DOI:10.35774/app2022.03.153
UDC УДК 351.746

Dr Agata Opalska-Kasprzak,
Instytut Nauk o Polityce i Administracji, Wydział Nauk Społecznych, Uniwersytet Humanistyczno-Przyrodniczego w Siedlcach
ORCID: https://orcid.org/0000-0002-4872-0715

Dr Wojciech Kasprzak,
Wyższa Szkoła Bankowa w Warszawie
ORCID: https://orcid.org/0000-0003-3683-7825

WSPÓŁCZESNE ZAGROŻENIA CYBERBEZPIECZEŃSTWA. ANALIZA NA ROK 2022 W OPARCIU O BADANIA MANDIANT

Współczesne zagrożenia cyfrowe cały czas ewoluują by optymalnie dostosować swój obecny kształt i charakter. W artykule przedstawiono najpopularniejsze rodzaje zagrożeń od strony programowej (malware) oraz opisano główne kategorie złośliwego oprogramowania w oparciu o raport firmy Mandiant na rok 2022. Przedstawiono dane statystyczne dotyczące przestępczości teleinformatycznej na terenie Polski, posługując się dostępnymi oficjalnie statystykami sporządzonymi przez pracowników Komendy Głównej Policji.

Słowa kluczowe: *cyberbezpieczeństwo, zagrożenia, oprogramowanie, Mandiat.*

Opalska-Kasprzak A., Kasprzak W.
Modern cybersecurity threats. 2022 Analysis based on Mandiant research
Contemporary digital threats are constantly evolving to optimally adapt their present shape and character to the present times. The article presents the most popular types of threats from the software side (malware) and describes the main categories of malware based on the Mandiant report for 2022. Statistical data on ICT crime in Poland are presented, using officially available statistics prepared by employees of the National Police Headquarters.

Keywords: *cyber security, threats, software, Mandiant.*

Опальська-Каспжак А., Каспржак В.
Сучасні загрози кібербезпеці. Аналіз 2022 року на основі досліджень Мандіант
Сучасні цифрові загрози постійно розвиваються, щоб оптимально адаптувати свою поточну форму та характер до теперішнього часу. У статті представлено найпопулярніші типи загроз з боку програмного забезпечення (зловмисне програмне забезпечення) та описано основні категорії шкідливого програмного забезпечення на основі звіту Mandiant за 2022 рік. Наведено статистичні дані щодо злочинів у сфері ІКТ у Польщі з використанням офіційно доступної статистики, підготовленої співробітниками Головним управлінням поліції на підставі відкритого провадження.

Ключові слова: *кібербезпека, загрози, програмне забезпечення, Мандіат.*

Sformułowanie problemu. Współczesne społeczeństwo informacyjne 2.0 powoli wchodzi w okres przygotowawczy do adaptacji rozwiązań dla kategorii 3.0 - szerzej korzystające z algorytmów AI (Artificial Intelligence - z ang. Sztuczna inteligencja), IoT (Internet of Things – z ang. Internet rzeczy) i AR (Augmented Reality – z ang. Rzeczywistości rozszerzona). W kontekście wyjaśnienia, mowa tutaj o wysoce rozwiniętym społeczeństwie używającym dobrodziejstw technologicznych do realizacji codziennych celów. Rozwój technologiczny zawsze możemy porównać do dwóch przeciwstawnych płaszczyzn. Pierwsza otwiera nam drogę do najnowocześniejszych technologii - zachęcając do korzystania z nich. Druga natomiast to sfera stale rosnących zagrożeń wynikających z niekontrolowanego rozwoju technologicznego, ale także z faktu, że wiele współczesnych technologii, jak np. AI jest adaptowana na rzecz działań przestępczych. Należy zatem stale monitorować sieć i wiadomości dotyczące incydentów bezpieczeństwa, by lepiej zrozumieć konieczność adaptacji rozwiązań cyberbezpieczeństwa aktywnego [w znaczeniu współczesnej sfery programistycznej, analizy złośliwego kodu i możliwości zdalnego ograniczenia działań hakera w cyberprzestrzeni; zaliczamy tutaj również wszelkie kategorie oprogramowania zapewniającego bezpieczeństwo cyfrowe i rozwiązania aktywnego monitorowania połączeń teleinformatycznych], proceduralnego [służy celom stworzenia jak najbardziej optymalnych zasad korzystania z

