Cyberbezpieczeństwo – jak się możemy obronić

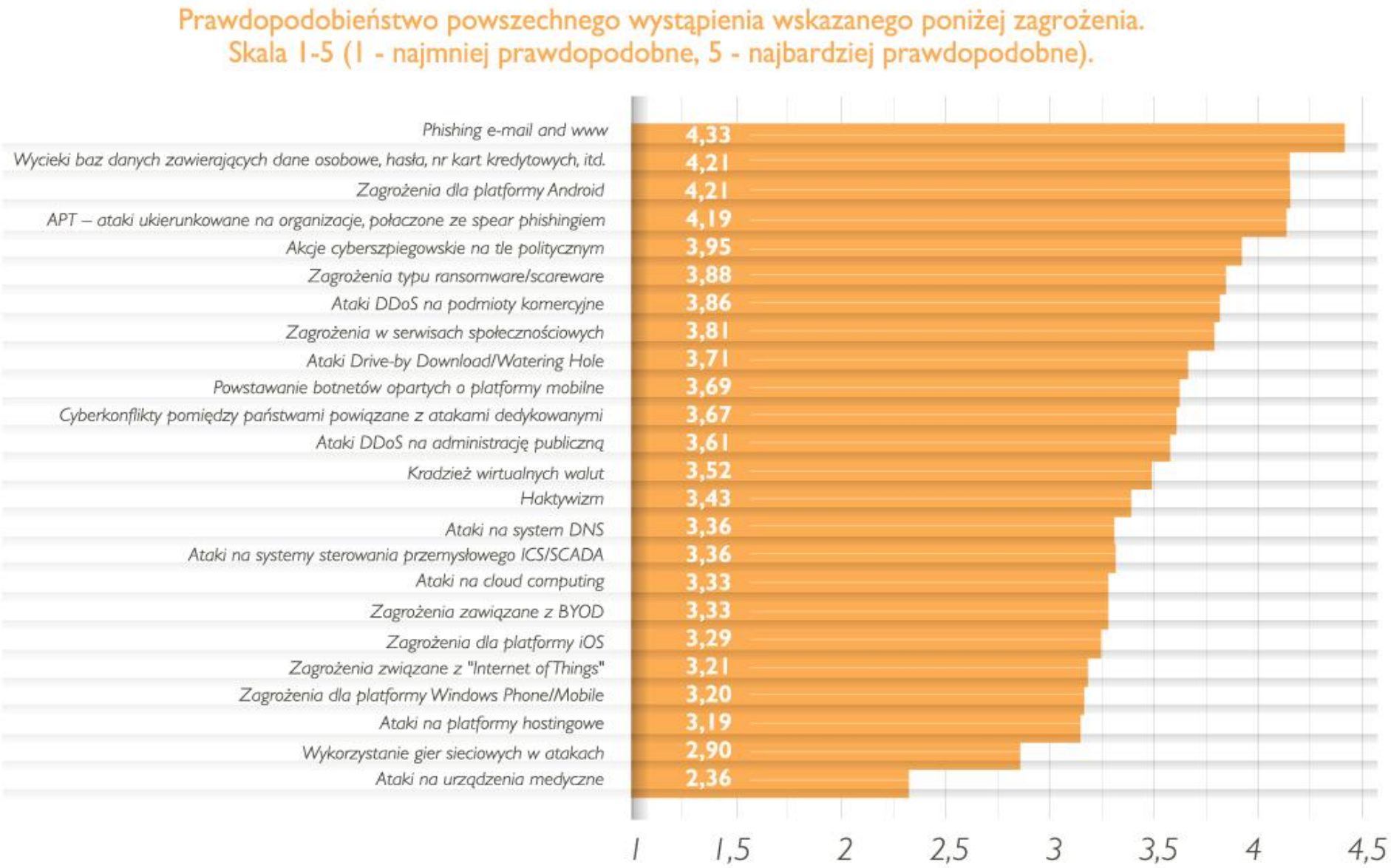
Sławek Brzeziński

Plan

Z dnia na dzień ilość zagrożeń w Cyberprzestrzeni gwałtownie rośnie :
Co nam grozi ?
Czy wiemy jak się przed nimi bronić ?
Jak rozpoznać że jesteśmy atakowani ?
Jakie są rodzaje ataków ?
Jakie są fazy ataku (kill chain) ?
Jakie są rozwiązania których możemy użyć do obrony przed atakiem (Firewall, Anty Malware, …),

i najważniejsze : jak się nie dać zhakować.

