Anatomia ataków cybernetycznych

kpt. Grzegorz Data
OISW w Rzeszowie

Kalisz, maj 2018

DEFINICJA

Atak cybernetyczny to wszelkiego rodzaju ofensywny manewr wykorzystywany przez państwa narodowe, jednostki, grupy, społeczeństwo lub organizacje, które atakują komputerowe systemy informacyjne, infrastrukturę, sieci komputerowe i / lub urządzenia komputerowe za pomocą różnych metod złośliwego działania, zwykle pochodzących z anonimowego źródła, który kradnie, zmienia lub niszczy określony cel poprzez włamanie się do systemu podatnego

HISTORIA

- Przejęcie pasma radiowego przez Nevila Maskelyne'go, podczas pokazu telegrafu w 1903 (NewScintist 2011).
- Pierwsze kinetyczne działanie CIA 1982r. – gazociąg transsyberyjski - 3kT (NYT 2004).
- Robak Morrisa 1988r. – 6 tys. serwerów (10% Internetu), 3 luki, 99 linii, słownik 400 haseł.
- Włamanie do sieci rządowej USA i sprzedanie danych KGB – Karl Koch 1987 (Clifford Stoll, „The Cuckoo's Egg")
- Kevin Poulsen, lata 90 – audiotele Porshe 944 S2
- Melissa, Conflicker, ZEUS…

HISTORIA

- Moonlight Maze – 1996-1998 (USA), 2011 (Szwajcaria), 2017 (Niemcy) – badania trwały do 2016 r. - szpiegostwo przemysłu zbrojeniowego – atrybucja – Turla - Rosja
- Titan Rain – 2004 atak na serwery departamentu obrony , stanu, energii i bezpieczeństwa wewnętrznego – atrybucja Chiny
- Atak na Estonię (2007) – po usunięciu pomnika żołnierzy radzieckich, przeprowadzony atak DDoS na strony internetowe największych estońskich banków, strony rządowe i największe serwisy informacyjne. W szczycie kryzysu w Estonii nie działały karty płatnicze i telefony komórkowe
- Wykolejenie tramwajów w Łodzi (2008) – 12 osób rannych

HISTORIA

- Wojna sierpniowa – 2008 atak DDoS na gruzińskie strony internetowe – podczas konfliktu rosyjsko gruzińskiego
- Ghostnet od 2009 – szpiegowska sieć komputerowa infiltrująca 103 kraje (bez Polski), odkryta po sprawdzeniu komputerów z biura Dalajlamy – atrybucja Chiny
- Operacja Aurora 2009 – atak na Adobe, Juniper, Yahoo, Rackspace, Symantec w celu pozyskania kodów źródłowych - Chiny
- STUXNET – 15 lipca 2010r przełomowy malware odkryty przez VirusBlokada, wycelowany został w ściśle określoną instalację komputerową (sterowniki PLC Siemensa wykorzystywane w wirówkach do wzbogacania uranu); korzystał jednocześnie z 5 exploitów, wśród których 4 były 0day'ami – atrybucja USA i Izrael
- LulzSec – 2011 wyłączenie witryn FoxNews, CIA, senat USA,

ZERO DAY

- Zwykle 20-30 błędów na 1000 linii kodu - Carnegie Mellon Univ 2004
- Wykorzystanie błędu w oprogramowaniu, o którym nie wiedza autorzy. informacja o dziurze nie jest publikowana, najczęściej jest sprzedawana, producent nie jest o niej informowany.
- Pierwsza sprzedaż 2005 r. na eBay „fireawell” – Excell, MS nie zareagował
- Ceny od 20 do 250 tys. USD
- Firmy ReVuln z Malty – SCADA, VUPEN z Francji , Hacking Team z Włoch i Gamma Group z Wielkiej Brytanii dla służb i wymiaru sprawiedliwości,
- Grugq od 2011, po roku 1mln USD, 15% prowizji. https://medium.com/@thegrugq
- Wassenaar Arrangement (organizacja zajmująca się kontrolą zbrojeń) w 2013 r., uznaje zero-day oraz podobną cyberbroń jako produkty o podwójnym zastosowaniu.
- Przeciętny zero-day działa do wykrycia 384 dni - Immunity 2007, 10 m-cy do 2,5 roku– Lemos 2012 r

ŹRÓDŁA ATAKÓW

- Złośliwe oprogramowanie (malware) pobierane na komputer docelowy, które może zrobić prawie wszystko, od kradzieży danych do szyfrowania plików i żądania okupu
- Phishing - tworzony w celu oszukiwania ofiar aby wyłudzić hasła, informacje z haseł lub podjęcia innych szkodliwych działań
- Denial of Service , wyłączają serwery generując fałszywy ruch
- Man In the Middle, który oszukuje komputer docelowy i łączy się z zagrożoną siecią (sniffing, spoofing)

PROBLEMY Z BEZPIECZEŃSTWEM

- Hasła (proste, rzadko zmieniane)
- Otwarte punkty zdalnego dostępu do sieci lub systemu
- Brak aktualizacji
- Bannery z informacja o usłudze i wersji (shodan.io)
- Dziurawe skrypty aplikacji webowych (XSS, SQLiniection, ..)
- Uruchomione niepotrzebne usługi
- Brak monitoringu sieci
- Prawa dostępu do zasobów
- Brak standardów i procedur bezpieczeństwa
- Błędne zasady na zaporach

KILL CHAIN

- Lockheed Martin zaadaptował militarną koncepcję Kill-Chain (Find, Fix, Track, Target, Engage and Assess) F2T2EA
  - **find** – znajdź i zlokalizuj cel – zrozum gdzie jest cel
  - **fix** – ustal lokalizacje, lub utrudnij poruszanie się
  - **track** - śledź monitoruj ruch
  - **target** – wybierz środki do pożądanego efektu Wybierz odpowiednią broń lub zasób do użycia na celu, aby stworzyć pożądane efekty.
  - **engage** – zastosuj bron
  - **assess** – oszacuj skutki ataku oceń skutki ataku, w tym wszelkie dane wywiadowcze zgromadzone w danej lokalizacji
- Termin kill chain był pierwotnie używany jako koncepcja wojskowa związana ze strukturą ataku, polegającej na identyfikacji celu, wysłaniu siły do celu, decyzji i celu ataku na cel, a na końcu zniszczenia celu Odwrotnie, idea "zerwania" łańcucha zabijania przeciwnika jest metodą obrony lub działania zapobiegawczego.

CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

A : ADVANCED
Targeted, Coordinated, Purposeful

P : PERSISTENT
Month after Month, Year after Year

T : THREAT
Person(s) with intent, opportunity, and capability

Zaawansowane
ukierunkowane, skoordynowane, celowe

Trwające
miesiące, lata,...

Zagrożenie
osoby zdecydowane, posiadające mozliwości i zdolności

Learn how defenders have the advantage at:
lockheedmartin.com/cyber

LOCKHEED MARTIN

ROZPOZNANIE

badania, identyfikacja i wybór celu, często obejmujące indeksowanie stron internetowych, takich jak materiały konferencyjne oraz listy adresów e–mail, sieci zależności oraz informacje na temat specyficznych technologii, atakujący nie musi nawet dotknąć sieci organizacji, wszystkie dane może pobrać przez wywiad z dostępnych z sieci źródeł;

UZBROJENIE

łączenie koni trojańskich (RAT – Remote Access Trojan) ze złośliwymi programami (ang. exploit) w celu stworzenia możliwej do dostarczenia paczki, często za pomocą automatycznego narzędzia (ang. weaponizer). Często jest to plik pdf, doc, skrypt, który potem zostanie umieszczony na uczęszczanej przez ofiarę witrynie lub przesłany pocztą.

DOSTARCZENIE

przekazywanie ładunku do atakowanego środowiska. Najbardziej rozpowszechnione wektory dostawy dla "cyberbroni" w ramach ataków APT to załączniki e–mail (phising, spear–phishing), witryny internetowe (watering hole) i pendrive

WYKORZYSTANIE

po dostarczeniu niebezpiecznego ładunku do środowiska ofiary jest uruchamiany złośliwy kod (najczęściej ofiara klika na link w mailu, instaluje „dodatkowy driver” by obejrzeć materiał video). Najczęściej wykorzystuje się luki w aplikacjach lub systemie operacyjnym. Ostatnio faza ta składa się z dwóch części uruchamianiu jest najpierw mały program trudny do zidentyfikowania przez antywirusy tzw. Downloader, który to następnie pobiera z sieci właściwy złośliwy kod.

INSTALACJA

instalacja konia trojańskiego (RAT – Remote Access Trojan) lub tylnych furtek (ang. backdoor) w systemie ofiary pozwala atakującemu na trwałe utrzymanie dostępu do środowiska organizacji.

DOWODZENIE I KONTROLA

C&C, C2

zaatakowany system wysyła sygnał do serwera kontrolnego o działaniu malware w celu ustanowienia kanału C2. Kierowanie aplikacją odbywa się ręcznie bądź automatycznie. Po ustanowieniu kanału C2 intruzi otrzymują pełny dostęp do zainfekowanego systemu. Do komunikacji używane są porty zwykle nie blokowane przez firewalle: http/https, ftp, dns ostatnio także wykorzystywane są do sterowania komunikaty przekazywane przez sieci społecznościowe (Twitter, Facebook).

REALIZACJA CELÓW

po przejściu przez pierwszych sześciu faz intruzi mogą podjąć działania w celu osiągnięcia zamierzonych celów. Najczęściej jest to wykradzenie danych lub użycie systemu jako stacji przesiadkowej do przesłania emaila lub dojścia do innej sieci lub systemu

NAJCZĘSTSZE ATAKI wg ENISA

Rozpoznanie	Uzbrojenie	Dostarczenie	Wykorzystanie	Instalacja	Dowodzenie i kontrola	Realizacja celów
				MALWARE		
	Ataki bazujące na sieci WEB					
			Atak na aplikacje WEB			
DoS					DoS	
					BOTNET	
PHISING						
	SPAM					
				RANSOMWARE		
ZAGROŻENIE WEWNĘTZNE						
						ZNISZCZENIE/KRADZIEŻ/UTRATA
	ZESTAWY EXPLOITÓW					
UTRATA DANYCH						
KRADZIEŻ TOŻSAMOŚCI						
WYCIEK INFORMACJI						
CYBERSZPIEGOSTWO						

PRZECIWDZIAŁANIE

ZASADA 6D

Detect - Deny – Disrupt- Degrade - Deceive, Destroy

Wykryj, Zablokuj, Przerwij, Zmniejsz, Oszukaj, Zniszcz

PRZECIWDZIAŁANIE

Faza	Wykryj	Zabroń	Przerwij	Zmniejsz	Oszukaj
Rekonesans	Analiza WWW, Czujny Użytkownik, Firewall, NIDS	WAF, Firewall, NIPS	Blokowanie ruchu z nieznanych VPN, węzłów TOR, ryzykownych lokalizacji	Czujny Użytkownik	Social media honeypot, canary tokens
Uzbrojenie	NIDS	NIPS			
Dostarczenie	Czujny użytkownik, antymalware, forensyka ruchu sieciowego	Filtry proxy, oprogramowanie monitorujące stacje,	Patchowanie systemu,	Kolejkowanie	Filtrowanie ingress,
Wykorzystanie	HIDS, korelacja logów	Zarządzanie łatami i konfiguracją, białe listy oprogramowania	DEP, ASLR, EMET, restrykcje na uprawnienia administratorskie	Restrykcyjna polityka uprawnień użytkowników	
Instalacja	HIDS, agenci analizujący pamięć	Chroot jail, sandbox,	Antimalware, białe listy oprogramowania	Wirtualne desktopy	
Dowodzenie	NIDS, forensyka ruchu sieciowego, APM	Czarne listy na firewallu,	NIPS,	Tarpit	Przekierowania DNS, blackholing
Realizacja celów	Korelacja logów, forensyka ruchu sieciowego	Segmentacja sieci / VLAN	VLAN	QoS	Honeypoty