systemów teleinformatycznych, urządzeń cyfrowych i ogólnie rozumianego bezpieczeństwa w czasie korzystania z cyberprzestrzeni w warunkach prywatnych i służbowych] oraz technik kryminalistyki informatycznej [4, s. 64; 2; s. 308].

Jedną z firm będących najlepszym źródłem informacji z dziedziny cyberbezpieczeństwa i narzędzi hakerskich jest Mandiant. „Firma Mandiant jest uznawana przez przedsiębiorstwa, rządy i organy ścigania na całym świecie za lidera rynku w zakresie analizy zagrożeń i wiedzy zdobytej na frontach cyberbezpieczeństwa. Aby każda organizacja była gotowa na zagrożenia cybernetyczne, Mandiant skaluje swój wywiad i wiedzę ekspercką za pośrednictwem platformy Mandiant Advantage SaaS, aby dostarczać aktualne informacje, automatyzować badanie ostrzeżeń, ustalać priorytety oraz weryfikować produkty kontroli bezpieczeństwa pochodzące od różnych dostawców" [6]. Zakres badania incydentów cyfrowych dotyczy okresu od 1 października 2020 roku do 31 grudnia 2021 roku (15 miesięcy) [5, s. 6].

W pierwszej kolejności należy zwrócić uwagę na dane statystyczne przedstawiające rodzaj zastosowanego złośliwego oprogramowania w roku 2021 [5, s. 24]:

Zdecydowaną większość zagrożeń powodowały incydenty z wykorzystaniem oprogramowania typu „Backdoor" [1, s. 93] (z ang. „Tylne drzwi"), obejmując blisko 40% zdarzeń. Metoda ta polega na zdalnym dostaniu się napastnika do wnętrza systemu i możliwości przejęcia kontroli. Haker może wtedy wydawać zarażonej maszynie skonkretyzowane polecenia i uzyskuje dostęp do wewnętrznych zasobów danych przechowywanych w systemie. Możliwe jest również wejście głębiej w atakowany system, używając zarażonego komputera jako furtki do zamkniętego systemu, np. korporacyjnego lub rządowego. Złośliwe oprogramowanie typu Backdoor najczęściej infekuje dany system poprzez zastosowanie ataku phishingowego i ręczne uruchomienie wirusa podszywającego się pod plik o innym przeznaczeniu (np. fałszywe pliki z rozszerzeniem .pdf lub .doc) przez ofiarę [3, s. 890]. Rzadziej i w bardziej wyrafinowanych przypadkach Backdoor może zostać odkryty w systemie jako luka w zabezpieczeniu poprzez działanie hakera i dane na temat potencjalnej drogi wejścia (błędzie w kodzie systemowym) dostarczane są agresorowi.

Drugie miejsce zajmuje Dropper. Program ten służy do swoistego zakraplania (pobierania i instalowania bez wiedzy użytkownika) innych złośliwych programów, które nie mogą się dostać do systemu odrębnymi metodami. Dropper jest groźny z tego powodu, że nigdy nie wiadomo, jakie dodatkowo oprogramowanie pobierze do pamięci urządzenia.

Trzecie miejsce na podium zajął atak typu Ransomware przeznaczony w głównej mierze do szyfrowania danych zawartych w systemie i wyłudzania okupu od ofiary w zamian za przywrócenie dostępu. Złośliwe oprogramowanie tego typu najczęściej jest uruchamiane przez ofiarę samodzielnie poprzez plik o pierwotnie innym przeznaczeniu, np. archiwum graficzne lub plik instalacyjny programu użytkowego. Program infekuje system po zainstalowaniu i dokonuje szyfrowania znacznej części przestrzeni dyskowej. Okup najczęściej żądany jest za pośrednictwem kryptowalut.