Co nam grozi ?
Największe cyberzagrożenia wg Fundacji Bezpieczna Cyberprzestrzeń



Co nam grozi ?
Największe cyberzagrożenia wg Fundacji Bezpieczna Cyberprzestrzeń wynik analizy ryzyka (wysokie prawdopodobieństwo oraz wysokie straty)

- **APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem**
- **Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd.**
- **Akcje cyberszpiegowskie na tle politycznym**
- **Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi**
- **Ataki na systemy sterowania przemysłowego ICS/SCADA**
- **Zagrożenia dla platformy Android**

Co nam grozi ?

1. Ataki **DDOS** z wykorzystaniem między innymi **Internet of Things** – IoT
2. Ataki na zwykłych użytkowników i korporacje – pozyskiwanie informacji (często **phishing**)
3. Ataki na sektor finansowy – Carbanak, atak na infrastrukturę SWIFT
4. Paraliż internetu z wykorzystaniem słabości protokołów BGP i DNS
5. Ransomware – szyfrowanie danych dla okupu
6. Ataki APT (Advanced Persistent Threat)
7. Ataki na urządzenia **IoT**
8. Ataki na urządzenia mobilne (w tym Apple)
9. Malvertising – ataki poprzez reklamy na stronach (w tym adware)
10. Ataki użyciem wbudowanych języków i narzędzi administratorskich (PowerShell)
11. Zwiększenie ruchu szyfrowanego w internecie (problem w analizie ruchu)
12. Ataki exploit na systemy wirtualne w chmurze – współdzielenie zasobów ułatwia ataki (technologia Docker, AWS – ostatnie problemy w trakcie awarii)
13. Ataki polityczne i społeczne

Czy wiemy jak się przed nimi bronić ?

1. Ataki **DDOS** z wykorzystaniem między innymi **Internet of Things** – IoT
Systemy AntyDDOS (w warstwie sieciowej oraz aplikacyjnej
2. Ataki na zwykłych użytkowników i korporacje – pozyskiwanie informacji (często **phishing**)
„Higiena" urządzeń końcowych, wysoka świadomość
3. Ataki na sektor finansowy – Carbanak, atak na infrastrukturę SWIFT
Zaawansowane systemy cyberochrony
4. Paraliż internetu z wykorzystaniem słabości protokołów BGP i DNS
Wdrażanie zabezpieczeń po stronie dostawców internetu (ryzyko nowych luk)
5. Ransomware – szyfrowanie danych dla okupu
„Higiena" stacji, zaawansowane systemy zabezpieczeń stacji, backupy danych
6. Ataki APT (Advanced Persistent Threat)
Zaawansowane mechanizmy zabezpieczeń w każdej fazie ataku
7. Ataki na urządzenia **IoT**
Korzystanie z urządzeń markowych dostawców, utrzymanie „higieny" urządzeń
8. Ataki na urządzenia mobilne (w tym Apple)
Utrzymanie w „higienie" urządzeń, systemy zabezpieczające w systemie Android, aplikacje tylko z zaufanych źródeł

Czy wiemy jak się przed nimi bronić ?

9. Malvertising – ataki poprzez reklamy na stronach (w tym adware)
Korzystanie z dodatków blokujących podejrzaną treść
10. Ataki użyciem wbudowanych języków i narzędzi administratorskich (PowerShell)
Minimalizacja korzystania z wysokich uprawnień, czujność przy korzystaniu z narzędzi do testów penetracyjnych i innych
11. Zwiększenie ruchu szyfrowanego w internecie (problem w analizie ruchu)
Zastosowanie systemów rozszyfrowujących (przepakowanie https) i analiza ruchu do warstwy 7
12. Ataki exploit na systemy wirtualne w chmurze – współdzielenie zasobów ułatwia ataki (technologia Docker, AWS – ostatnie problemy w trakcie awarii)
Utrzymanie wysokiego poziomu bezpieczeństwa (hardening, patchowanie)
13. Ataki polityczne i społeczne
Wszystko co powyżej ☺

Jak rozpoznać że jesteśmy atakowani ?

