CYBERSECURITY FOUNDATION

Przegląd rozwiązań EDR_XDR

EDYCJA 2

Symulacja ofensywnych ataków fileless z uwzględnieniem widoczności incydentów w telemetrii

Wykorzystane narzędzia: Metasploit, Atomic Red Team Framework, Caldera Framework

2024

na skróty

I Widoczności ataków w telemetrii i reagowanie na incydenty z perspektywy SOC (Security Operation Center)

Rozwiązania klasy Endpoint Detection and Response (EDR) oraz eXtended Detection and Response (XDR) wywodzą się z rozwijanej na przestrzeni lat wielowarstwowej ochrony punktów końcowych. Głównym ich zadaniem jest monitorowanie w czasie rzeczywistym systemów operacyjnych i aplikacji w chmurze. Prawidłowo wdrożone podnoszą na wyższy poziom wyszukiwanie zagrożeń pozwalając dostrzec wskaźniki kompromitacji. Dla każdej firmy może to oznaczać dostęp do przydatnych informacji ze wszystkich punktów końcowych, co na pewno przyczyni się do lepszego zabezpieczenia całej sieci, jak również pracowników przed cyberatakami.

Korzystanie z produktów tej klasy daje podgląd na techniczne informacje z całej infrastruktury. Innymi słowy obserwacja telemetrii z cyberataków daje szerszy obraz tego, co się działo w przeszłości i co aktualnie ma miejsce na punktach końcowych.

Jak udowadnia ten test, dzięki korelacji incydentów ze systemów operacyjnych oprogramowanie EDR-XDR może stanowić istotną wartość dla dużych oraz małych organizacji o dowolnym poziomie umiejętności technicznych. Jednocześnie zwracamy uwagę, aby wdrożenie tej klasy produktu było świadomą strategią ochrony przed cyberatakami.

II

EDR a XDR – różnice

Rozwiązania EDR zazwyczaj koncentrują się wyłącznie na bezpieczeństwie punktów końcowych (ang. endpoint), podczas gdy XDR obejmuje szerszy zakres integracji systemów. Oba rozwiązania mają na celu identyfikację i reagowanie na zagrożenia cybernetyczne, lecz to XDR wspiera więcej źródeł danych m.in.: urządzenia mobilne, czujniki IoT, aplikacje Web 2.0 takie jak Google Workspace i Microsoft Office, logi sieciowe z urządzeń brzegowych, systemy IDS, SIEM itp. Ostateczny wybór pomiędzy EDR a XDR powinien zależeć od potrzeb i złożoności środowiska IT danej organizacji, jednocześnie już teraz w pewnych kategoriach bezpieczeństwa granice pomiędzy EDR a XDR zaczynają się zacierać.

Podstawowe różnice pomiędzy rozwiązaniami EPP » EDR » XDR

	EPP	EDR	XDR
INTEGRACJA Z INFRASTRUKTURĄ IT	Podstawowe elementy infrastruktury IT, niektóre aplikacje i usługi biznesowe.	Szerszy zakres systemów bezpieczeństwa, aplikacje i usługi biznesowe.	Najszerszy zakres systemów bezpieczeństwa, aplikacje i usługi biznesowe, chmura obliczeniowa, urządzenia IoT.
ZAKRES MONITOROWANIA	Monitorowanie punktów końcowych. Wykrywanie i blokowanie złośliwego oprogramowania.	Monitorowanie punktów końcowych. Wykrywanie i reagowania na bardziej zaawansowane zagrożenia.	Monitorowanie punktów końcowych, sieci i aplikacji w chmurze. Zapewnienie kompleksowego widoku bezpieczeństwa.
REAGOWANIE NA CYBERATAKI	Dosyć ograniczone zapobieganie, wykrywanie i automatyczne reagowanie.	Zaawansowane zapobieganie, wykrywanie i reagowanie, izolacja oraz automatyzacja.	Detekcja i zapobieganie atakom z najbardziej różnorodnych różnych obszarów. Dostępność tzw. Threat Hunting.

* Powyższa tabela zawiera wiele uproszczeń. Nie wszystkie cechy da się przyporządkować do jednej kategorii produktu. Na przykład rozwiązania EPP ewoluowały do EDR, a różnice pomiędzy EDR a XDR nie są już tak duże jak dawniej. Zachowano wspólny rdzeń, czyli zaawansowaną ochronę stacji roboczych przed zagrożeniami i cyberatakami, ale to EDR i XDR potrafią lepiej korelować logi z różnych punktów końcowych. Dodatkowo zapewniają najbardziej szczegółową widoczność danych oraz umożliwiają polowanie na zagrożenia tzw. Threat Hunting, co skutecznie zabezpiecza punkty końcowe.