Miejsce czwarte możemy przypisać oprogramowaniu Downloader, czyli oprogramowaniu przeznaczonemu w głównej mierze do pobierania masowych danych z wnętrza zainfekowanego systemu. Program ten najczęściej nie posiada dodatkowych funkcji, ale przez swoją minimalną inwazyjność jest trudno wykrywalny. Niektóre Downloadery mogą działać nawet przez okres kilku miesięcy lub lat. Oprogramowanie tego typu zazwyczaj nie kategoryzuje pobieranych treści pod kątem ważności, a przechwytuje np. wszystkie nowo powstające pliki tekstowe, graficzne, projektowe itp., w systemie.

Kolejna pozycja z progiem 5% to Credential Stealer (z ang. Złodziej Danych Uwierzytelniających) jest to narzędzie, którego celem jest pobieranie, kopiowanie i przekazywanie do hakera wszelkich danych uwierzytelniających, np. danych logowania zawierających loginy i hasła. Program śledzi system i użytkownika do chwili, w której ten nie zostanie poproszony o podanie danych uwierzytelniających, co aktywuje odpowiedni algorytm wirusa. Wprowadzone dane zostają skopiowane razem z informacją o rodzaju danych, witrynie użycia, treści danych.

Przedostatnim z wyróżnionych kategorii programowych jest Launcher (z ang. Wyrzutnia), posiada podobny mechanizm działania co Dropper, ale różnica polega na inicjowaniu uruchomienia jednego lub kilku plików, bądź funkcji znajdujących się w systemie. Przykładowo może to być wyłączenie zapory lub odblokowanie określonych portów by ułatwić atak właściwy. W systemie cyberbezpieczeństwa może zostać odnotowane działanie Launchera, co umożliwi jego dezaktywację. Problematyczne natomiast staje się odnalezienie plików lub poleceń, jakie program aktywował i poradzenie sobie z potencjalnymi konsekwencjami. Pod postacią ostatniej kategorii utworzono „Inne", w skład której wchodzą np. keyloggery, POS, eksplorator danych, itp.

Drugim istotnym czynnikiem przeanalizowanym przez ekspertów Mandiant była kwestia dostępności do złośliwego oprogramowania [5, s. 26]:

Kategoria publiczna stanowi jedynie 28% dostępu do złośliwego oprogramowania z poziomu zwykłej przeglądarki internetowej. Aby pobrać dostępne w ten sposób wirusy w celu późniejszego ich użycia nie jest wymagana żadna znajomość specjalistycznego oprogramowania kodującego. Paradoksalnie wystarczy jedynie wiedza na temat tego, czego dokładnie szukamy oraz narzędzie, takie jak wyszukiwarka google. Pozostałe oprogramowanie do celów przestępczych, czyli 72% to dostęp niepubliczny. Oznacza to, że wejście w ich posiadanie nie jest związane z darmowym dostępem i konieczne może okazać się wniesienie określonej opłaty. Mogą to być programy przekazywane przez prywatne łącze, znajdujące się na dyskach sprawców, podlegające ciągłym modyfikacjom poprzez nadpisywanie i edycję kodu, jak również te, w których dostęp do programu jest ściśle powiązany z uczestnictwem w zorganizowanej grupie społeczności DarkWeb lub zorganizowanej grupie cyberprzestępczej.