Wykorzystywanie zaawansowanych systemów klasy SIEM (Security information and event management) zbierających i korelujących logi z systemów operacyjnych, baz danych, aplikacji,

analizy Threat intelligence – źródła zewnętrzne i wewnętrzne

analiza anomalii ruchu sieciowego

analizy zdarzeń z systemów File Integrity monitoring

Jakie są rodzaje ataków ?

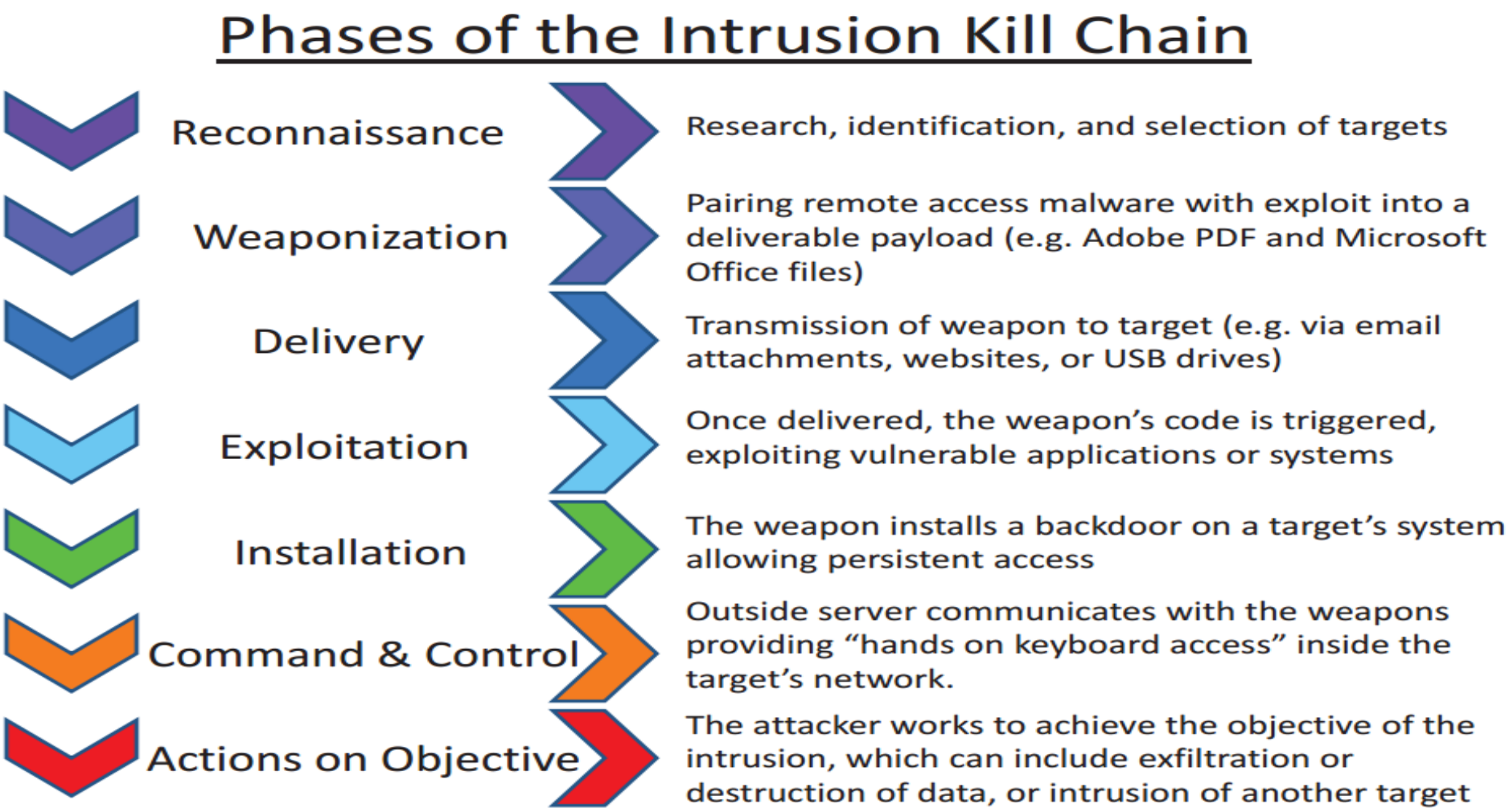
Ataki odmowy dostępu - DDOS
Ataki z wykorzystaniem malware
Podsłuchiwanie / przejęcie sesji
Ataki na serwery www dostępne w internecie
Przejęcie haseł
…….
…….