Dlaczego warto

Dlaczego warto rozważyć wdrożenie EDR?

Dzięki EDR osoby odpowiedzialne za bezpieczeństwo IT mogą monitorować i analizować incydenty, które będą skorelowane z procesami systemowymi, plikami, połączeniami sieciowymi, modyfikacjami kluczy rejestru itp. Tutaj automatyzacja, jako że bazuje na maszynowym uczeniu, pozwala szybko zidentyfikować podejrzane lub wyraźnie złośliwe działania na urządzeniach. Jest to kluczowe w wykrywaniu zaawansowanych ataków ATP, w tym ataków 0-day.

Rozwiązania wyposażone w EDR oferują bardzo precyzyjną widoczność zdarzeń z urządzeń końcowych. Niektórzy producenci implementują do nich funkcje znane do tej pory wyłącznie z XDR. Mowa o tak zwanym Threat Hunting, dzięki czemu EDR doskonale sprawdza się w rękach analityków złośliwego oprogramowania. Trzeba też wspomnieć o skutecznych mechanizmach obronnych, takich jak: izolowanie zainfekowanych urządzeń, przeszukiwanie śladów włamań, uzyskiwanie informacji o przebiegu ataku, ujawnienie początkowego wektora ataku, metody rozprzestrzenienia się malware.

Dlaczego warto rozważyć wdrożenie XDR?

XDR łączy w sobie cechy EPP i EDR. Wykorzystuje dane telemetryczne ze wszystkich punktów końcowych, nawet ze systemów i aplikacji w chmurze. Zapewnia kompleksowy i holistyczny widok na bezpieczeństwo całej infrastruktury. Dzięki XDR możliwe jest szybkie i skuteczne identyfikowanie ataków. Zespoły SOC mogą równie szybko podejmować odpowiednie działania zaradcze.

Produkty tej klasy ułatwiają śledzenie nie tylko podejrzanych aktywności na wszystkich poziomach infrastruktury IT, lecz także zdarzeń pozornie zaufanych, gdzie pośród tzw. „systemowego szumu" może znajdować się złośliwy kod napastnika. Rozwiązanie podniesienie na wyższy poziom bezpieczeństwo organizacji wskutek skrócenia czasu reakcji na zagrożenie i automatyczną naprawę systemów po odnotowanym incydencie.