Do najczęściej wykorzystywanych rodzin złośliwego oprogramowania (malware) odnotowanych przez Mandiant należą:

Beacon to backdoor, który jest dostępny komercyjnie jako część platformy oprogramowania Cobalt Strike. Służy do oceny bezpieczeństwa i odtwarzania taktyki i techniki wykorzystywanej przez zaawansowanego hakera w sieci. W czasie, gdy testy penetracyjne koncentrują się na niezałatanych lukach w zabezpieczeniach i błędach konfiguracji, oceny wskazane przez Cobalt Strike są korzystne dla operacji bezpieczeństwa i reagowania na incydenty [7], są także powszechnie używane do testów penetracyjnych środowisk sieciowych. Złośliwe oprogramowanie obsługuje kilka możliwości, takich jak - wstrzykiwanie i wykonywanie dowolnego kodu, przesyłanie i pobieranie plików oraz wykonywanie poleceń. Mandiant potwierdził, że beacon jest używany przez szeroką gamę nazwanych grup zagrożeń, w tym APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9, FIN11, FIN12 i FIN13, a także 650 UNC [5, s. 28]. Technika jest przykładem zaadaptowania rozwiązań cyberbezpieczeństwa do celów przestępczych.

Sunburst to backdoor oparty na platformie .NET, który początkowo komunikuje się za pośrednictwem DNS. Technologia generuje domenę początkowego zdalnego serwera przy użyciu algorytmu generowania domeny. Odpowiedź DNS zwraca rekord CNAME zawierający domenę serwera C2 używanego do późniejszej komunikacji przez HTTP. Obsługiwane polecenia backdoora obejmują pobieranie i wykonywanie plików, zarządzanie plikami, manipulowanie rejestrem i kończenie procesów. Sunburst może również wyłączyć usługi docelowe, aby uniknąć wykrycia i jednocześnie przesłać podstawowe informacje o systemie, w tym adres IP systemu, konfigurację DHCP i informacje o domenie.

Metasploit to platforma do testów penetracyjnych, która umożliwia użytkownikom znajdowanie, wykorzystywanie i weryfikowanie luk w zabezpieczeniach. Mandiant potwierdził, że metasploit jest używany przez grupy APT40, APT41, FIN6, FIN7, FIN11, FIN12, FIN13 i 40 UNC z celami końcowymi od szpiegostwa i zysków finansowych po testy penetracyjne.

Systembc to tuneler napisany w C, który pobiera polecenia związane z proxy, z serwera C2 przy użyciu niestandardowego protokołu binarnego przez TCP. Serwer C2 kieruje systembc do działania jako proxy między serwerem C2 a systemem zdalnym. Systembc może również pobierać dodatkowe ładunki za pośrednictwem protokołu HTTP. Niektóre warianty mogą w tym celu wykorzystywać sieć Tor. Pobrane ładunki mogą być zapisywane na dysku lub mapowane bezpośrednio w pamięci przed wykonaniem. Systembc jest często używany do ukrywania ruchu sieciowego związanego z innymi rodzinami złośliwego oprogramowania. Obserwowane rodziny to DANABOT, SMOKELOADER i URSNIF. Mandiant potwierdził, że systembc używany jest przez FIN12 i aż 10 grup UNC. Cele związane są z zyskiem finansowym. Lockbit to ransomware napisane w C, które szyfruje pliki przechowywane lokalnie i w udziałach sieciowych. Lockbit może również identyfikować dodatkowe systemy w sieci i propagować za pośrednictwem SMB. Przed zaszyfrowaniem plików lockbit czyści dzienniki zdarzeń, usuwa kopie woluminów w tle oraz kończy procesy i usługi, które mogą mieć wpływ na jego zdolność do szyfrowania plików. Lockbit został zaobserwowany przy użyciu rozszerzenia pliku „.lockbit" dla zaszyfrowanych plików. Mandiant potwierdził, że lockbit jest używany przez ponad 10 grup UNC, a cele są związane z zyskami finansowymi i szpiegostwem [5, s. 28].

Ryuk to ransomware napisane w C, które szyfruje pliki przechowywane na dyskach lokalnych i sieciowych. Usuwa również pliki kopii zapasowych i kopie woluminów w tle. Niektóre warianty ryuk mogą rozprzestrzeniać się do innych systemów w sieci. Mandiant potwierdził, że ryuk był używany przez FIN6, FIN12 i 10 odrębnych grup z kategorii UNC [5. s. 28].