Czym jest kill chain ?

Kill chain wywodzi się z obronności.
Żeby doszło do uśmiercenia pociskiem przeciwnika zachodzi cały łańcuch poprzedzających to wydarzenie zdarzeń. Określa się go kill chain. Rozpoczyna się od produkcji kuli w fabryce do zabicia wroga.

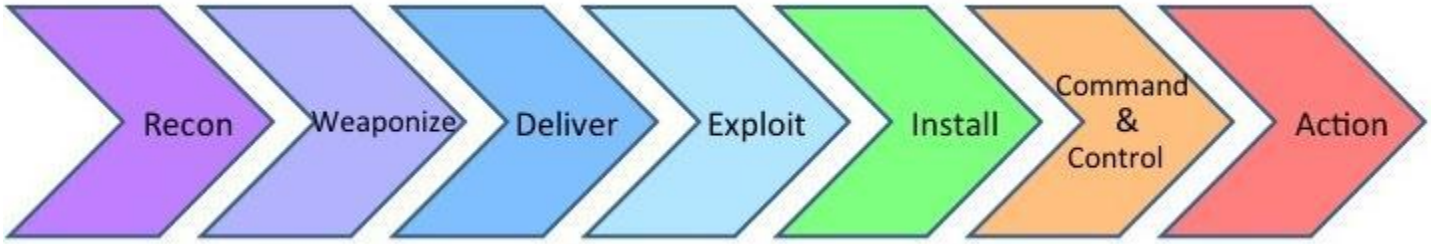
Firma Lockheed Martin opierając się na tym modelu opracowała model **Cyber kill chain** który wspiera działania w zakresie zapewnienia bezpieczeństwa cybernetycznego w szczególności atakom **APT**.

Czym jest kill chain – fazy ataku ?



Źródło *Lockheed Martin*

Czym jest kill chain – fazy ataku ?



Rekonesans – rozpoznanie celu ataku
Weaponization – działania przygotowujące do przeprowadzenia ataku
Delivery – dostarczenie niebezpiecznego oprogramowania (malware)
Exploitation – wykonanie złośliwego kodu na komputerze ofiary
Install (Persistence/Lateral Movement) – przechodzenie pomiędzy systemami w celu penetracji zasobów i zdobycia wyższych uprawnień
Command and Control – instalacja nowego malware oraz zarządzanie zainfekowanymi / przejętymi przez stacjami
Actions – zdobycie danych przez przestępcę
Kolejny krok który można wydzielić to **Exfiltration** – wyciek danych z zasobów instytucji