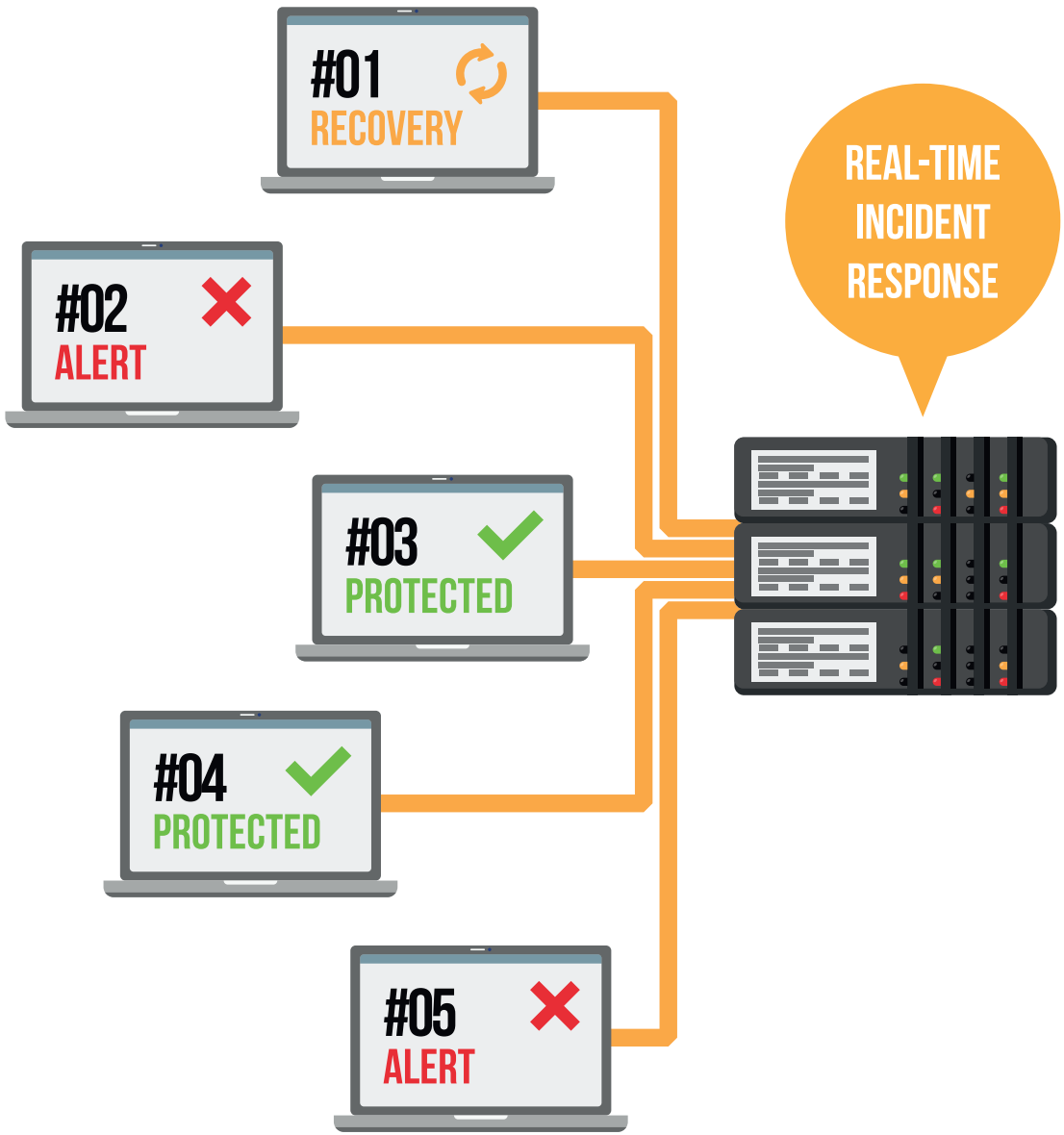
EDR XDR

IV Telemetria i widoczność ataków – cechy wspólne EDR i XDR

Uzasadniając inwestycję w dany produkt do obrony systemów przed cyberatakami przeprowadziliśmy analizę modułów EDR i XDR. Jako Red Team symulowaliśmy działania napastników, którzy już uzyskali dostęp do infrastruktury informatycznej. Jako Blue Team analizowaliśmy dane z tych ataków, aby ocenić możliwości testowanego produktu na wykrywanie i reagowanie na zagrożenie.

Na podstawie zgromadzonych danych uważamy, że najważniejsze jest, aby produkt rejestrował ślady ataków w konsoli administratora. Nie ma znaczenia, czy te zdarzenia zostaną przetworzone automatycznie, czy manualnie przez zespół wykwalifikowanych pracowników. Produkt musi zapewniać widoczność w zdarzenia systemowe wraz z telemetrią, która pozwala zrozumieć kontekstu ataku i wychwycić niezbędne detale techniczne.

W tym badaniu nie sprawdzaliśmy skuteczności ochrony przed cyberatakami. Raczej skupiliśmy się na tym, aby rozwiązanie gwarantowało widoczność incydentów poprzez telemetrię ataku.
Brak widoczności incydentu albo telemetrii może bowiem oznaczać, że produkt nie sprawdził się w boju albo wykrył zagrożenie zbyt późno.



Testowane rozwiązania dla biznesu

Konfiguracja polityk dla agentów antywirusowych zazwyczaj była domyślna lub zawierała dodatkowe ustawienia w celu uzyskania bardziej szczegółowej telemetrii. Co ważne nie wyłączaliśmy ochrony antywirusowej ani żadnych innych funkcji. Rozwiązania, którym po instalacji należało przydzielić predefiniowaną konfigurację agenta, były konfigurowane z możliwe najbardziej utwardzonymi ustawieniami, aby uzyskać szczegółowy wgląd w łańcuch ataku i telemetrię, co było celem tego testu. Na prośbę producentów przydzielaliśmy proponowane ustawienia.