Przedstawiona analiza procentowa względem obecnych zagrożeń cyfrowych jasno pokazuje, że obecnie najczęściej wykorzystywane są narzędzia dostępu poprzez lukę systemową i oprogramowanie szyfrujące dane. Brak dokładnych danych dotyczących potencjalnych zysków grup przestępczych z wymuszonych okupów za możliwość odszyfrowania zakodowanych plików. Wzrost zagrożenia technikami typu „backdoor" jest związany z premierą nowego systemu Windows 11, która miała miejsce 20 września 2022 roku, jednak wcześniej istniała możliwość testowania wersji próbnej. Początkowo opcja ta była udostępniona wybiórczo dla wybranych grup podmiotów, a dopiero po pewnym czasie dla odbiorców indywidualnych w formie darmowej i dobrowolnej aktualizacji z systemu Windows 10. Każda duża premiera systemu operacyjnego wiąże się ze wzrostem ilości potencjalnych zagrożeń cyfrowych wynikającej ze znacznej ilości błędów w systemie zabezpieczeń. Część ataków może mieć charakter sondowania systemu, by wybadać optymalne metody nieautoryzowanego dostępu. Działa to na zasadzie opóźnienia ataku, by jak najwięcej osób miało już zainstalowany nowy system. Sprawcy natomiast są już w posiadaniu informacji dotyczących określonych luk w zabezpieczeniach mogących ułatwić atak. W innych wypadkach zastosowanie mogą mieć klasyczne, znane, ale nadal skuteczne metody socjotechniki, czego przykładem może być phishing stosowany w celu wyłudzenia kluczowych informacji.

Dostępne dane statystyczne na terenie Polski obejmują przestępczość do roku 2020 i zamieszczone są w zbiorach Komendy Głównej Policji [2, s. 320]. Zestawienie zawiera informacje zbiorcze na temat wszystkich zarejestrowanych spraw z każdego rodzaju przestępczości na tle cyfrowym w Polsce. Należy jednak pamiętać, że nie ma możliwości określenie prawdziwych danych ze względu na występowanie, tzw. ciemnej liczby przestępstw.

Bezprawne uzyskanie informacji – Art. 267 k.k.					
Rok	2016	2017	2018	2019	2020
Suma	2165	2055	2081	4502	4884
Niszczenie danych informatycznych – Art. 268 k.k.					
Rok	2016	2017	2018	2019	2020
Suma	546	506	384	588	714
Uszkodzenie danych informatycznych – Art. 269 k.k.					
Rok	2016	2017	2018	2019	2020
Suma	5	2	6	7	7
Zakłócanie systemu komputerowego – Art. 269a k.k.					
Rok	2016	2017	2018	2019	2020
Suma	39	30	35	30	19
Wytwarzanie programów komputerowych – Art. 269b k.k.					
Rok	2016	2017	2018	2019	2020
Suma	40	24	30	37	41
Oszustwo komputerowe – Art. 287 k.k.					
Rok	2016	2017	2018	2019	2020
Suma	3326	3539	5125	8443	9147
Przestępstwa seksualne przeciwko nieletnim, m.in. z wykorzystaniem systemu teleinformatycznego lub sieci telekomunikacyjnej – Art. 200, 200a, 200b, 202 k.k.					
Rok	2016	2017	2018	2019	2020
Suma	2338	2376	4182	13 882	6044
Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych – Art. 115, 116, 117, 118, 119 ustawy o prawie autorskim i prawach pokrewnych					
Rok	2016	2017	2018	2019	2020
Suma	5479	13 872	7152	4594	11 164
Oszustwo komputerowe – Art. 286 k.k.					
Rok	2016	2017	2018	2019	2020
Suma	39 922	44 162	46 523	55 063	55 036
Wizerunek nagiej osoby lub w trakcie czynności seksualnej – Art. 190a k.k.					
Rok	2016	2017	2018	2019	2020
Suma	1579	1687	2211	2989	2695

