Krajobraz zagrożeń na jakie ataki musimy być gotowi

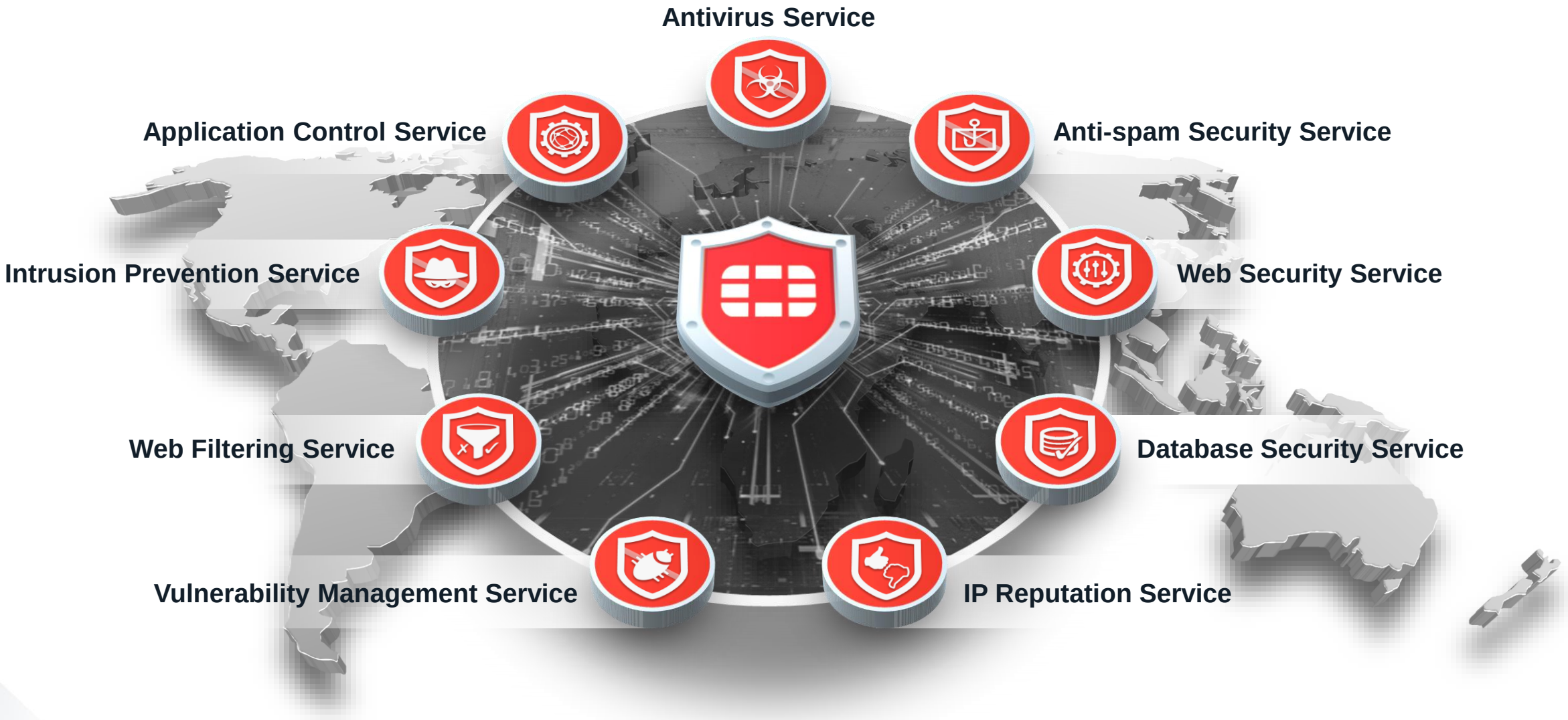
Robert Dąbrowski, CISSP

FORTIGUARD LABS 2019

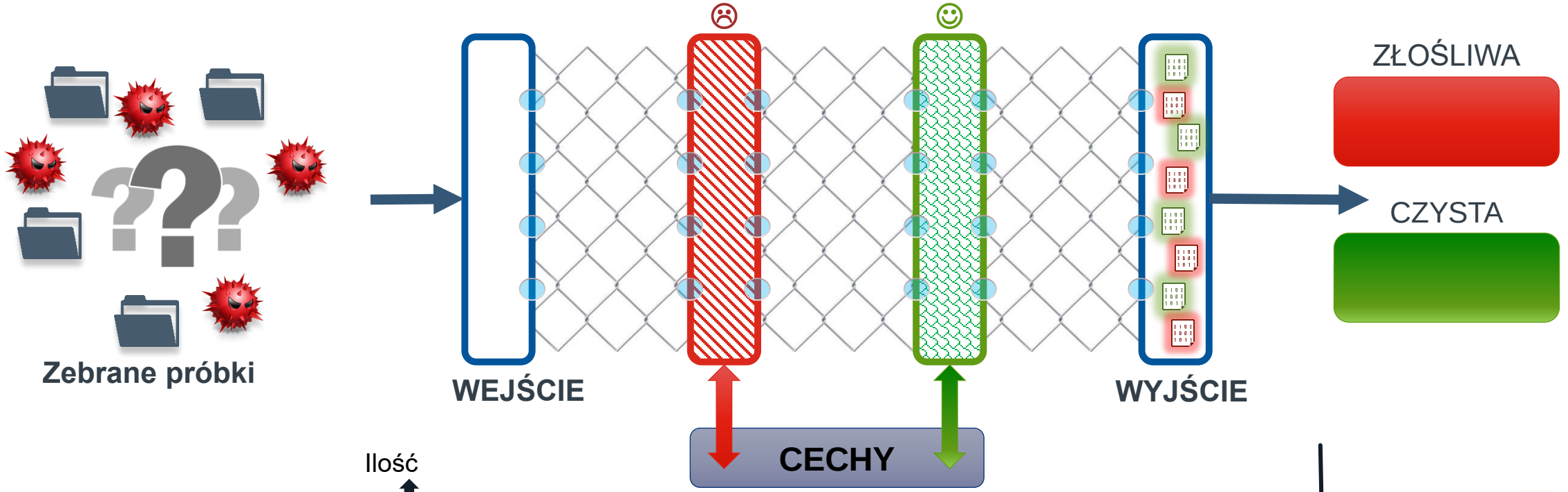
Od 2000, FortiGuard Labs prowadzi prace badawcze w zakresie mechanizmów rozpoznania i ochrony przed cyberzagrożeniami, wyposażając platformy Fortinet w sygnatury i bazy reputacyjne. Oferuje też zaawansowane usługi analityczne bezpośrednio dla klientów Fortinet.