EMSISOFT

Emsisoft Enterprise Security + EDR
ustawienia domyślne

emsisoft.com

eset

Eset Protect Elite + XDR
ustawienia domyślne
+ włączone wszystkie reguły dla EDR

eset.com

Microsoft Defender for Business + EDR
ustawienia domyślne

microsoft.com

SITE METRAS

Metras + EDR
ustawienia domyślne

site.sa

xcitium

Xcitium Advanced + EDR
predefiniowana polityka 8.1

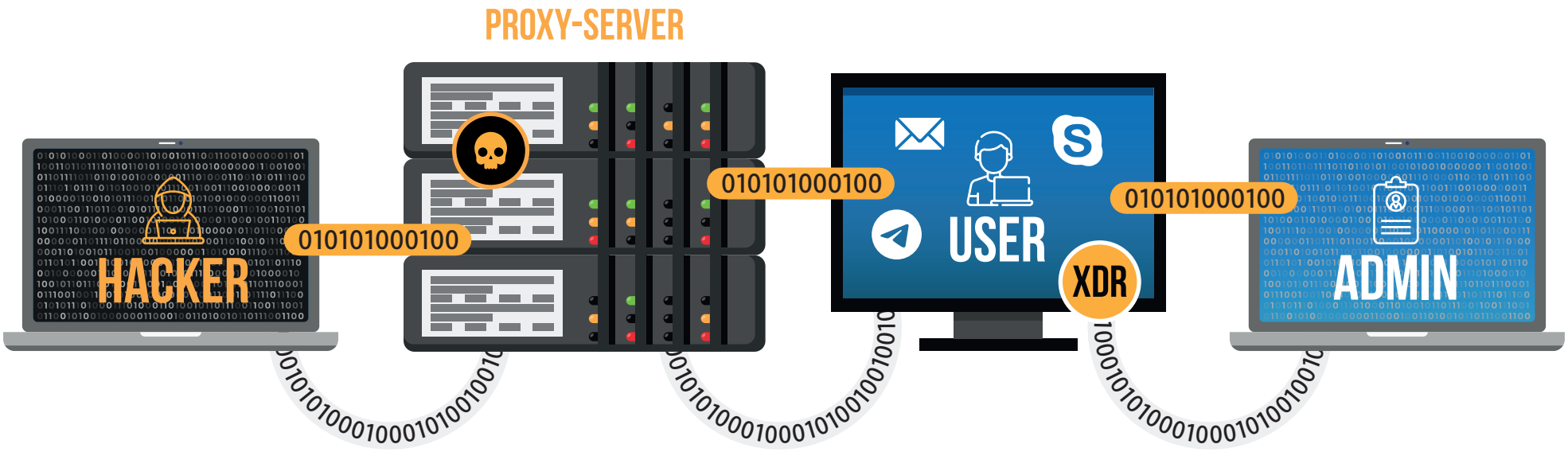
xcitium.com

VI Konfiguracja systemu ofiary oraz agenta

Do zasymulowania ataków wykorzystaliśmy maszynę wirtualną z systemem Kali Linux jako serwer Command and Control z oprogramowaniem Metasploit. Dodatkowo narzędzie Atomic Red Team z predefiniowanymi rodzajami ataków, a także Caldera Framework oraz kilka własnych metod dostarczenia złośliwego ładunku i uruchomienia w systemie operacyjnym.

Maszyny wirtualne z Windows 11 Pro z zainstalowanym agentem danego rozwiązania miały pełny dostęp do Internetu. Zastosowaliśmy całkowicie domyślną konfigurację Windows.

Zrezygnowaliśmy z tworzenia kampanii od początku do końca. Tak zwany payload dostarczaliśmy opisywanymi protokołami z ominięciem socjotechniki, ponieważ rodzaj i cel ataku w symulowanym scenariuszu był znany testerom.



VII

Porównanie cech bezpieczeństwa rozwiązań EDR-XDR

	Emsisoft Enterprise Security	ESET Protect Elite	Metras	Microsoft Defender for Business	Xcitium Advanced
Widoczność ataku	✓	✓	✓	✓	✓
Graficzna wizualizacja ataku (korelacja zdarzeń)	✓	✓	✓	✓	✓
Pełna telemetria ataku	✓	✓	✓	✓	✓
Przybliżona reputacja złośliwego pliku	✓	✓	✓	✓	✓
Możliwość wyszukiwania śladów włamań	✓	✓	✓	✓	✓
Graficzna symulacja bezpieczeństwa (np. podatności w systemach, słabe hasła, niepoprawna konfiguracja agenta)	✗	✓	✗	✓	✓
Wgląd w podejrzane listy obiektów (adresy IP, URL, SHA)	✓	✓	✓	✓	✓
Proponowane środki naprawy po ataku	✓	✓	✗	✓	✗
Dodatkowa opinia o zagrożeniu (piaskownica, VirusTotal, reputacja pliku, inne)	✓	✓	✓	✓	✓
Izolacja stacji roboczej, użytkowania, pliku po wykrytym ataku	✓	✓	✓	✓	✓
Zarządzanie aktualizacjami	✗	✓	✗	✓	✓
Przywracanie danych po ataku (pliki użytkownika)	✓	✗	✗	✗	✗
Zabezpieczenie logowania do panelu administratora	✓	✓	✓	✓	✓
Używane technologie firm trzecich	**Emsisoft, Bitdefender**	**Eset**	**Metras**	**Microsoft**	**Xcitium, Comodo**
Wspierane systemy operacyjne dla EDR/XDR*	**Windows, Windows Server**	**Windows, Windows Server, macOS, Linux**	**Windows, Windows Server, Linux**	**Windows, Windows Server, macOS, Linux**	**Windows, Windows Server**

✱ Ze względu na ograniczenia technologiczne funkcje dla EDR-XDR mogą się różnić dla systemów operacyjnych.