Przedstawione statystyki ukazują niepokojącą tendencję wzrostową mimo istniejących technik prewencji cyfrowej. W niektórych przypadkach możemy zaobserwować wzrost liczby czynów przestępczych nawet o 25%. Analizując zebrane liczby nie sposób odnieść wrażenia, że w wielu przypadkach rok 2019 był okresem znacznego nasilenia się działań przestępczych z powodu początku pandemii COVID-19 na świecie. Widać to szczególnie przy wzmożonej aktywności pedofilii w sieci teleinformatycznej, tzw. grooming i łamaniu praw autorskich przez piractwo komputerowe i nielegalne powielanie treści chronionych prawnie. Obecnie w 2022 nadal możemy spodziewać się wzrostu działań przestępczych, biorąc pod uwagę statystycznie zachowanie się liczb w poprzednich okresach oraz czynniki takie jak rozpoczęcie agresji Federacji Rosyjskiej w działaniach wojennych wobec niepodległej Ukrainy, czy też ogólnoświatowy kryzys gospodarczy. Tworzy to pole do działania dla kreatywnych grup cyberprzestępczych. Do rozpowszechniania złośliwego oprogramowania lub wyłudzania danych użytkowników wykorzystuje się fałszywe informacje o chwytliwej i przykuwającej oko nazwie, np. nowe sensacyjne doniesienia dotyczące działań na froncie, aktów terroru, przemocy wobec cywili, itp. Takie informacje zamieszczane na portalach społecznościowych, czy też rozsyłane drogą wiadomości prywatnych mogą wzbudzać zaciekawienie użytkowników, którzy aktywując fałszywe linki lub dokumenty nieświadomie pobierają wirusa. Zatem są to elementy dotyczące wykorzystywania socjotechniki w celu rozpowszechnienia złośliwego oprogramowania. Kryzys ekonomiczny to z kolei idealny sposób na wyłudzanie danych osobowych poprzez oferowanie fałszywych form łatwego i szybkiego zarobku na kryptowalutach, inwestycjach w nieprawdziwe akcje i obligacje spółek państwowych lub reklamowanie różnych form aktywności finansowej przez sfałszowane podobizny znanych autorytetów.

Podsumowując obserwujemy niebezpieczną tendencję wzrostową zagrożeń cyfrowych wykorzystujących zaawansowane metody programowe w skali globalnej i stale rosnącą liczbę czynów zabronionych w obrębie jurysdykcji Polski. Doprowadza to do sytuacji szybszego rozwoju narzędzi hakerskich i metod socjotechnicznego wyłudzania danych, aniżeli tworzenie narzędzi i opracowywanie skutecznych metod prewencji w kategoriach cyberbezpieczeństwa jednostki społecznej, osoby prawnej, bezpieczeństwa państwowego i kryminalistyki informatycznej.

Bibliografia

1. Chojnowski, A. (2020). *Informatyka sądowa w praktyce [Forensic informatics in practice]*. Gliwice: Helion [in Polish].
2. Hołyst, B. (2022). *Kryminologia [Criminology]*; wydanie 12. Warszawa: Wolters Kluwer [in Polish].
3. Hołyst, B. (2018). *Kryminalistyka [Criminology]*; wydanie 13. Warszawa: Wolters Kluwer [in English].
4. Tanner Nadean, H. (2021). *Blue Team I cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczeń sieci [Blue Team I cybersecurity. A toolkit for network security professionals]*. Gliwice: Helion [in English].
5. *M-Trends 2022: Insights into Today's Top Cyber Trends and Attacks*. Retrieved from https://www.mandiant.com/resources/report/m-trends-2022 [in English].
6. *Mandiant*. Retrieved from https://www.mandiant.com/company [in English].
7. https://www.cobaltstrike.com/ (dostęp 31.10.2022).

Стаття надійшла до редакції 18.09.2022