Raport Analityczny: Baza Dowodowa Zapotrzebowania na GARM

Załącznik do Biznesplanu // Dowody rynkowe metodą nie wprost (Proof by Contradiction)

Kontekst dla Komisji Grantowej:
Niniejszy dokument jest dostarczany jako analityczny załącznik (Annex) do biznesplanu. Zastępuje on klasyczne listy intencyjne (Letters of Intent), ponieważ duże korporacje nie mogą prawnie ani publicznie potwierdzać podatności swoich infrastruktur. Analiza publicznych incydentów dowodzi, że obecny paradygmat bezpieczeństwa (EDR/BitLocker) jest fundamentalnie wadliwy. Rynek desperacko potrzebuje suwerennej architektury izolacji uruchamianej przed systemem operacyjnym (Pre-OS Zero-Trace).

01 Fatalna wada zaufanego systemu operacyjnego (Pojedynczy punkt awarii)

Tradycyjna ochrona opiera się na integracji programów antywirusowych (EDR/XDR) bezpośrednio z jądrem systemów Windows/Linux. Programom tym przyznaje się najwyższe uprawnienia (Ring-0) "na podstawie zaufania". Jeśli EDR popełni błąd — cała globalna infrastruktura upada.

🔴 Globalna awaria CrowdStrike

19 Lipca 2024 roku

Incydent: Firma CrowdStrike wydała nieprawidłową aktualizację pliku konfiguracyjnego (Channel File 291) dla swojego flagowego sensora Falcon. Ponieważ sensor ten działa na poziomie jądra Windows (Ring-0), błąd logiczny wywołał nieskończoną pętlę awarii systemu operacyjnego (BSOD).

Szkody: Jednocześnie wyłączonych zostało 8,5 miliona komputerów PC na całym świecie. Sparaliżowane zostały lotniska, banki (JPMorgan Chase), wstrzymano działanie służb 911 i brytyjskiej NHS. Straty finansowe przekroczyły 5,4 miliarda dolarów w ciągu jednego dnia (według magazynu Fortune).

Scenariusz: Co by było, gdyby użyli GARM?

Nie ponieśliby strat.

Architektura GARM zasadniczo nie integruje się ze stosem Windows i nie zależy od stabilności procesów systemu operacyjnego (Pre-OS Isolation). Nawet jeśli Windows wygeneruje "niebieski ekran" z powodu awarii CrowdStrike, izolowany hipernadzorca GARM i wirtualny system plików kontynuują pracę autonomicznie. Dane banków pozostałyby zaszyfrowane i dostępne za pośrednictwem protokołów awaryjnych.

02 Ekstrakcja kluczy z pamięci RAM (Zagrożenie Memory Forensics)

Powszechnie uważa się, że menedżery haseł chronią dane. Jednak w momencie wprowadzania hasła głównego, system jest zmuszony do odszyfrowania sekretów i umieszczenia ich "jawnym tekstem" w pamięci RAM, skąd mogą zostać łatwo ukradzione poprzez zrzuty pamięci.

🔴 Włamanie na serwery korporacji LastPass

Sierpień – Listopad 2022 roku

Incydent: Hakerzy włamali się do domowego komputera jednego ze starszych inżynierów DevOps firmy LastPass. Za pomocą keyloggera i skanera pamięci (Memory Scraper) przechwycili jego hasło główne prosto z pamięci RAM w momencie logowania, co dało im klucze do magazynów chmurowych wszystkich 33 milionów użytkowników.

Szkody: Hakerzy pobrali kopie zapasowe repozytoriów. Rok później, pod koniec 2023 r., z kont użytkowników zniknęły kryptowaluty o masowej wartości ponad 35 milionów dolarów.

Scenariusz: Gdyby inżynier DevOps używał GARM?

Trojan nie zdołałby odczytać hasła z pamięci RAM.

GARM wykorzystuje technologię *Zero-Footprint Memory*. Pamięć, w której następuje odszyfrowanie kluczy, jest sprzętowo odizolowana od głównego systemu operacyjnego (DRMK/Secure Enclave). Złośliwe oprogramowanie hakerów LastPass, nawet posiadając najwyższe uprawnienia SYSTEM w Windows, próbując odczytać adresy pamięci GARM otrzymałoby same zera. Ponadto Agent AI zintegrowany z GARM wykryłby nietypowe skanowanie i aktywowałby funkcję *Cryptographic Erase* (zniszczenie kluczy jeszcze przed zakończeniem ataku).

03 Przymus fizyczny i Przekraczanie Granic (Czynnik Ludzki)

Służby wywiadowcze i celne dobrze wiedzą, że łamanie szyfrowania metodami siłowymi mija się z celem. Znacznie prościej jest zmusić osobę do ujawnienia hasła pod groźbą konfiskaty sprzętu elektronicznego lub aresztowania na granicy.