VIII Wyniki na podstawie symulowanych ataków

Głównym celem testu było sprawdzenie widoczności ataków w konsoli rozwiązań EDR-XDR na symulowane działania sieciowe, które powinny być przechwytywane przez zainstalowanego agenta na stacji roboczej.

USER

Próba bądź otworzenie złośliwej strony.

Próba lub otworzenie złośliwego pliku.

HACKER

Brak komunikacji z atakowanym hostem.

Poprawne uruchomienie niebezpiecznego kodu i nawiązanie połączenia z systemem ofiary.

Możliwa eksfiltracja niektórych plików i informacji systemowych.

ADMIN

Alert w konsoli.

Wymagana reakcja administratora.

Atak częściowo widoczny w telemetrii.

Pełna widoczność ataku w konsoli.

Identyfikacja ataku w MITRE ID.

Prewencyjna blokada ataku.

Automatyczna naprawa incydentu.

Brak telemetrii ataku.

Perspektywa postrzegania ataku przez: użytkownika, hakera, administratora.

EMSISOFT

Enterprise Security with EDR

	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
PsExec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			

ESET Protect Elite

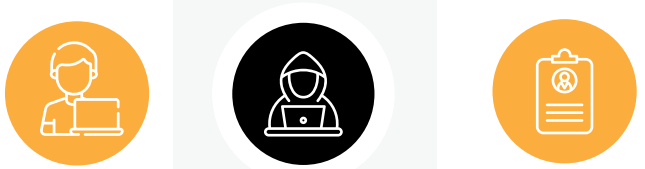
	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
PsExec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			

SITE METRAS

METRAS

	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
PsExec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			