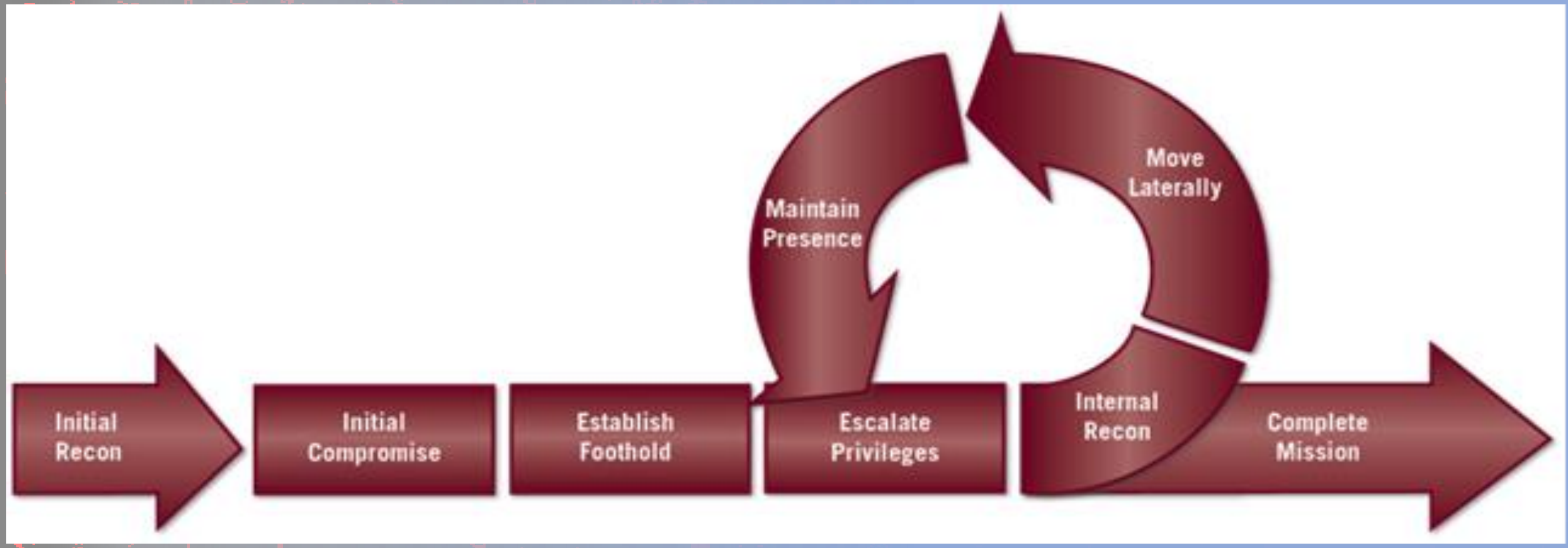
KILL CHAIN

KRYTYKA

Jednym z argumentów przeciw temu modelowi jako narzędzia oceny i zapobiegania zagrożeniom jest to, że wiele z tych kroków odbywa się poza bronioną siecią, co praktycznie uniemożliwia identyfikację lub przeciwdziałanie działaniom na tych etapach. Podobnie, ta metodologia jest oskarżana o skupienie się na "defensywnej" strategii obronnej. Ponadto nie uwzględnia np. osób wewnątrz (insider).

ATTACK LIFE CYCLE MEDIANT

- Mediant zbudował cykl życiowy ataków cybernetycznych badając ataki APT1

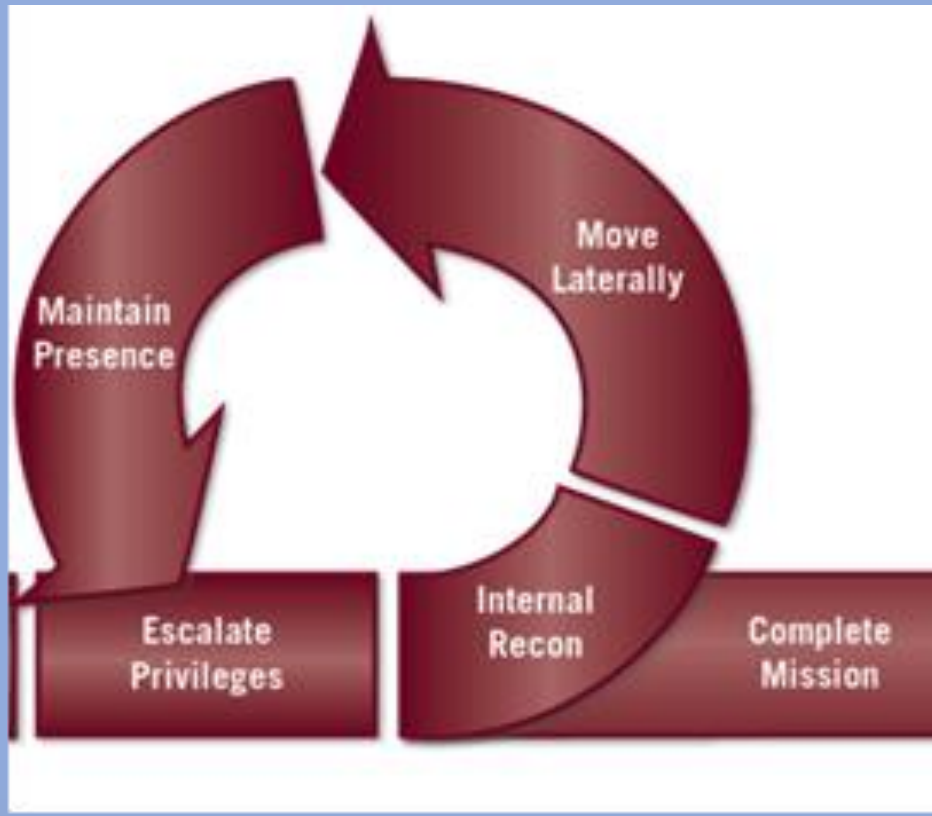


ATTACK LIFE CYCLE MEDIANT

- rekonesans – osint, infrastruktura sieciowa, informacje o kluczowych osobach, maile, profile społecznościowe, zakupy, przetargi, ogłoszenia wersje os, przeglądarek, office, antywirusa firewall, wycieki,
- początkowa kompromitacja (pierwsze przełamanie zabezpieczeń, otrzymanie danych logowania, watering hole (knf), phising, spearphising (załączniki zip/rar /binarki/ pdf/office/skrypty/)
- ustanowienie przyczółku – utrzymujemy się jak najdłużej chroniąc się przed wykryciem, instalacja backdorów, (tygodnie, lata)