Industry Leading Patented Security Technology

FORTIGUARD LABS 2019

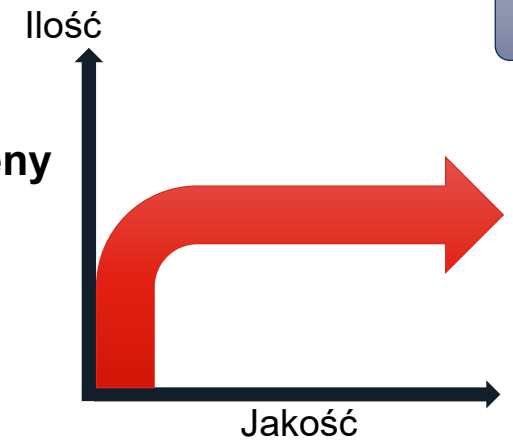


Sztuczna Inteligencja FortiGuard AI

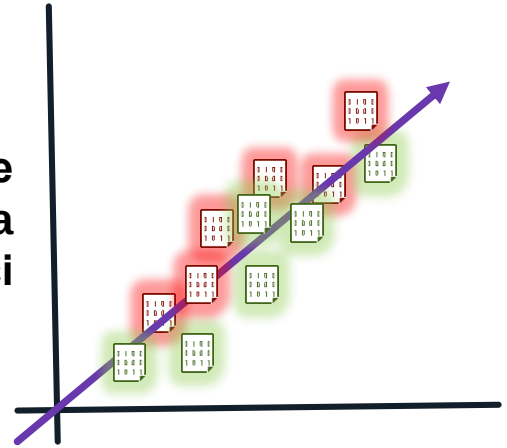


Zwiększenie jakości oceny

- Jakość
- Stabilizowana ilość
- Przypisanie wag



Ciągłe zwiekszanie jakości oraz stopnia pewności



Silence Group

https://www.fortinet.com/blog/threat-research/silence-group-playbook.html

Spear phishing

Złośliwy załącznik:

MS Word

CHM

Download

Kontakt z C&C

Pobranie pliku

Dedykowanego dla

użytkownika

Moduł proxy

Tuning dostępnych narzędzi

Obfuskacja

Trampolina do innych segmentów

Moduł monitorowania

Szpiegowanie zainfekowanej maszyny

Screenshot'y

Komunikacja między procesami

Moduł ATM

Jackpotting

Przejęcie kontroli nad bankomatem

Wynajęcie „Słupa" do pobrania pieniędzy

Statystyki ataków– 4Q2018

Malware

33,653 unikalnych próbek

6,405 różnych rodzin

18% odkrytych Cryptojacking

13.7 wariantów per firma

Exploits

8,309 unikalnych exploit'ów

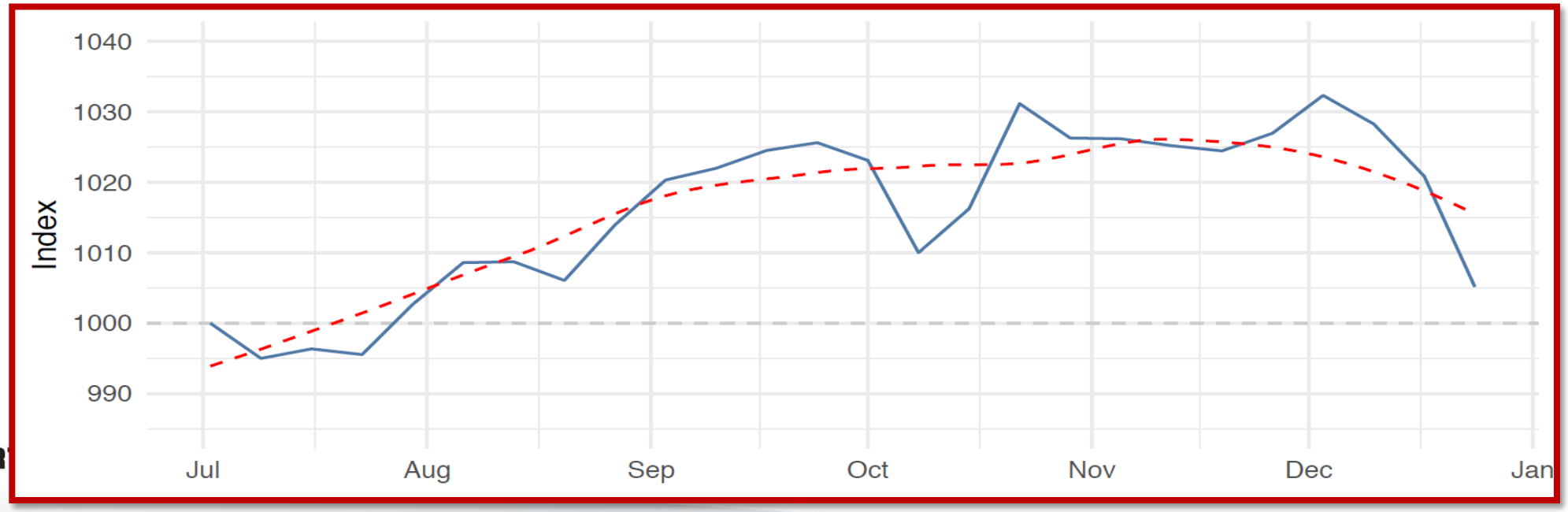
1,218 exploit'ów per firma

54% które doświadczyło poważnych exploit'ów

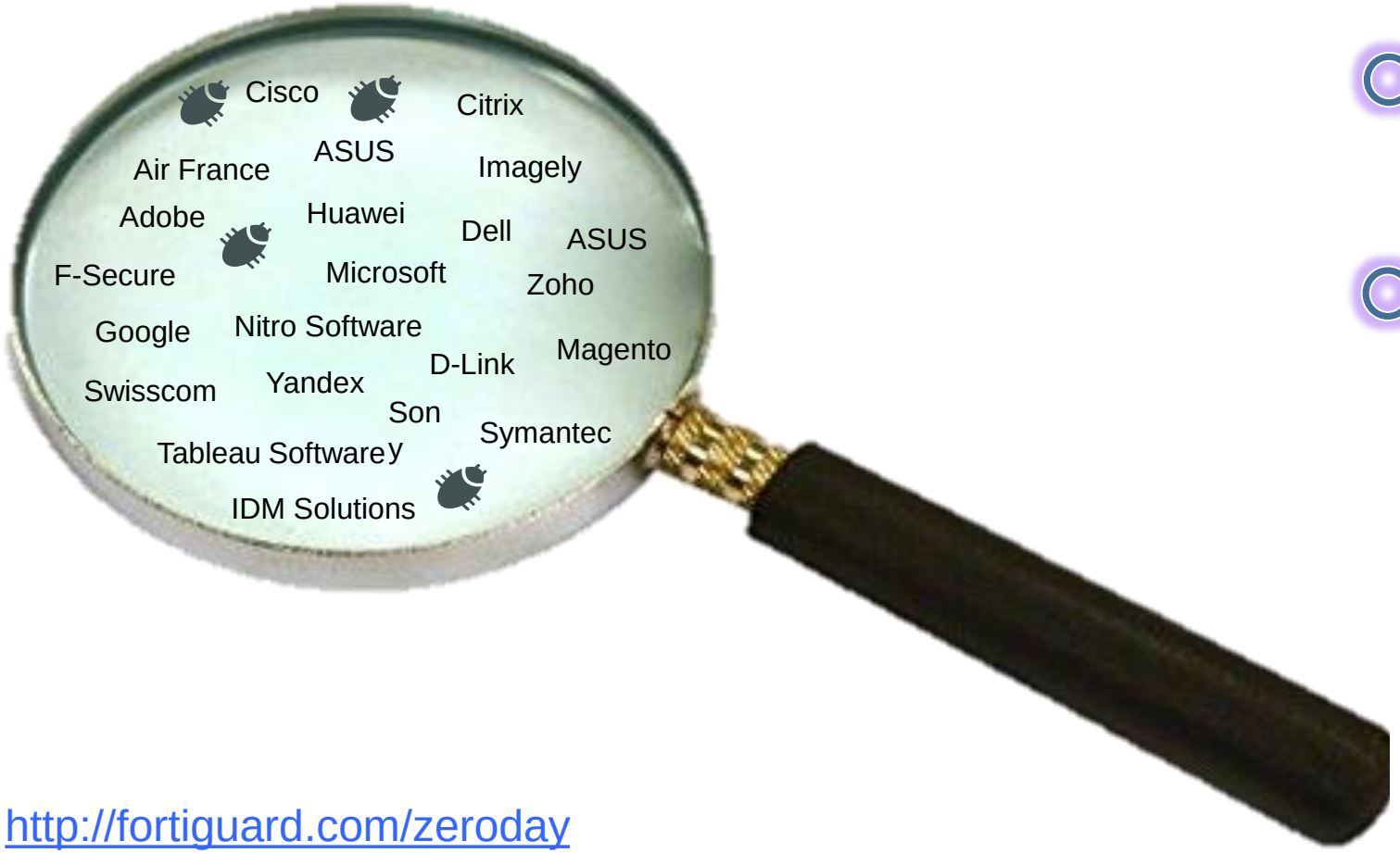