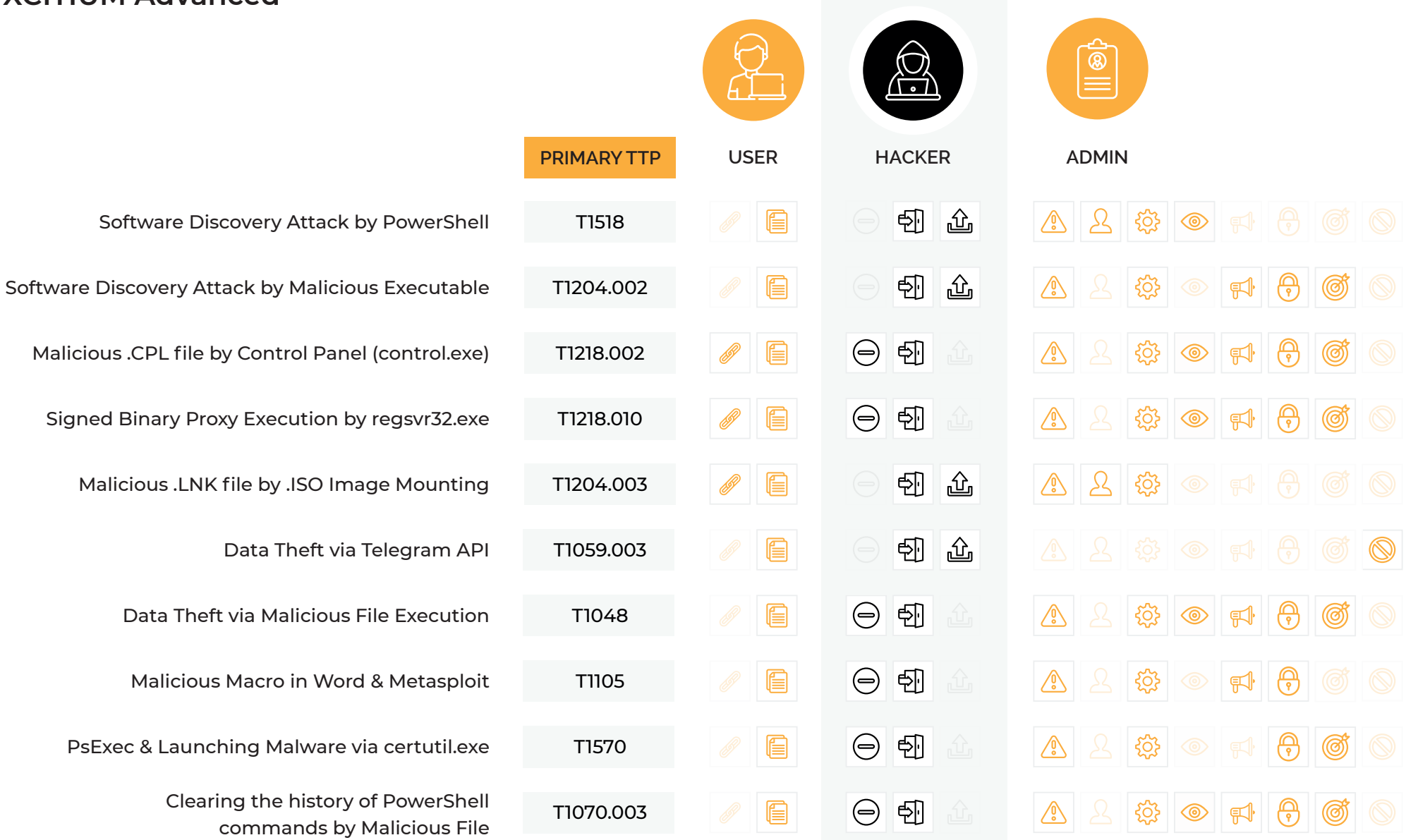
MICROSOFT Defender for Business



	PRIMARY TTP
Software Discovery Attack by PowerShell	T1518
Software Discovery Attack by Malicious Executable	T1204.002
Malicious .CPL file by Control Panel (control.exe)	T1218.002
Signed Binary Proxy Execution by regsvr32.exe	T1218.010
Malicious .LNK file by .ISO Image Mounting	T1204.003
Data Theft via Telegram API	T1059.003
Data Theft via Malicious File Execution	T1048
Malicious Macro in Word & Metasploit	T1105
PsExec & Launching Malware via certutil.exe	T1570
Clearing the history of PowerShell commands by Malicious File	T1070.003

XCITIUM Advanced

	PRIMARY TTP	USER	HACKER	ADMIN
Software Discovery Attack by PowerShell	T1518			
Software Discovery Attack by Malicious Executable	T1204.002			
Malicious .CPL file by Control Panel (control.exe)	T1218.002			
Signed Binary Proxy Execution by regsvr32.exe	T1218.010			
Malicious .LNK file by .ISO Image Mounting	T1204.003			
Data Theft via Telegram API	T1059.003			
Data Theft via Malicious File Execution	T1048			
Malicious Macro in Word & Metasploit	T1105			
PsExec & Launching Malware via certutil.exe	T1570			
Clearing the history of PowerShell commands by Malicious File	T1070.003			



IX

Opis symulowanych ataków

1

T1518 - Software Discovery

W początkowej fazie ataku cyberprzestępcy mogą spróbować pozyskać listę zainstalowanego oprogramowania lub konfiguracji systemu, aby przejść do kolejnego kroku. Aby wyodrębnić podstawowe informacje z atakowanego hosta wykorzystaliśmy polecenie PowerShell.

2

T1204.002 - Software Discovery

W tej metodzie wykorzystaliśmy skrypt zawierający podobne polecenie, co w pierwszym scenariuszu. W teorii uzyskiwaliśmy takie same dane wyjściowe, lecz w praktyce atak może być inaczej interpretowany przez testowane rozwiązanie w konsoli administratora.

3

T1218.002 - Signed Binary Proxy Execution: Control Panel

Do uruchomienia potencjalnie niebezpiecznego pliku użyliśmy zaufanej aplikacji control.exe (Panel Sterowania Windows) z parametrem do pliku z rozszerzeniem .CPL, co pozwala na automatyczne uruchamiane kodu wraz z panelem sterowania. Chociaż w ataku uruchamiany był kalkulator calc.exe, to w prawdziwym scenariuszu może to być dowolne złośliwe oprogramowanie.

4

T1218.010 - Signed Binary Proxy Execution: Regsvr32

W systemie Windows do wykonania kodu z biblioteki DLL potrzeba procesu, który uruchomi plik DLL. Wykorzystaliśmy systemowe narzędzie Regsvr32.exe jako proxy, czyli popularną metodę załadowania pliku DLL do pamięci.