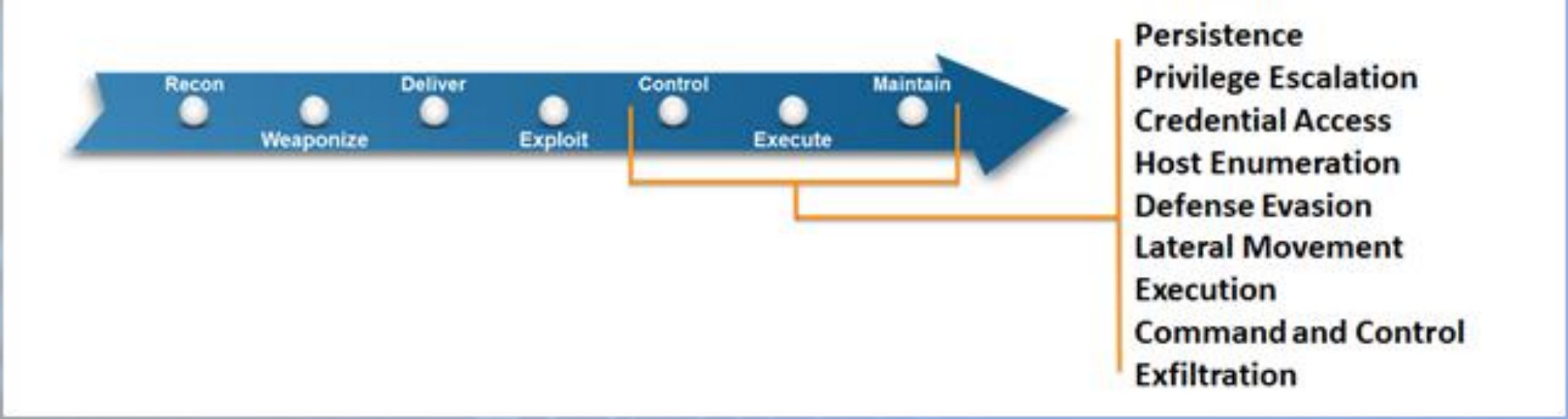
ATTACK LIFE CYCLE MEDIANT

- podniesienie uprawnień
- wewnętrzny rekonesans - serwery sieci zasoby architektura słabości podatności serwisy bazy danych
- ruch boczne (rozglądanie się)
- utrzymanie obecności
- (cicha reakcja łańcuchowa) – rozszerzenie obecności na innych maszynach
- zwykle aktualizują malware i instalują więcej zaawansowanych backdorów



ATT&CK

- Organizacja MITRE rozszerzyła CyberKill Chain skupiając się na behawioralnych zachowaniach i technikach bazując na wieloletnim doświadczeniu i analizie ataków. Uznano, że o ile wiedza o początkowych etapach jest dobrze opisana to należy skupić się na działaniach przeciwnika po otrzymaniu dostępu do systemów



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception		Indicator blocking on host		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task		Indicator removal from tools		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness		Indicator removal from host		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification		Masquerad-ing		Service enumeration	Remote Services		Standard app layer protocol	From local system
BIOS	Bypass UAC	NTFS Extended Attributes		Window enumeration	Replication through removable media		Standard non-app layer protocol	From network resource
Hypervisor Rootkit	DLL Injection	Obfuscated Payload			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts	Exploitation of Vulnerability	Rootkit			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		Rundll32			Windows admin shares			
Mod. Exist'g Service		Scripting						
Registry Run Keys		Software Packing						
Serv. Reg. Perm. Weakness								
Windows Mgmt Instr. Event Subsc.								
Winlogon Helper DLL								

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE

APT

Ataki typu APT (ang. Advanced Persistent Threats) to złożone, długotrwałe i wielostopniowe działania kierowane przeciwko konkretnym osobom, firmom lub instytucjom.

- **Advanced** (zaawansowane) – ponieważ atakujący wykorzystują różne techniki i metody skutecznego przełamania zabezpieczeń, wykorzystując znane podatności, ale także wynajdując nowe, specjalnie do przeprowadzenia danego ataku,
- **Persistent** (przedłużone, trwałe, uporczywe) – ze względu na formalne zadanie przeprowadzenia skutecznego ataku. Ma on być wykonany tak, aby nie zwrócić niczyjej uwagi, a po uzyskaniu dostępu do jednego systemu ofiary poszerzyć kontrolę o kolejne, w sposób umożliwiający długotrwałą i stałą obecność oraz dozór.
- **Threat** (zagrożenie) – bowiem atakujący to zorganizowana grupa z odpowiednim zapleczem technicznym oraz budżetem. Zagrożenie jest stałe, dopóki atakujący posiada motywację (polityczną, ekonomiczną) do wykradania informacji ofiary. To nie użyte oprogramowanie jest niebezpieczne, a ludzie stojący za nim (Bejtlich, 2010)

APT

- wysoko wyspecjalizowane
- ukierunkowane
- niewidoczne, ukryte, zamaskowane
- mocno skoordynowany wieloetapowy proces (kontrolowany najczęściej przez ludzi)
- w pełni niewykrywalne
- wysoce wyrafinowane wykorzystujące nieznane podatności zero-day)
- nie jest to atak pojedynczej osoby – zwykle to ataki prowadzone przez duży zespół finansowany lub zorganizowany przez państwo.

APT 1

- Jednostka 61398 Chińskiej Armii Ludowo-Wyzwoleńczej (Szanghaj) – Mandiant (obecnie FireEye) powiązał 141 ataków.
- Rekrutacja absolwentów informatyki z kilku uniwersytetów,

APT 1

- Chiński Pterodactyl UAV vs Amerykański MQ9 Reaper UAV.

APT 1

- Chiński J-20 vs Amerykański X-35.