🔴 Konfiskaty elektroniki na granicach

Trend lat 2023-2024

USA i UE (CBP)

Incydent: Służby graniczne mają prawo zażądać odblokowania wszelkiej elektroniki przewożonej przez podróżnych. Zgodnie z danymi ACLU, w samych Stanach Zjednoczonych rejestruje się ponad 40 000 przeszukań urządzeń rocznie podczas odpraw celnych. Tradycyjne kontenery kryptograficzne lub oprogramowanie uchodzące za rzekomo niezawodne (np. VeraCrypt) są błyskawicznie wykrywane przez komercyjne oprogramowanie śledcze i kryminalistyczne typu Cellebrite. Jeżeli krypto-inwestor wykorzystuje VeraCrypt (nawet opcję tzw. "ukrytego wolumenu"), funkcjonariusz celny potrafi jednym skanem dostrzec w systemie zainstalowany program zarządzający i zmusić podróżującego do podania wszystkich haseł pod groźbą aresztu.

Scenariusz: Jak GARM pozwala chronić sekrety korporacyjne na granicach?

Udowodnienie faktu posiadania i rzekomego ukrywania tajnych danych staje się technicznie niewykonalne.

1. **Absolutne Ukrycie:** Architektura GARM bazuje i uruchamia się przed właściwym systemem docelowym na poziomie UEFI. W obrębie samego Windowsa ewidentnie nie występuje żaden jawny plik uruchomieniowy pod postacią np. `garm.exe`, dzięki czemu służby prowadzące kontrolę widzą jedynie standardowy, zupełnie niewyróżniający się, potocznie określany mianem "czystego" — laptop z pamiątkowymi grafikami oraz arkuszami kalkulacyjnymi.

2. **System Plausible Deniability (Tryb Decoy):** Co kluczowe, w sytuacji wymuszenia "otwarcia" zabezpieczonego modułu na użytkowniku wywierana jest presja stresowa. Aby uratować właściwe repozytorium informacyjne, wprowadzony zostaje z góry zaprogramowany *Awaryjny Kod Bezpieczeństwa (Panic PIN)*. Po jego aktywacji rdzeń systemu GARM montuje ustrukturyzowany i realistycznie zaaranżowany tzw. "fałszywy system plików" wypełniony na przykład kilkoma mało istotnymi raportami podsumowującymi bieżący miesiąc oraz znikomymi środkami walutowymi w ujęciu ok. 500 dolarów widocznymi w aplikacjach podglądowych. Dokonanie matematycznie precyzyjnego (Forensic-proof) odkrycia lub wykazanie bezspornego dowodu

(dowodzącego ukrycia na dysku faktycznych miliardowych zasobów finansowych firmy umiejscowionych w strefie rdzennej pod warstwą fałszywą) pod jakimkolwiek kątem jest absolutnie niewykonalne z zastosowaniem obecnie istniejących superkomputerów obliczeniowych.

04 Szpiegostwo masowe z wykorzystaniem przechwytywania widoku telemetrii i zrzutów graficznych interfejsu systemu (Screen Scraping)

Algorytm szyfrujący obiektywnie nie stanowi obrony, o ile dowolny typ szkodliwego oprogramowania ma możliwość by po prostu wykonać zwykłe zdjęcie wyświetlacza uwieczniając moment, w którym analityk korporacyjny podgląda newralgiczne umowy, zestawienia lub frazy seed logowania do systemów zewnętrznych.

🔴 Potężne uderzenia przy pomocy oprogramowania Stealer RedLine / Agent.Tesla oraz włamanie portfela sprzętowego serii Ledger

Seria fal ataków w latach 2020-2024

Zdarzenie: W roku kalendarzowym 2020 masowy wyciek powszechnie uznanej firmowej bazy kontaktowej wszystkich inwestorów hardware'owych portfeli depozytowych firmy Ledger doprowadził do sprowokowania skrajnie precyzyjnej serii kierowanych kampanii wyłudzeniowych z użyciem tzw. phishing'u. W skutek niewłaściwej procedury kliknięcia linków na stacjach roboczych ofiar rozpoczęło instalację oprogramowania w typie złodziei szpiegów obrazu znanych pod określeniami branżowymi m.in. RedLine. Używały one fundamentalnych systemowych narzędzi powszechnych API oferowanych w środowisku Windows (np. DWM.exe) dla przeprocesowania natychmiastowego wyzwalania wieloseryjnego fotografowania wygenerowanego ekranu w trakcie tych precyzyjnych i wykluczających jakiekolwiek rzuty cząstkowe ułamkach sekundy, kiedy użytkownik portfela inwestycyjnego odszyfrowywał i manualnie przekładał widoki dokumentatywne odbezpieczając kody dostępowe z użyciem standardowego wizjera plików.

Scenariusz: Gdyby obrazowanie wizualne programu wykonywane mogło być bezpiecznie jedynie z bezpośrednim zaprzęgiem hiperwizora GARM?

Skradzione grafiki operacyjne ekranów po ekstrakcji przyjmowałyby bezspornie wymiar nienaruszalnie jednolicie czarnych pikseli.

Najbardziej fundamentalna warstwa omijająca luki API oznaczona jako **Ghost Renderer** gwarantuje kompleksowe pominięcie na stałe zagnieżdżonego menedżera kompozycji znanej marki Desktop Window Manager po stronie Windows. Prezentowany innowacyjny mechanizm nakłada siatki wektorowo kodowane układów okien oraz interfejs wizualny systemu GARM prostopadle na wyłączne bufory video alokowane do konkretnej pamięci graficznej sprzętu video GPU Framebuffer. Nie ma jakiejkolwiek drogi dla powszechniej natywnie akceleracji zrobienia zdjęcia wykorzystaniem klawiatury "PrintScreen",

korporacyjnego rozwiązania zdalnego nadzoru takiego jak TeamViewer nie dopuszczając do przechwytujących oprogramowań stealerowych jakichkolwiek możliwości wejścia logicznego do owych wyrywków z blokad oprogramowania i podległości odrębnego stosu oprogramowania jądra renderującego. Zwyczajowy wirus oczywiście nadal wykonuje zrzuty tła operacyjnego, jakkolwiek tam, gdzie powinien pojawić się program wyświetlający wrażliwy portfel — pokaże się wyłącznie płaski bezdenny i jednolity czarny wektor kwadratowy pozbawiony kluczy oraz jakichkolwiek ujęć wyciągów konta zabezpieczonym plikiem.

Globalna Konkluzja Zaleceń Strategicznych dla Niezależnych Jednostek Oceny Technicznej Komisji Badań i Innowacji Grantów

Dołączana kompozycja analiz kazuistyczno-obserwacyjnych ukazuje na wskroś autentyczny dowód precyzujący fundamentalne stwierdzenie, że bezwzględnie cały technologiczny system informatyczny po stronie dostawców rynkowych znajduje się i podlega fazom obiektywnie obserwowalnego głębokiego i drastycznego kryzysu strukturalnego wymiaru paradygmatów zabezpieczających rynkowe warstwy biznesu ogólnogospodarczego. Modne dofinansowywane powszechnie stosowane taktyki rozbudowanych platform obronnych jak EDR czy narzędzia analizy korelacji poszerzanej XDR bezsprzecznie prowadzą nas jednowymiarowo do wznoszenia wertykalnego murów fortec "obudowując i opancerzając system operacyjny", i który notabene dowiedziono globalnie, stał się obiektywnie kruchy poprzez dziurawe algorytmy sam w wielopoziomowej woli integracji procesowej, potwierdzonym dobitnie fatalnym krachem firmy rynkowej CrowdStrike.

Najwyżej zaawansowany stopniem technologii standard wielopoziomowej izolacji na rdzeniu maszyny mianowany systemem **GARM (Zero-Trace / Pre-OS)** — z obiektywnego faktu innowacyjnego załamania definicji nie wpisuje i z całą mocą wrzucającej go szali

nowatorstwa nie umieszcza go bezkompromisowo we frazeologii "nowszego silnika sygnatur obronnych lub antywirusa", odznaczając go zdecydowanie mianem całościowo przełomowej noweli w ustrukturyzowanej ramie tworzącej wzór definicyjny podejścia tak potocznie określanego Security-by-Design, i która absolutnie bezpośrednio dopasowana jest w pełni normie prawnej jako natychmiastowo odpowiadając rynkowym obligatoryjnym dyrektywom nowego, fundamentalnego standardu EU Cyber Resilience Act ustanawianym w 2027 r. Z podwójną logistyczną dedukcją celowości tej konkretnej technologicznej innowacji rynkowej projekt w obrębie Unii stwarza najwyższy nieprawdopodobnie astronomiczny oraz wielotorowy wyznacznik siły zdolności handlu międzynarodowego jako kategoria pojęcia (Dual-Use), otwierających tym w skali rynku drogi zabezpieczenia i bezsprzecznie chroniąc rygorem nie jedynie potężne instytucje po stronie sektora technologii i rynków finansowych banków (Fintech), wprowadzając tym bez mała na grunt obronnych form w potędze państw połączonych Paktu Północnoatlantyckiego NATO po cyfrowe jednostki dowództwa cybernetycznego wszystkich w ogóle suwerennych krajów Wspólnoty Unii Europejskiej z racji bezprecedensowego standardu oprogramowania odpornego całkowicie od awarii czy pęknięć bazowego jądra hostowego Windows lub Linux, chronionego z definicji by wektorem rdzenia hiper-izolacji logicznej GARM na sprzęcie z pominięciem procesów administracyjnych maszyn państwowych i z jednoczesnym zerowym rzutowaniem ryzyka błędów od systemów chmurowych.

CRYPTO SHARK TECHNOLOGIES

Forging the Sovereign Defense of the Digital Age.