NASK

CERT.PL

Poradnik ransomware

Poradnik ransomware

Poradnik ten jest dedykowany dla małych organizacji i osób fizycznych. Przedstawiamy w nim najważniejsze aspekty, które stosunkowo małym nakładem pracy pomogą znacznie ograniczyć ryzyko i skutki infekcji złośliwym oprogramowaniem typu ransomware.

Spis treści

Co to jest ransomware?

Ransomware to rodzaj złośliwego oprogramowania, infekującego oraz blokującego system komputerowy poprzez zaszyfrowanie wybranych plików. Często okno lub plik zawierający instrukcję odszyfrowania, sugeruje, że odzyskanie danych możliwe jest wyłącznie po wpłacie określonej kwoty na konto atakującego. W coraz większej liczbie przypadków, atakujący nie tylko szyfrują dane, ale także wykradają je, grożąc upublicznieniem w przypadku nie zapłacenia okupu. Warto pamiętać, że zapłacanie okupu nie zawsze gwarantuje odzyskanie danych.

Wykorzystywane przez złośliwe oprogramowanie szyfry, poprawnie użyte gwarantują, że zaszyfrowane dane nie będą mogły zostać odszyfrowane bez klucza deszyfrującego, znajdującego się w posiadaniu przestępców.

Sporadyczne błędy w kodzie oprogramowania, lub upublicznienie odpowiednich kluczy, mogą pozwolić na odzyskanie zaszyfrowanych plików, jednak nie są to częste sytuacje.

Najczęstszym źródłem ataku złośliwego oprogramowania tego typu są:

- podatności w publicznie dostępnych usługach – VPN, RDP, serwer pocztowy, itp. Często podatności są wykorzystywane już w ciągu godzin, lub dni po pojawieniu się publicznej informacji o ich istnieniu,
- niewystarczająco zabezpieczone (najczęściej słabe hasło) kanały zdalnego dostępu do infrastrukturyoraz publicznych usług – RDP, VNC, FTP, bazy danych, itp.,
- maile nakłaniające do pobrania i uruchomienia załączonego lub umieszczonego w linku pliku.

Działania prewencyjne

Weryfikacja procedur wykonywania kopii zapasowych

Wspomniany wcześniej cel ransomware to zmuszenie do zapłaty okupu za możliwość odszyfrowania danych, znajdujących się na dotkniętych atakiem serwerach lub stacjach roboczych. Dlatego tak ważne jest posiadanie sprawnych i zweryfikowanych procedur odzyskania danych z kopii zapasowych. W szczególności mowa tutaj o wszystkich systemach zawierających informacje kluczowe dla funkcjonowania podmiotu, np. dane pacjentów, informacje o leczeniu, informacje o kontrahentach, dane kadrowo-płacowe, ale także obrazy systemów operacyjnych, oprogramowania wykorzystywanego przez pracowników.

W związku z kopiami zapasowymi, należy zbadać następujące zagadnienia:

- czy takie procedury są zaimplementowane?
- czy treść kopii zapasowych jest aktualna?
- czy cyklicznie wykonywane są kopie zapasowe?
- czy kopie zapasowe są przechowywane w sposób trwały i odporny? (w szczególności należy zwrócić uwagę, by kopia zapasowa nie była podłączona jako zasób sieciowy w sieci roboczej)
- czy kopia zapasowa faktycznie daje możliwość odtworzenia pracy?
- czy przeprowadzane są cykliczne testy utworzonych kopii zapasowych?

Jedną ze strategii tworzenia kopii zapasowych jest reguła 3-2-1, mówiąca o tym, że:

- należy przechowywać co najmniej 3 kopie danych,
- co najmniej dwie z nich powinny być przechowywane na różnych nośnikach danych,
- co najmniej jedna kopia powinna być odizolowana, w celu uniknięcia jej zaszyfrowania przez ransomware.

Ważne jest również regularne testowanie kopii zapasowych, pod kątem późniejszego przywrócenia danych. Zapobiegnie to sytuacji, gdzie pomimo utworzonych backupów, nie udało się przywrócić stanu sprzed infekcji ze względu na błąd w kopii.

Regularna aktualizacja oprogramowania

Oprócz weryfikacji procedur wykonywania kopii zapasowych, należy również pamiętać o aktualizacji systemu, usług dostępnych z poziomu internetu oraz aplikacji z których korzysta użytkownik, takich jak przeglądarki, programy biurowe, pocztowe, itp.

Segmentacja sieci

Ważne jest zapewnienie separacji logicznej lub fizycznej pomiędzy różnymi działami lub komórkami firmy, co, przy odpowiedniej konfiguracji, pozwoli na ograniczenie skutków infekcji w sieci. Temat jest na tyle złożony, że nie będzie w szczegółach rozwijany w tym poradniku.