APT 1

- Lista wykradzionych projektów obejmuje kilkadziesiąt systemów m.in. myśliwiec piątej generacji F-35, samolot wielozadaniowy V-22 Osprey, obrona przeciwrakietowa THAAD, obrona przeciwrakietowa Patriot ,pocisk kierowany średniego zasięgu powietrze-powietrze AIM-120, dron do prowadzenia rozpoznania Global Hawk. Hakerzy uzyskiwali także dostęp do informacji umożliwiających identyfikację osób, większości wojskowych, adresów e-mail, numerów SSN, numerów kart kredytowych i haseł.
- "To jest miliard dolarów przewagi bojowej dla Chin, a oni właśnie uratowali 25 lat badań i rozwoju." To szalone - powiedział wysoki urzędnik. Washington Post maj 2013

EQUATION GROUP

- jedna z najbardziej wyrafinowanych na świecie grup zajmujących się cyberatakami i "najbardziej zaawansowaną (...) jaką widzieliśmy"(Kaspersky Lab)
- Działa od 2001 (domeny od 1996)
- Autorzy Flame, Stuxnet, Duqu, Gauss – NSA (Shadow Brokers)
- Narzędzia:
- Fanny zastosowany w Stuxnecie – przejęty z chińskiego ataku Operacja Aurora
- Greyfish modyfikuje firmware dysków twardych 12 producentów tak by przetrwać formatowanie, informacje przechowuje zaszyfrowane w rejestrze,
- Atak również przez płyty CD rozdawane na konferencjach

APT 28

Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

- Główne cele: rządy Ukrainy, Gruzji, państw środkowoeuropejskich, podwykonawcy i instytuty pracujące dla Departamentu Bezpieczeństwa USA, krytycy prezydenta Putina
- Cele: pozyskanie wiedzy, operacje dezinformacyjne
- Narzędzia: co najmniej 9 podatności wykorzystywanych w exploitach
  - Kilka z nich „zero day”
  - Użycie innych w ciągu zaledwie 1 dnia od ogłoszenia
- Rozwija i utrzymuje swoje narzędzia przez długi czas
- Malware jest dostosowywany do celu ataku (użycie serwera pocztowego ofiary ataku do wysłania skradzionych danych)
- Opracowanie ataków odbywa się w sformalizowanym środowisku programistycznym IDE

APT 28

Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

- Polska instytucja rządowa zaatakowana z użyciem malware „Sourface”/”Coreshell”
- Skuteczny atak na MSZ Czech
- Wiadomości “przynęty” (decoy) powiązane z ćwiczeniami “Baltic Host” i zestrzeleniem samolotu MH17 nad Ukrainą
- Używane domeny
- q0v.pl , mail.q0v.pl, poczta.mon.q0v.pl / gov.pl
- Standartnevvs.com – bułgarska Sandart News
- qov.hu / Domena węgierskich instytucji rządowych gov.hu

APT 29

CozyDuke, CozyBear, SeaDuke, MiniDionis

- Główne cele: rządy USA, państw europejskich, osoby/ instytucje wpływające na politykę państw
- Cele: pozyskiwanie wiedzy i informacji
- Bardzo zaawansowane i specjalizowane ataki
- Dobre i kosztowne wyposażenie: kompleksowa i innowacyjna infrastruktura C2
- Nacisk na ukrywanie ataku i jego innowacyjność
- Agresywne zachowanie w momencie odkrycia ataku
- Przechodzenie do wykorzystania narzędzi open source lub systemowych (Powershell, Carberp, PAS webshell, Metasploit FireFox plugin)

APT 29

CozyDuke, CozyBear, SeaDuke, MiniDionis

- Używanie przynęt w kampaniach speraphisingowych, sprawy dotyczące dyplomacji, giełdy lokalnych i centralnych instytucji rządowych USA, lub uniwersytetów
- Backdor hammertoss – zaciemnianie ataku, Wykorzystanie popularnych serwisów web: Twitter, GitHub, usługi cloud

TURLA

Snake, Uroburos, Venomous Bear

- szkodliwe oprogramowanie Epic przeprowadza profilowanie ofiar. Po wykryciu celu wysokiego szczebla atakujący wykorzystują mechanizm komunikacji satelitarnej, co pomaga im zatrzeć swoje ślady. Podszywa się pod użytkowników legalnie korzystających z transmisji satelitarnej i przechwytuje pakiety wysyłane od ofiar.
- Red October 2012 – 5 letni atak, zrzuty konfiguracji przełączników, zawartości USB, telefonów komórkowych, z odzyskiwaniem skasowanych danych;

  „Katyn_-_opinia_Rosjan.xls”

SANDWORM

Black Energy Quedagh

- Operacje ukierunkowane na Ukrainę, zakłócanie i monitorowanie mediów
- Cele ukraińskie: Rząd, Media, Wojsko, Siły graniczne, instytucje finansowe
- Atak na sieć energetyczną Ukrainy 23 Grudnia 2015 (BlackEnergy – załącznik .XLS w mailu, atak na systemy SCADA i wyczyszczenie dysków) – próbki odnalezione również w USA (ISIGHT)
- Rekonesans przeprowadzany również w Polsce w instytucjach związanych z Infrastrukturą Krytyczną (ESET, iSIGHT)