Botnet

261 unikalnych botnetów odkrytych

11.69 dni z aktywną infekcją

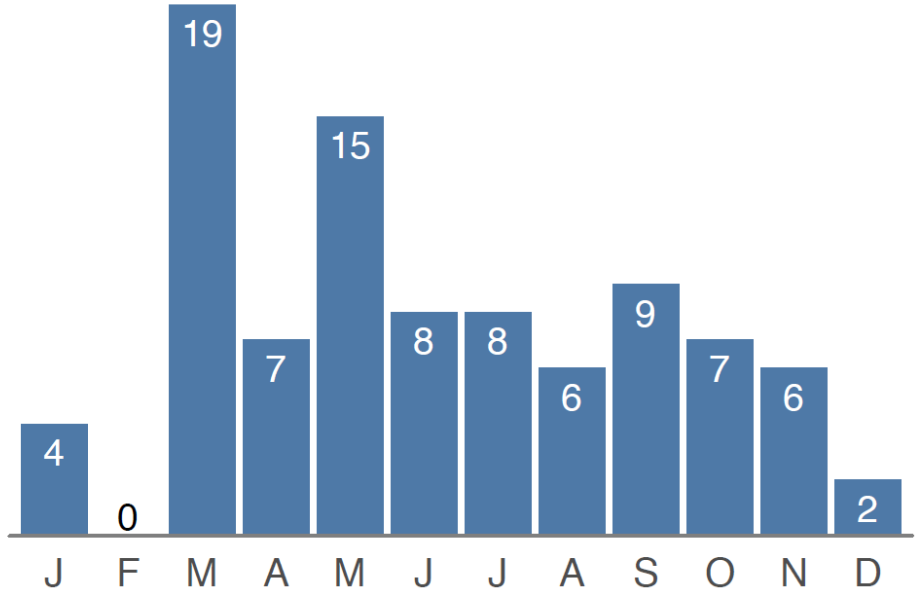


Ataki Zero Day



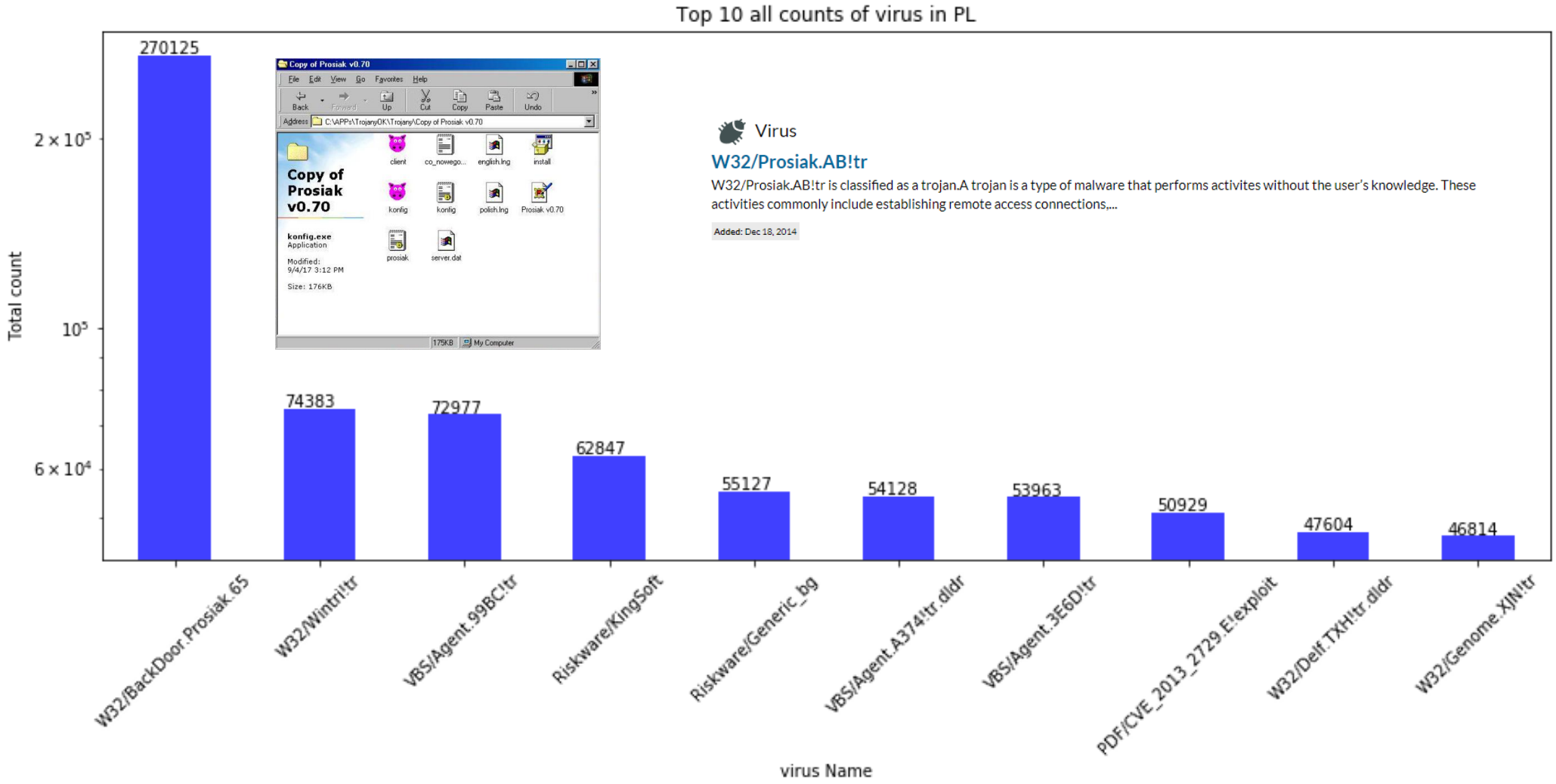
15 zero day
ODKRYTYCH w 4Q 2018

663 zero day
ODKRYTYCH od 2006

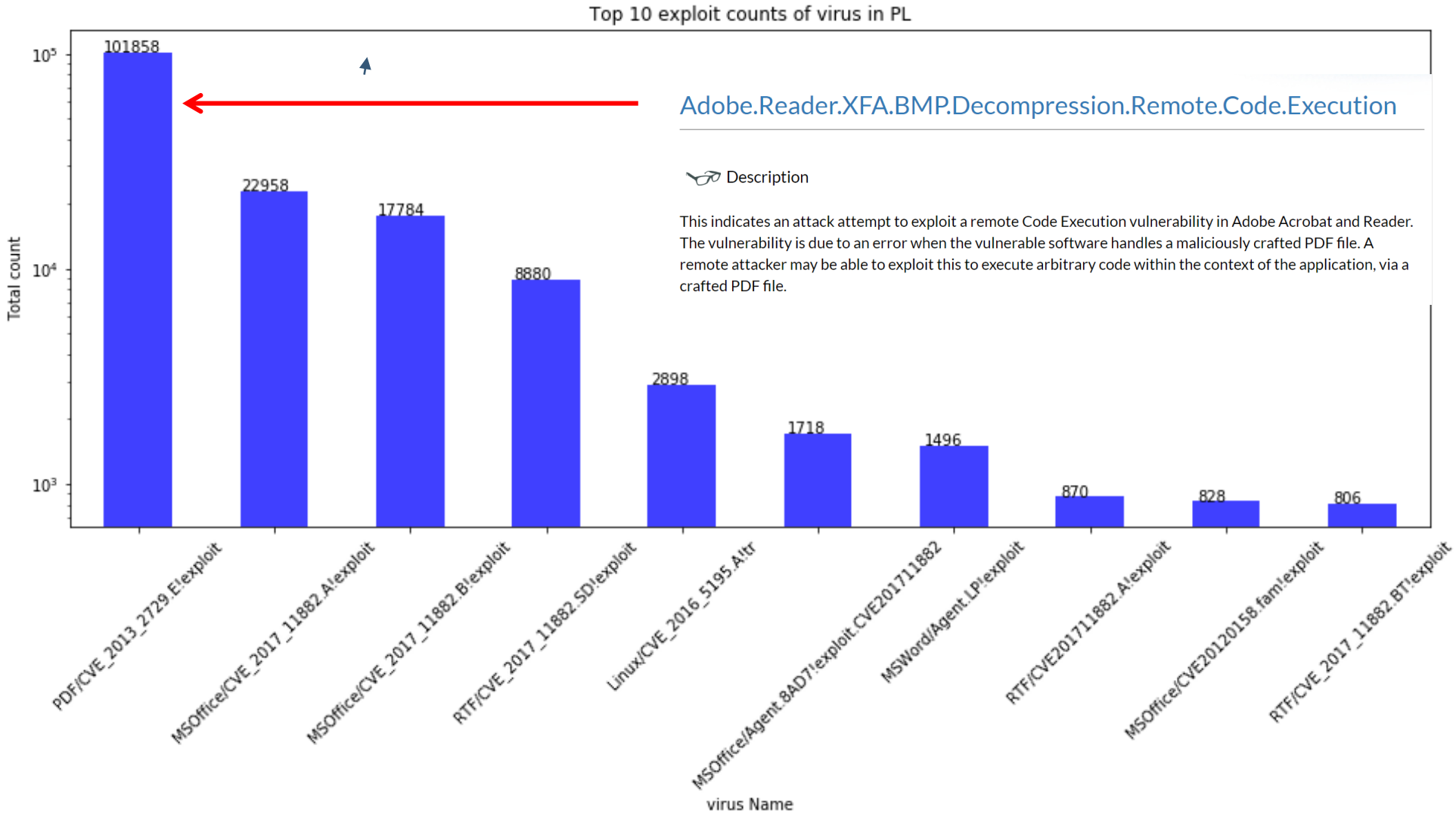


http://fortiguard.com/zeroday

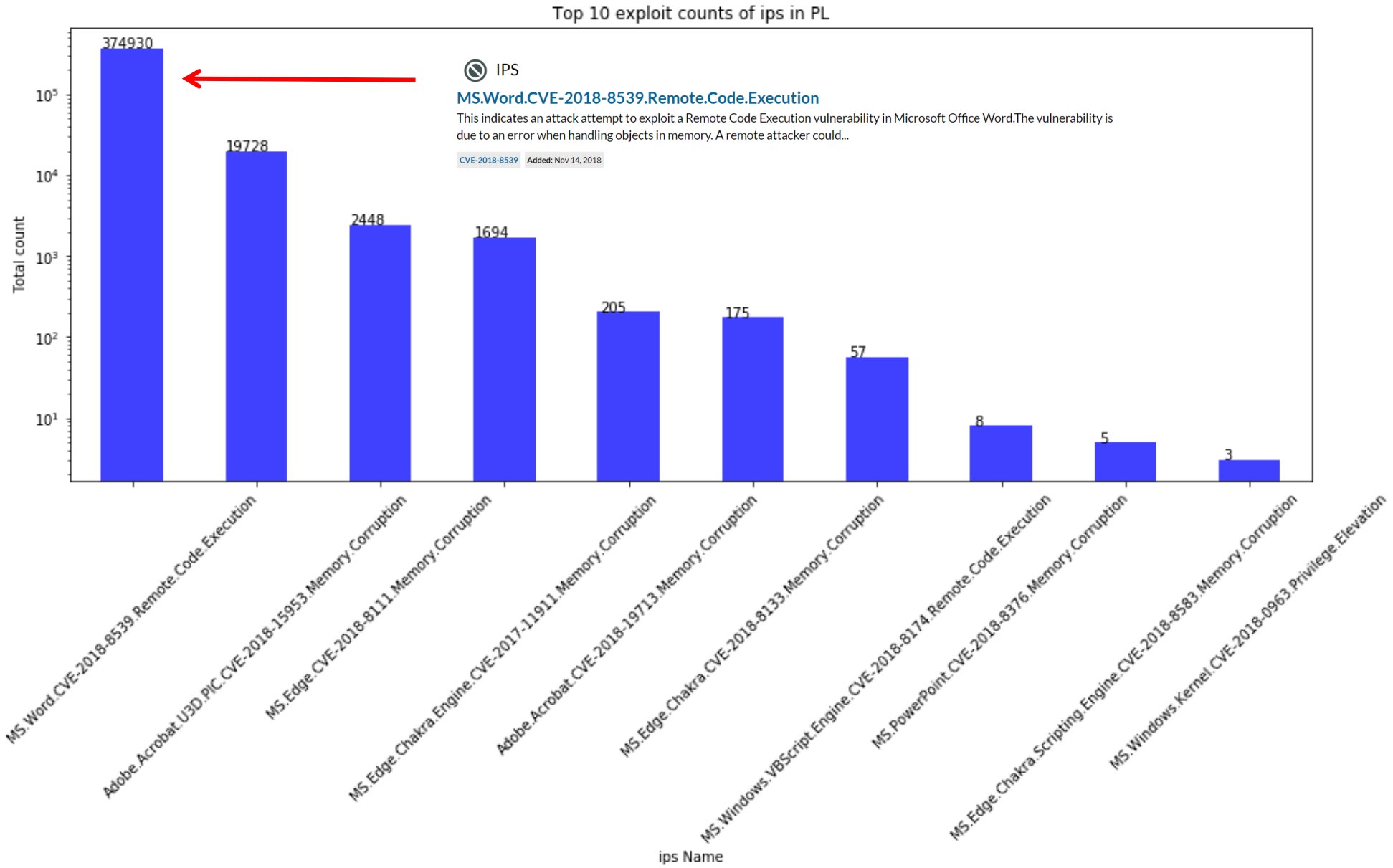
Wirus


Top 10 all counts of virus in PL
Total count
2 × 10⁵
10⁵
6 × 10⁴
270125
74383
72977
62847
55127
54128
53963
50929
47604
46814
W32/BackDoor.Prosiak.65
W32/Wintri!tr
VBS/Agent.99BC!tr
Riskware/KingSoft
Riskware/Generic_bg
VBS/Agent.A374!tr.dldr
VBS/Agent.3E6D!tr
PDF/CVE_2013_2729.E!exploit
W32/Delf.TXH!tr.dldr
W32/Genome.XJN!tr
virus Name
Copy of Prosiak v0.70
Copy of Prosiak v0.70
konfig.exe
Application
Modified: 9/4/17 3:12 PM
Size: 176KB
Virus
W32/Prosiak.AB!tr
W32/Prosiak.AB!tr is classified as a trojan.A trojan is a type of malware that performs activites without the user's knowledge. These activities commonly include establishing remote access connections,...
Added: Dec 18, 2014