Inwentaryzacja publicznie dostępnych usług

Obecnie, infekcje złośliwym oprogramowaniem ransomware najczęściej są zapoczątkowane poprzez niezabezpieczone lub podatne usługi dostępne z poziomu internetu. Dlatego tak ważne jest zinwentaryzowanie, spisanie usług udostępnionych w sieci, a następnie określenie aktualnego stanu oprogramowania, które udostępniają te usługi w sieci. Dzięki inwentaryzacji można upewnić się czy:

- dana usługa rzeczywiście powinna być dostępna z poziomu internetu?
- oprogramowanie udostępniające usługę jest odpowiednio zaktualizowane lub czy są zaaplikowane najnowsze łatki bezpieczeństwa?

- zastosowana jest odpowiednia polityka haseł, oraz jeśli to możliwe, uwierzytelnianie wieloskładnikowe?

W przypadku koniecznego zdalnego dostępu do usług czy zasobów placówki, silnie sugerujemy wprowadzenie dodatkowych środków bezpieczeństwa (np. udostępnienie zdalnego pulpitu tylko przez firmowy VPN z dwuskładnikowym uwierzytelnianiem).

Należy pamiętać, że przeprowadzona inwentaryzacja przedstawia jedynie stan obecny który szybko może się zdezaktualizować. Konieczne jest wprowadzenie polityki ciągłego zarządzania i dokumentowania zmian oraz procesu monitorowania i zarządzania podatnościami.

Zabezpieczenie potencjalnych źródeł infekcji

Częstym pierwszym etapem ataku jest infekcja pojedyńczego komputer pracownika, celem uzyskania dostępu do sieci firmowej. Ryzyko to można ograniczać zarówno na warstwie technicznej jak i ludzkiej. Infekcja z wykorzystaniem maili phishingowych. Maile phishingowe w dużej części odpowiadają za infekcję złośliwym oprogramowaniem. Dlatego tak ważne jest zwrócenie uwagi na ten potencjalny wektor infekcji.

Z punktu widzenia użytkownika ważne jest, aby:

- upewnić się czy nie doszło do podszycia w celu zachęcenia odbiorcy do uruchomienia załączonego szkodliwego pliku,
- zwrócić uwagę na rozszerzenia załączonych plików,
- w przypadku gdy w treści wiadomości zostało umieszczone hiperłącze, należy sprawdzić czy prowadzi ono do znanej i zaufanej strony.

Jako administrator, należy zwrócić uwagę na:

- filtrowanie maili z wykorzystaniem filtrów antyspamowych oraz ze względu na typ rozszerzenia pliku w załączniku,
- zastosowanie polityki bezpieczeństwa, odgórnie zapobiegającej uruchomieniu kodu w potencjalnie złośliwych dokumentach, tj. makr – dotyczy to w szczególności dokumentów z pakietu MS Office (rozszerzenia .doc, .docx, .xls, .xlsx)
- włączenie mechanizmów poczty, pozwalających na weryfikację nadawcy wiadomości.

Utwardzenie stacji roboczej

Gdy dojdzie już do próby uruchomienia złośliwego oprogramowania, istnieje szereg technicznych zabezpieczeń które organizacja może wdrożyć, aby to się nie powiodło:

- wykorzystanie regularnie aktualizowanego oprogramowania antywirusowego,
- konfigurację Access Control List (ACL) w celu zapewnienia minimalnych, niezbędnych uprawnień dla użytkowników. Jeśli użytkownik nie potrzebuje możliwości zapisu do danego katalogu lub zasobu – należy nadać uprawnienia tylko do odczytu, co ograniczy potencjalne straty,
- wykorzystanie rozwiązań Software Restriction Policies (SRP), AppLocker lub WDAC w celu zdefiniowania dozwolonych lokalizacji z których oprogramowanie może być uruchamiane:
  - foldery System oraz System32,
  - foldery Program Files oraz ProgramFiles (x86),
  - w przeciwieństwie do powyższej metody, możliwe jest zablokowanie wykonania programów z lokalizacji popularnych wśród złośliwego oprogramowania:
  - foldery tymczasowe,
  - foldery AppData oraz lokalne LocalAppData,
  - foldery ProgramData oraz UserProfile.
- reguły przed wdrożeniem produkcyjnym powinny zostać dokładnie przetestowane i dostosowane do wymagań organizacji. W niektórych przypadkach mogą spowodować zaprzestanie działania niezbędnego oprogramowania.
- ograniczenie możliwości uruchomienia skryptów Powershell, ze względu na coraz częstsze wykorzystanie ich w atakach ransomware.

Aktywne monitorowanie zdarzeń w sieci

Bieżące monitorowanie oraz bezpieczne przechowywanie logów z urządzeń w sieci, jest podstawą do sprawnej detekcji oraz skutecznego zablokowania ataku. Usprawni to również analizę powłamaniową w przypadku ewentualnego incydentu.

Poniżej opisane zostały ważniejsze zagadnienia związane z logowaniem oraz monitorowaniem urządzeń:

- wysyłanie logów z urządzeń do centralnego serwera logów. Uwzględnienie ich w regularnie wykonywanych kopiach zapasowych,
    - logi na serwerze powinny być przechowywane przez minimum 14 ostatnich dni.
- skorzystanie z systemów IDS, bieżąco analizujących logi z urządzeń,
- dla systemów Windows:
    - zwiększenie informacji o logowanych zdarzeniach poprzez włączenie oraz poprawne skonfigurowanie Audit Logging,
    - włączenie oraz poprawne skonfigurowanie serwisu Sysmon, służącego jako dodatkowe uzupełenie informacji z Audit Logging,
    - włączenie i odpowiednie skonfigurowanie usługi WEF (Windows Event Forwarding) pozwalającej na przesłanie wybranych logów do wskazanego serwera WEC (Windows Event Collector),
- dla systemów Linux:
    - włączenie oraz poprawne skonfigurowanie usługi Syslog.