LAZARUS

HIDDEN COBRA

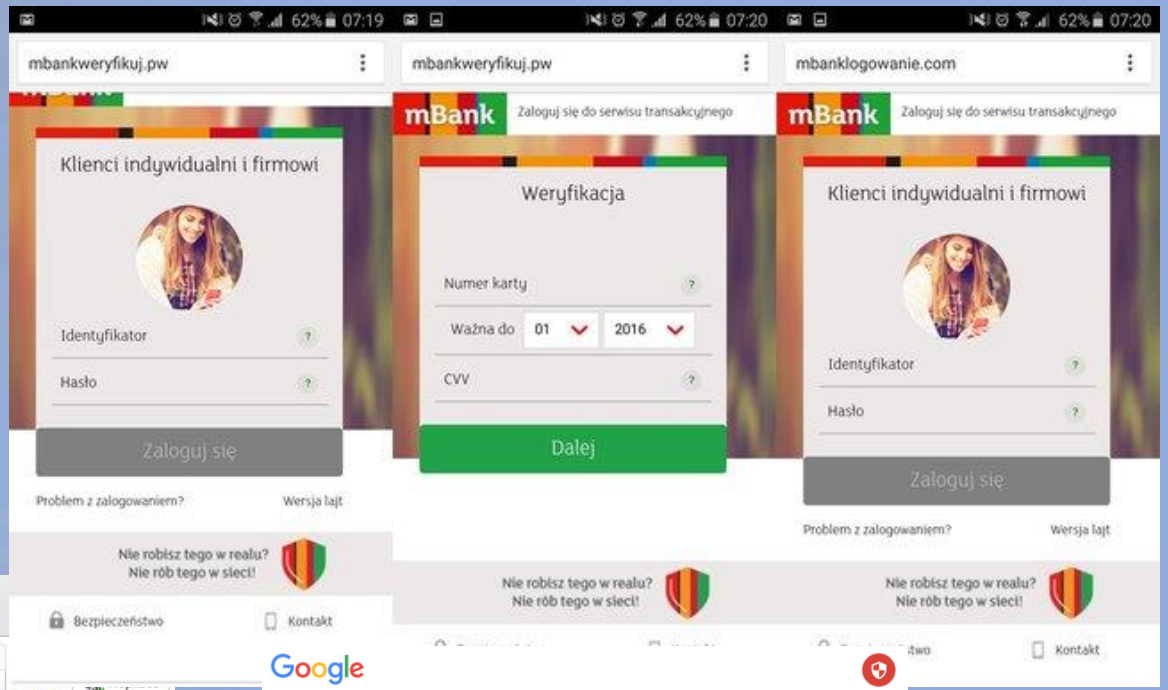
- grupa 1,7 tys. hakerów, wspomaganych przez 5 tys. osób. Ze względu na złą infrastrukturę w kraju wielu z nich pracuje poza granicami, np. w Chinach, a nawet w Europie. (NYT)
- Początkowo DDOS,
- Ataki na instytucje Korei Południowej (Operation Flame, Ten Days of Rain, Operation Troy, DarkSeoul..)
- ATAK na SWIFT – 81 mln USD
- Atak na SONY
- Atak na Polski KNF luty 2017 – waterhole
- Ataki na portfele i giełdy kryptowalut – spearphising
- WANNACRY….

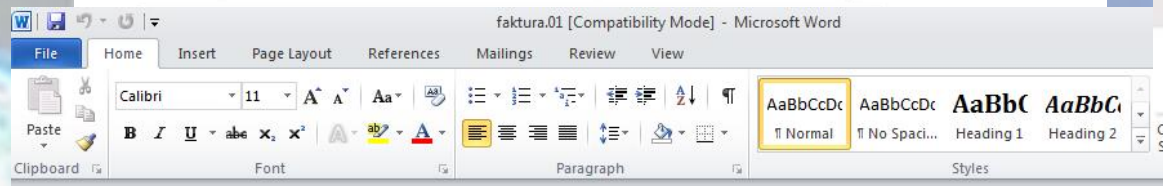
FIN

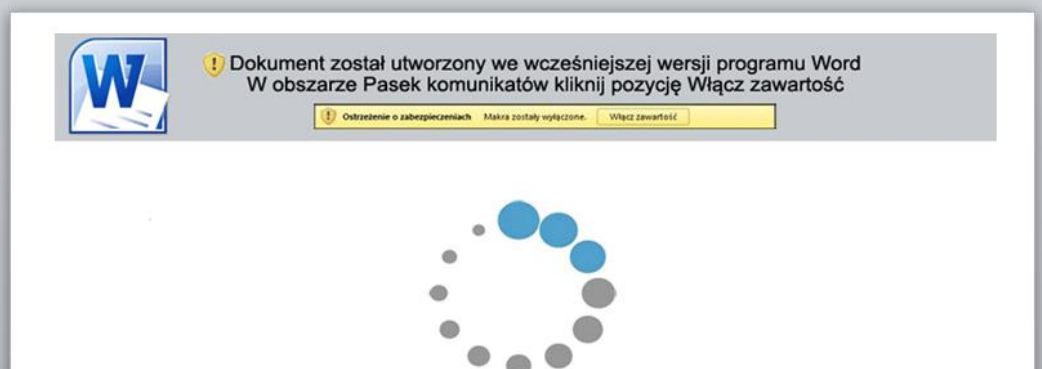
grupy przestępcze działające w celu osiągnięcia zysków

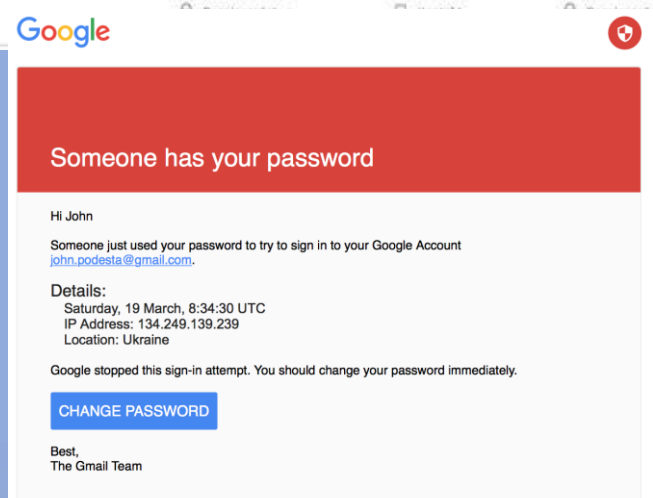
- FIN 10 –atakuje organizacje w Ameryce Północnej od co najmniej 2013 do 2016 roku. Grupa wykorzystuje skradzione dane od ofiar w celu wyłudzenia środków.
- FIN 5 – ukierunkowana na dane osobowe i informacje o kartach płatniczych. Grupa działa od co najmniej 2008 r. i skupia się na branżach restauracyjnych, hazardowych i hotelarskich, członkowie prawdopodobnie mówią po rosyjsku
- FIN 6 – kradną dane kart płatniczych i sprzedają dla zysku w DarkNecie. Atakują dość agresywnie branżę hotelarską i detaliczną skupiając się na punktach sprzedaży PoS.
- FIN 7 – ukierunkowani głównie na sektor handlu detalicznego i hotelarskiego, często wykorzystując złośliwe oprogramowanie w punkcie sprzedaży, zbliżone do innej Grupu Carbanak
- FIN8 – uruchamiająca specjalizowane kampanie spearphishingowe skierowane do branży detalicznej, restauracyjnej i hotelarskiej