5

T1204.003 - User Execution: Malicious Image

Zastosowaliśmy technikę polegającą na pobraniu obrazu pliku i zamontowaniu tego pliku jako dodatkowy napęd w systemie. To jeden ze sposobów ominięcia zabezpieczeń anty-spam i anty-malware na serwerach dostawców poczty. Co więcej w ten sposób możliwe jest ominięcie zabezpieczeń systemowych w postaci utraty atrybutu Mark-of-the-Web dla pliku, co może utrudnić analizę pliku przez oprogramowanie bezpieczeństwa.

6 T1059.003 – Data Theft via Telegram API

Interfejs API komunikatora Telegram posłużył nam za niestandardową metodę kradzieży plików z atakowanej maszyny. Wykradziony plik wysyłany był do bota Telegram kontrolowanego przez napastnika metodą HTTP POST. W prawdziwym scenariuszu polecenie wykorzystujące API Telegram można zintegrować z dowolnym złośliwym oprogramowaniem. Komunikator Telegram nie jest wymagany w systemie ofiary.

7 T1048 - Data Theft via Malicious File Execution

Wykorzystaliśmy to samo polecenie wykradające pliki z atakowanego hosta, skompilowane do pliku wykonywalnego EXE. Plik może być dostarczony do systemu ofiary najróżniejszymi sposobami.

8 T1105 - Malicious Macro in Word & Metasploit

Używanie dokumentów Word w atakach socjotechnicznych to technika bardzo stara. Ewoluują natomiast metody zaszywania złośliwego kodu. Przygotowane macro wykorzystuje popularną metodę pobrania pliku ze zdalnej lokalizacji i uruchamia plik bez interakcji z ofiarą. W tym scenariuszu może występować wiele technik i taktyk według MITRE.

9 T1570 - PsExec & Launching Malware via certutil.exe

Po raz kolejny używamy legalnego oprogramowania do uruchomienia złośliwego kodu. Tym razem jest to PsExec wchodzące w skład SysInternals. Posłużyło nam do zdalnego zalogowania się do atakowanego hosta, pobrania pliku ze zdalnej lokalizacji za pomocą certutil.exe i uruchomienia malware w systemie z linii poleceń.

10 T1070.003 - Clearing the history of PowerShell commands by Malicious File

W tym scenariuszu użyliśmy narzędzia Caldera to zainstalowania szkodliwego oprogramowania zdalnego dostępu, następnie spróbowaliśmy wyczyścić historii poleceń PowerShell.

X Wnioski z testu i ogólne rekomendacje

W tegorocznej edycji testu sprawdziliśmy zdolność produktów do szybkiego alarmowania, prawidłowego wykrywania ataków i tworzenia łańcucha podejrzanych zdarzeń. Zwracamy uwagę, że niektóre symulowane ataki były już wcześniej dobrze udokumentowane i są znane producentom oraz społeczności ekspertów. Tym niemniej test odzwierciedla możliwości ochronne produktów bezpieczeństwa w starciu z ukierunkowanymi i długotrwałymi atakami APT.

Badanie pozwoliło ocenić kilku liderów rozwiązań EDR-XDR, w tym uwzględniło możliwe podatności produktów na zagrożenia w symulowanym środowisku. Przeprowadzony test pozwolił dowiedzieć się więcej o oprogramowaniu tej klasy:

- Każdy produkt ma swoje wady oraz zalety, dlatego o jego wartości stanowi świadomy wybór organizacji, która na co dzień używa danego rozwiązania i poznała jego mocne i słabe strony.

- Bez modułów EDR-XDR niektóre ataki mogą być całkowicie niewykrywalne dla oprogramowania anty-malware. Brak jakiejkolwiek telemetrii może odznaczać dla zespołu bezpieczeństwa, że nie ma informacji o incydencie. Jest to otwarta droga do częściowego lub całościowego przełamania zabezpieczeń organizacji.

- Atak zwykle zaczyna się od jednego lub grupy komputerów w tej samej podsieci i może tam pozostać wiele tygodni niezauważony – jest to tzw. cykl planowania ataku. Organizacje, dzięki produktom tej klasy, mogą szybciej rozpoznawać sygnały ostrzegawcze i reagować na alerty, aby nie paść ofiarą hakerów.

- Oprogramowanie EDR-XDR nie może zasypywać analityka fałszywymi ostrzeżeniami, dlatego wysoka liczba alertów nie zawsze jest wskazana. Gromadzenie takich danych jest dobre, jeśli bezpieczeństwem zajmuje się dedykowana grupa ekspertów. Szczegółowe pokrycie telemetryczne ataków może dużo powiedzieć o produkcie, ale takie podejście nie sprawdzi tam, gdzie występuje luka kompetencyjna.