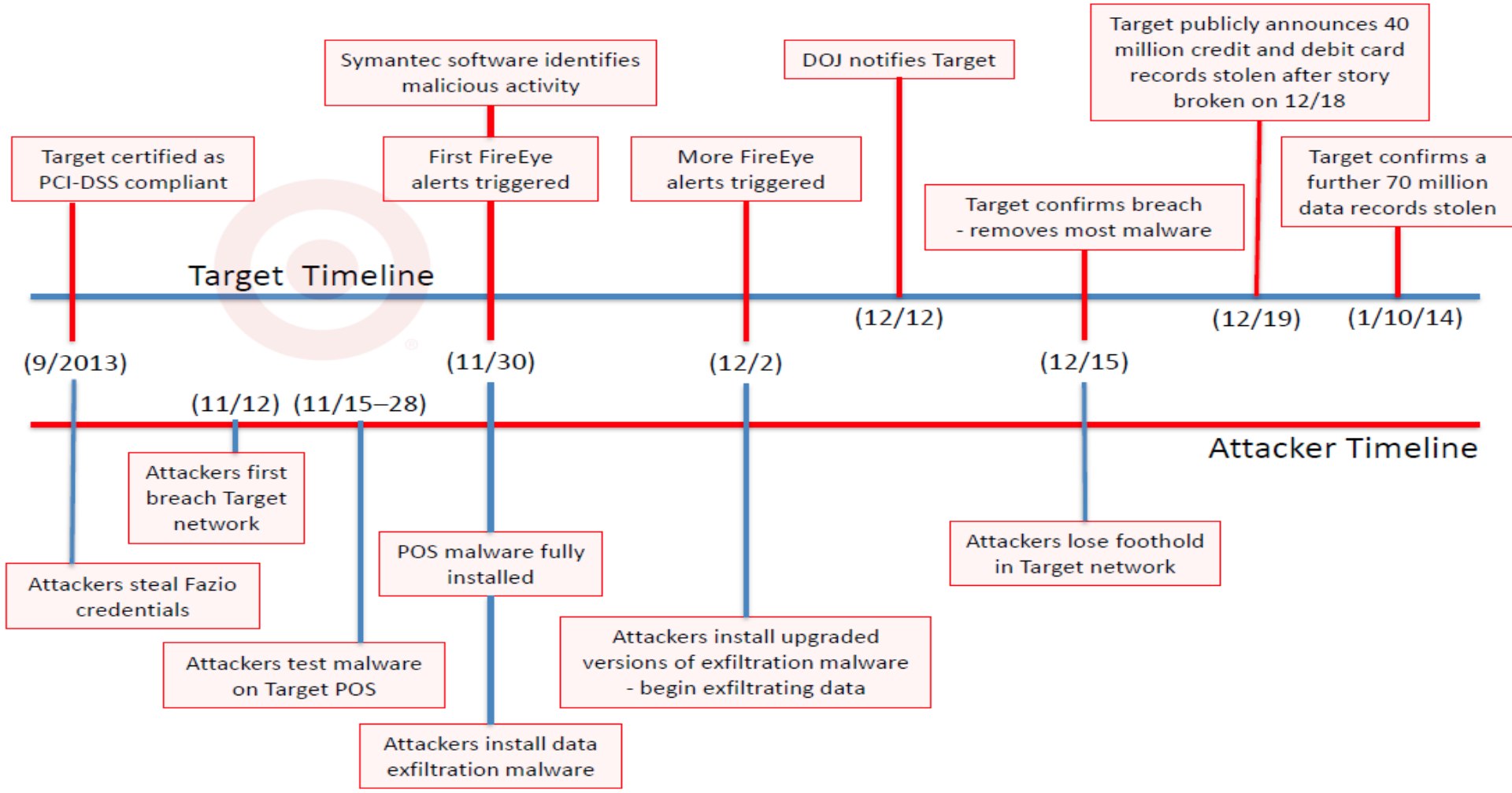
Źródło *Lockheed Martin*

Czym jest kill chain – metody obrony?

Detect – wykrycie ataku/zagrożenia
Deny – blokowanie ataku/zagrożenia
Disrupt – przerywanie ataku/zagrożenia
Degrade - przeszkadzanie w zmaterializowaniu się ataku/zagrożenia
Deceive – zmylenie atakującego
Contain - ograniczanie powierzchni ataku/zagrożenia

Źródło *Lockheed Martin*

Czym jest kill chain – przykład kradzież danych z kart z sieci sklepów Target ?



Źródło - A "Kill Chain" Analysis of the 2013 Target Data Breach. COMMITTEE ON COMMERCE, SCIENCE, AND TANSPORTATION

Przykład Kill chain z życia ☺