NAJCZĘSTSZE ATAKI

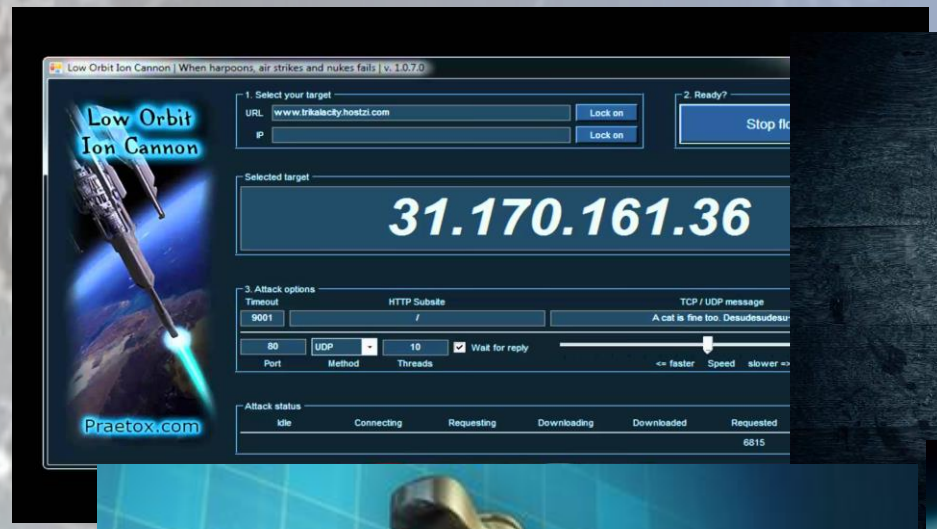








NAJCZĘSTSZE ATAKI



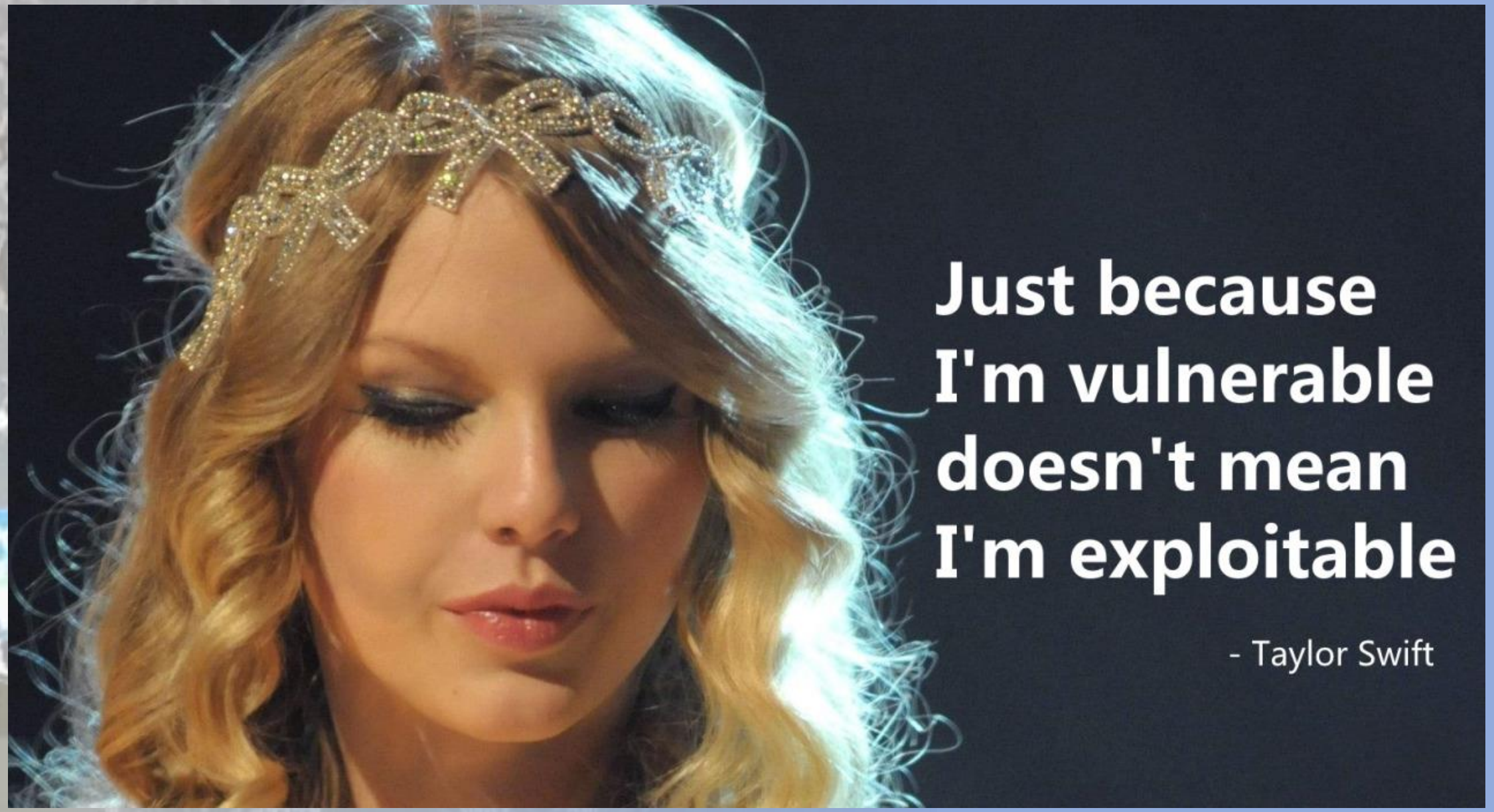
P4AWNP1

POISONTAP

MANA, KARMA

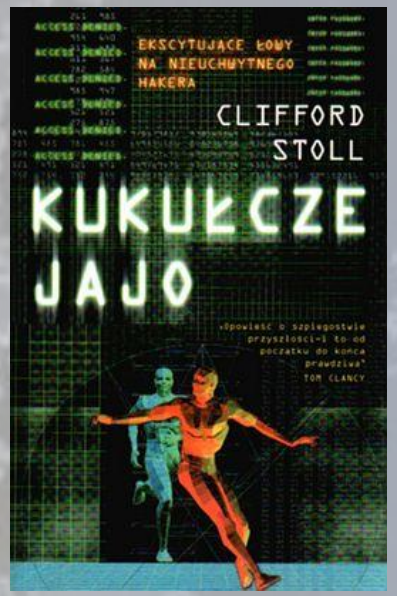
IMSI CATCHER

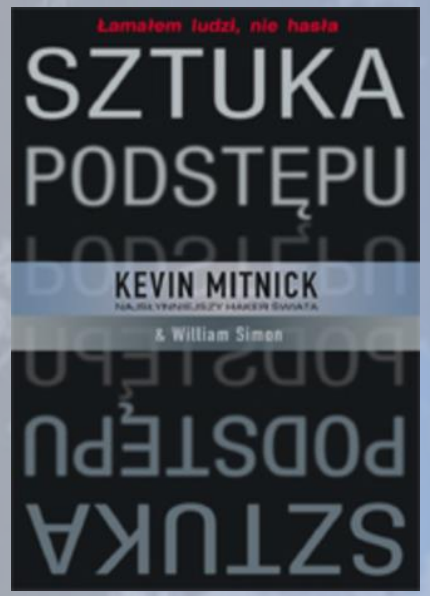
METASPLOIT

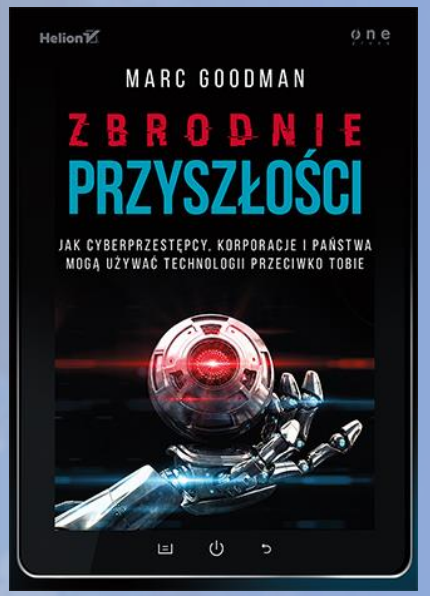

Just because
I'm vulnerable
doesn't mean
I'm exploitable
- Taylor Swift

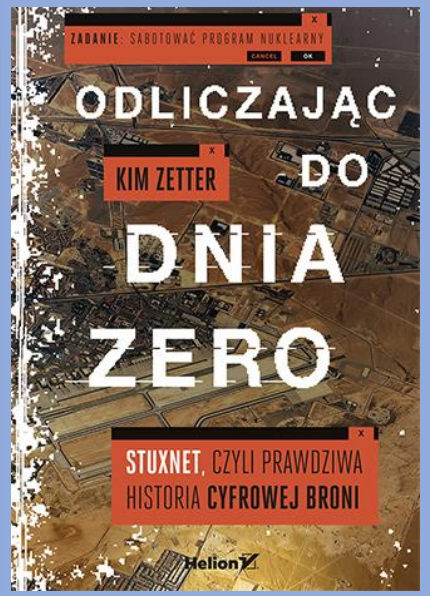
Jeśli znasz siebie
i swego wroga,
przetrwasz
pomyślnie sto bitew.