- Z tego samego powodu co telemetria, informacje o atakach mogą być frustrujące dla administratorów, jeżeli nie będą precyzyjne. Ataki można sklasyfikować na np. otworzenie w sieci złośliwego pliku, uzyskanie dostępu do aplikacji lub zasobu przy użyciu niezabezpieczonych danych uwierzytelniających, zalogowanie się za pomocą protokołu RDP itp. Bez odpowiedniej widoczności ataków zespół ds. bezpieczeństwa będzie nieskuteczny.

- Alerty w panelu administratora mogą zależeć w dużej mierze od ustawień polityki. Na przykład zdarzenia o niskim ryzyku (w skali od 0 do 10) mogą nie generować ostrzegawczego alertu podczas uruchomienia pliku z lokalizacji %TEMP%, aby nie doprowadzać analityków do szału. Brak alertu nie jest czymś złym w przeciwieństwie do braku telemetrii z ataku.

- Telemetria jest bardzo ważną informacją, ponieważ na jej podstawie analitycy mogą wyszukiwać nieznane złośliwe oprogramowanie lub tworzyć reguły w oparciu o zapisane zdarzenia przez agenta, dzięki czemu możliwe staje się dopasowanie produktu do potrzeb organizacji.

- Telemetria generuje bardzo dużo informacji. Są one zwykle posegregowane według czasu, powiązane z procesami w drzewo i grafy. Najważniejsze, aby wiedzieć, czego szukać oraz nauczyć się czytać logi. W większości rozwiązaniach jest to zrobione podobnie, logi różnią się strukturą zapisu, lecz ogólna zasada jest podobna.

- Niektóre rozwiązania EDR-XDR integrują się z VirusTotal, co pozwala szybko przeszukać zasoby Internetu pod kątem sumy kontrolnej podejrzanego pliku. Oferują też analizę pliku w tzw. piaskownicy lub ręczną analizę przez wykwalifikowany zespół producenta. Warto korzystać z dodatkowej opinii o zagrożeniu, jeżeli taka usługa nie jest dodatkowo płatna.

- Pomocne jest korzystanie z rekomendacji dotyczących błędnych ustawień systemowych lub braku zainstalowanych aktualizacji systemów operacyjnych, ponieważ brak aktualizacji wpływa o na obniżenie poziomu bezpieczeństwa.

- Rozważając wdrożenie danego rozwiązania należy się upewnić, że wspierane są systemy inne niż Windows, jeżeli jest to konieczne.

- Cyberprzestępcy wykorzystują legalne i zaufane oprogramowanie, a także wbudowane komponenty systemu Windows, aby ukryć złośliwą aktywność. Pliki Living off the Land Binaries (LOLBins) mają kluczowe znaczenie dla prawidłowego funkcjonowania systemu operacyjnego. Podczas cyberataku ich zablokowanie może być trudne lub nawet niemożliwe, co czyni je bardzo atrakcyjnymi dla twórców złośliwego oprogramowania. Z tego powodu telemetria ataku i moduł polowania na zagrożenia są często niezbędne do uzyskania informacji o zdarzeniach.

AVLAB
CYBERSECURITY FOUNDATION

Fundacja AVLab dla Cyberbezpieczeństwa jako niezależna organizacja stoimy na straży ochrony prywatności i bezpieczeństwa w Internecie. Budujemy świadomość użytkowników z zakresu ochrony cyfrowej. Wydajemy opinie, techniczne analizy oraz testy rozwiązań informatycznych w sferze cyberbezpieczeństwa. Udostępniamy również blog o bezpieczeństwie, na którym zamieszczamy artykuły o nowościach w zakresie bezpieczeństwa IT, lukach w zabezpieczeniach i rozwiązaniach IT.

Przeprowadzamy regularne testy różnych programów ochronnych i publikujemy wyniki na naszej stronie internetowej. Testy te obejmują szeroki zakres próbek złośliwego oprogramowania, w tym zarówno znane, jak i nieznane zagrożenia, i oceniają skuteczność każdego programu w ich wykrywaniu i usuwaniu. Pomaga to użytkownikom porównać skuteczność różnych programów bezpieczeństwa i podejmować świadomą decyzję przy wyborze rozwiązania do ochrony komputera.

Naszym najmocniejszym atutem są wnikliwe i szczegółowe recenzje, przygotowywanie raportów związanych z prywatnością i ochroną urządzeń końcowych, a w szczególności testy bezpieczeństwa, dzięki którym jesteśmy rozpoznawalni na całym świecie, jako jedno z najpopularniejszych laboratoriów testujących.

Aby poznać szczegóły techniczne producenci mogą kierować swoje zapytania na adres: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl