNS over HTTPS. Zaleca się przeprowadzenie analizy pod kątem możliwości ograniczenia takiej komunikacji oraz wdrożenie mechanizmów ograniczających użytkownikom możliwość włączenia jej z poziomu przeglądarki Internetowej [20] . Przykładowe użycie DNS over Https: https://8.8.8.8/resolve?type=TXT&name=onet.pl

10.3. **Monitorowanie lub blokowanie ruchu do serwisów kategorii File-share** – jeżeli nie ma to uzasadnienia biznesowego lub organizacyjnego, zaleca się wprowadzenie ograniczeń odnośnie dostępu i możliwości uploadu plików do serwisów świadczących usługę wymiany plików. Należy ograniczyć i monitorować możliwość uploadu do konkretnych usług.

10.4. **Monitorowanie lub blokowanie ruchu SMB/TFTP/FTP/SFTP do Internetu** – jeżeli nie ma to uzasadnienia biznesowego lub organizacyjnego zalecane jest zablokowanie na urządzeniach brzegowych możliwości połączeń z wykorzystaniem protokołów TFTP/FTP/SFTP lub ograniczenie połączeń do zaufanych usług/hostów w organizacji.

10.5. **Monitorowanie anomalii sieciowych** – zaleca się wdrożenie mechanizmów monitorowania anomalii sieciowych takich jak np. duży wolumen danych wysyłanych do Internetu, niestandardowe godziny występowania ruchu sieciowego. Zaimplementowanie reguł monitoringu, wykresów, jeżeli możliwe uruchomienie

[17] https://cert.pl/lista-ostrzezen/
[18] https://www.elastic.co/security-labs/identifying-beaconing-malware-using-elastic
[19] https://www.elastic.co/security-labs/identifying-beaconing-malware-using-elastic
[20] https://techdocs.akamai.com/etp/docs/disable-doh-browsers

analityki anomalii, zdefiniowanie progów dla transferu dla ruchu wychodzącego, po przekroczeniu którego zostanie wyzwolony alert i przeprowadzona zostanie analiza zdarzenia.

11. Impact

11.1. Utworzenie reguł monitorujących masowy nadpis plików i naruszanie ich integralności. Masowa modyfikacji plików i naruszanie ich integralności może świadczyć o próbie ich szyfrowania.

11.2. Utworzenie reguł wykrywających uruchomienie bibliotek typu pycrypto wykorzystanych w procesach szyfrowania.; Zaleca się utworzenie w EDR/XDR, antywirusach lub narzędziach typu sysmon, reguł monitorujących wykorzystanie bibliotek kryptograficznych, wykorzystywanych do szyfrowania plików przez oprogramowanie, które jest nieznane, nie znajduje się na listach autoryzowanego oprogramowania lub niepodpisane. Do przykładowych bibliotek zaliczyć można: bcrypt.dll, pycrypto, pycryptodome, cryptography. Poniżej przykładowa reguła sysmon; Należy zastosować listę wyjątków w celu ograniczenia potencjalnych detekcji false-positive.

```
<Sysmon schemaversion="4.0">
  <EventFiltering>
    <ImageLoad onmatch="include">
      <ImageLoaded condition="end with">bcrypt.dll</ImageLoaded>
    </ImageLoad>
  </EventFiltering>
</Sysmon>
```

11.3. Zapewnienie bezpiecznych dostępów do kopii zapasowych, tak by użytkownicy nieuprawnieni oraz złośliwe oprogramowanie nie miały do niego dostępu i nie mogły w nie ingerować. Nie należy przechowywać kopii zapasowych na serwerach na których ta kopia została wykonana. W przypadku tworzenia kopii zapasowych przesyłanych do miejsca backupu za pomocą sieci, należy rozważyć stworzenie reguł pozwalających narzędziom i systemom backupowym jedynie na tworzenie nowych kopii zapasowych bez możliwości ich usuwania czy nadpisywania. Należy szczególnie chronić rolę Backup Administrator (przeważnie ma ona dostęp do wszystkich przestrzeni dyskowych).

11.4. Przygotowanie i utrzymanie backupów krytycznych danych – w przypadku ataku ransomware dostępność oraz integralność backupów jest kluczowym elementem pozwalającym w procesie utrzymania ciągłości działania organizacji. Krytycznym elementem procesu tworzenia kopii zapasowych jest regularne testowanie backupów pod kątem poprawności ich wykonywania i możliwości ich odtworzenia. Warto również utrzymywać i regularnie aktualizować tzw. „Golden Image” – wzorcowe obrazy systemów, które w znacznym stopniu usprawnią proces przywracania dostępności infrastruktury.

ZAŁĄCZNIK 2: Przykładowy wzór listy kontaktów w ścieżce eskalacyjnej (lista do własnego uzupełnienia/modyfikacji)

Zasadne jest aby organizacja ustaliła ścieżkę powiadomień z uwzględnieniem, że poszczególne osoby/jednostki będą potrzebowały innego zakresu informacji do podjęcia działań wynikających z poszczególnych kompetencji i wewnętrznych procedur. Dodatkowo, w miarę możliwości, warto również ustalić alternatywne kontakty, w razie gdyby wskazane w liście nie były dostępne, a także alternatywne kanały komunikacji.

Jednostki operacyjne:

DANE OSOBY/ STANOWISKO/ROLA/ NAZWA ZESPOŁU	TELEFEON	E-MAIL	PREFEROWANA FORMA KONTAKTU	GODZINY PRACY
Koordynator incydentów (osoba pełniejąca obowiązki)				
Administrator serwerów				
Zespół sieciowy				

Jednostki zarządcze/raportowe:

DANE OSOBY/ STANOWISKO/ROLA/ NAZWA ZESPOŁU	TELEFEON	E-MAIL	PREFEROWANA FORMA KONTAKTU	GODZINY PRACY
Dyrektor departamentu Cyberbezpieczeństwa				
Kierownik zespołu obsługującego incydent/podejrzenie incydentu				
CISO organizacji				
CSIRT sektorowy				

Dostawcy zewnętrzni:

NAZWA DOSTAWCY	TELEFEON	E-MAIL	PREFEROWANA FORMA KONTAKTU	GODZINY PRACY

Źródła wiedzy:

https://attack.mitre.org/

https://cert.pl/lista-ostrzezen/

https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/tier-model-for-partitioning-administrative-privileges

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://medium.com/@DatBoyBlu3/sigma-rule-psexec-command-execution-684bbc036cbe
https://socprime.com/blog/what-are-lolbins/

https://techdocs.akamai.com/etp/docs/disable-doh-browsers

https://unit42.paloaltonetworks.com/trigona-ransomware-update/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

https://www.cisa.gov/resources-tools/resources/stopransomware-guide

https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf

https://www.cisa.gov/stopransomware

https://www.elastic.co/security-labs/identifying-beaconing-malware-using-elastic

https://www.hhs.gov/sites/default/files/medusalocker-ransomware-analyst-note.pdf