Działania naprawcze

Izolacja zainfekowanej maszyny

W pierwszym kroku najważniejsze jest określenie, które maszyny zostały zainfekowane oraz ich odłączenie od sieci (zarówno przewodowej jak i bezprzewodowej). Należy pamiętać, że wyłączenie komputerów powinno być wykonane tylko i wyłącznie, gdy niemożliwe jest odłączenie urządzenia od sieci. Pamięć ulotna może zawierać informacje niezbędne do analizy incydentu, jak i późniejszego odzyskania zaszyfrowanych danych.

Możliwe jest także pozostawienie go w trybie hibernacji. Dodatkowo, zalecane jest wykonanie kopii zapasowej zainfekowanych plików - w przypadku, gdy w danym momencie nie będzie możliwe odszyfrowanie plików, umożliwi to dostęp do utraconych danych w przypadku pojawienia się dekryptora.

Identyfikacja oraz eliminacja źródła infekcji

Ważnym krokiem przy identyfikacji źródła infekcji jest analiza dostępnych logów zdarzeń pod kątem nietypowych działań czy połączeń sieciowych. Ważne jest jego wyeliminowanie, chociażby poprzez aktualizację usługi czy usunięcie publicznie dostępnej instancji, ponieważ atakujący mogą ponownie przeprowadzić atak.

Identyfikacja rodziny ransomware

Po wyeliminowaniu zagrożenia, kolejnym najważniejszym działaniem jest określenie rodziny oprogramowania szyfrującego. Najczęściej, jest to możliwe poprzez analizę notatki z okupem oraz przykładowych zaszyfrowanych plików.

Z pomocą przychodzą dwa narzędzia – nomoreransom.org oraz id-ransomware.malwarehunterteam.com. Na podstawie dostępnych

danych, składających się z adresów mailowych pochodzących z notatek okupu, rozszerzeń zaszyfrowanych plików, adresów portfeli Bitcoin itp., możliwe jest określenie, w przybliżeniu, rodziny ransomware z którą mamy do czynienia. W przypadku istnienia dekryptora do znalezionej rodziny, zostanie wyświetlona instrukcja postępowania pozwalająca na próbę odzyskania plików.

W przypadku znalezienia odpowiedniego dekryptora na wspomnianej stronie, w celu odszyfrowania danych należy postępować ściśle według załączonej instrukcji dla danego narzędzia.

Przywrócenie działania systemów

Po identyfikacji zagrożenia, kolejnym krokiem jest przywrócenie działania systemów priorytetyzując krytyczne dla działania firmy. Wykorzystujemy do tego czyste, prekonfigurowane obrazy systemów.

Zgłoszenie incydentu

W przypadku wykrycia infekcji oprogramowaniem szyfrującym, należy podjąć niezwłoczny kontakt z zespołem CSIRT NASK poprzez stronę incydent.cert.pl albo e-mail cert@cert.pl. W przypadku kontaktu, rekomendowane jest dołączenie następujących plików:

- minimum 2 zaszyfrowane pliki,
- notatka z żądaniem okupu od przestępcy.

Rekomendowane jest również wysłanie następujących plików, w przypadku gdy jest to możliwe:

- próbka złośliwego oprogramowania, która zainfekowała maszynę,
- logi z zainfekowanej maszyny oraz systemów bezpieczeństwa z czasu infekcji,
- oryginały plików, które zostały zaszyfrowane, jeżeli się zachowały.

Źródła wiedzy

https://www.cisa.gov/stopransomware/ransomware-guide

https://www.cyber.gov.au/sites/default/files/2020-11/FINAL_ACSC_Prevention-And-Protection-Guide_v8.pdf

https://docs.microsoft.com/en-us/archive/msdn-magazine/2008/november/access-controlunderstanding-windows-file-and-registry-permissions

https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-lists

https://docs.microsoft.com/en-us/windows-server/identity/software-restriction-policies/softwarerestriction-policies

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defenderapplication-control/applocker/applocker-overview

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defenderapplication-control/wdac-and-applocker-overview

https://www.ncsc.gov.uk/guidance/macro-security-for-microsoft-office

https://docs.microsoft.com/en-us/DeployOffice/security/plan-security-settings-for-vba-macros-inoffice

https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-eventforwarding-to-assist-in-intrusion-detection

https://www.cert.govt.nz/it-specialists/critical-controls/network-segmentation-andseparation/architecting-your-network/

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-securityaudit-policy-settings

https://github.com/SwiftOnSecurity/sysmon-config

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

https://www.cyber.gov.au/acsc/view-all-content/publications/securing-powershell-enterprise

NASK

CERT.PL