Jeśli nie poznasz
swego wroga, lecz
poznasz siebie,
jedną bitwę wygrasz,
a drugą przegrasz.
Jeśli nie znasz ni
siebie, ni wroga,
każda potyczka
będzie dla Ciebie
zagrożeniem.

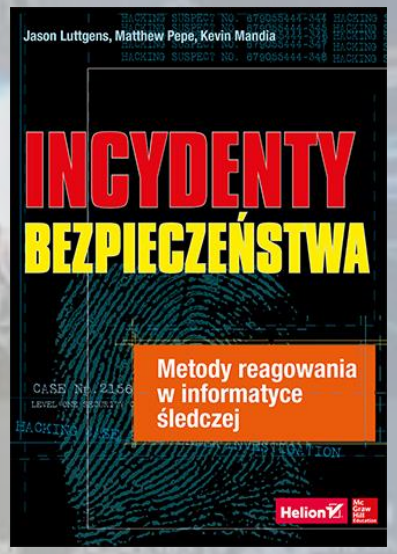
DALSZA LEKTURA

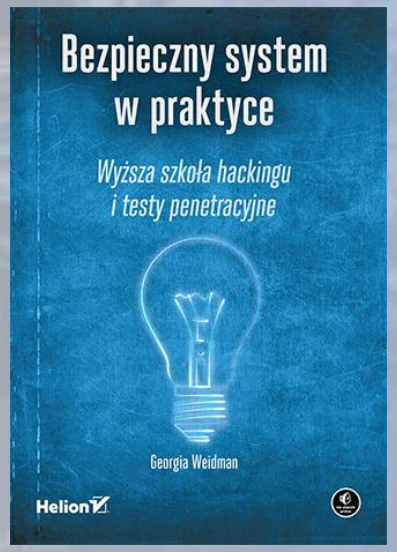


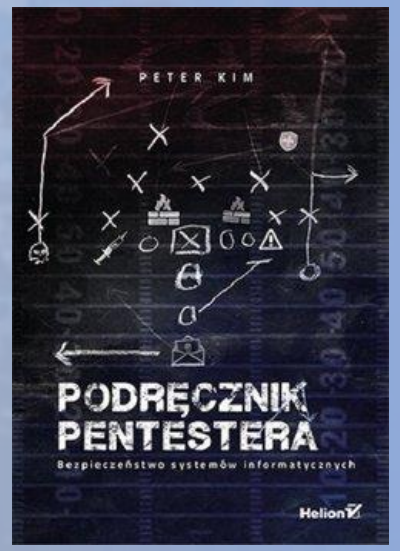












Dziękuję za uwagę

kpt. Grzegorz Data
OISW w Rzeszowie
tel: 17 8580775
voip: 6021060
email: grzegorz.data@sw.gov.pl
JID: 021036gdat@swnet.sw.gov.pl