Wirus

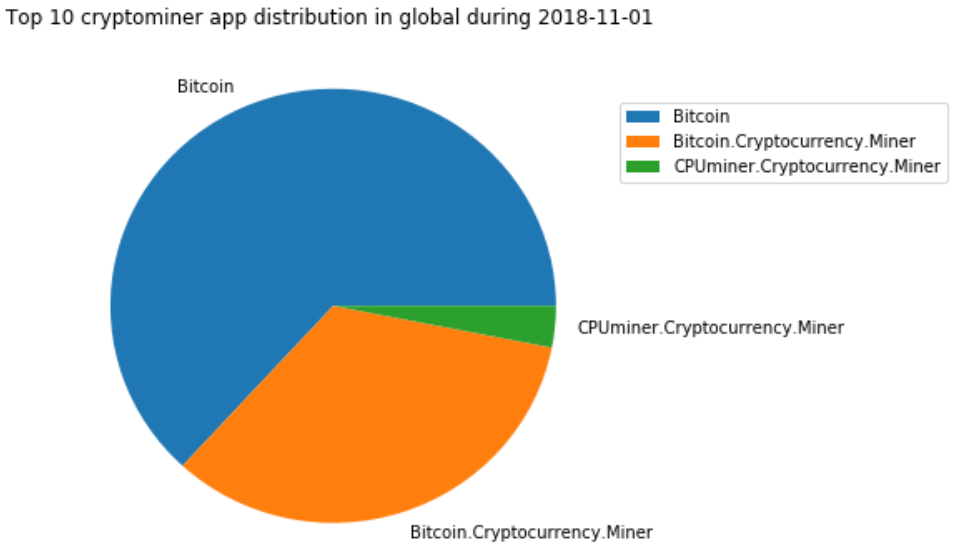


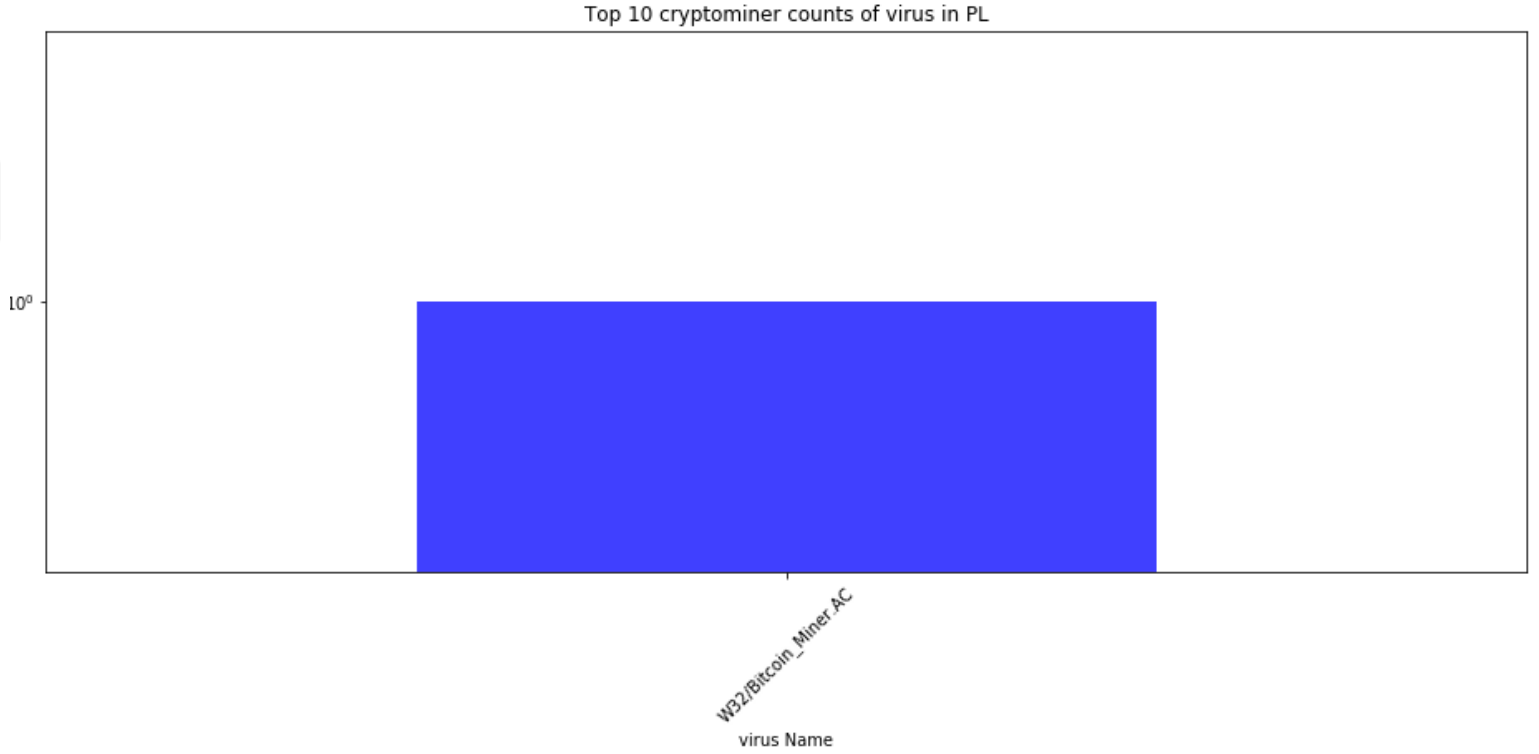
Exploit


Top 10 exploit counts of ips in PL
Total count
ips Name
374930
19728
2448
1694
205
175
57
8
5
3
IPS
MS.Word.CVE-2018-8539.Remote.Code.Execution
This indicates an attack attempt to exploit a Remote Code Execution vulnerability in Microsoft Office Word.The vulnerability is due to an error when handling objects in memory. A remote attacker could...
CVE-2018-8539
Added: Nov 14, 2018
MS.Word.CVE-2018-8539.Remote.Code.Execution
Adobe.Acrobat.U3D.PIC.CVE-2018-15953.Memory.Corruption
MS.Edge.CVE-2018-8111.Memory.Corruption
MS.Edge.Chakra.Engine.CVE-2017-11911.Memory.Corruption
Adobe.Acrobat.CVE-2018-19713.Memory.Corruption
MS.Edge.Chakra.CVE-2018-8133.Memory.Corruption
MS.Windows.VBScript.Engine.CVE-2018-8174.Remote.Code.Execution
MS.PowerPoint.CVE-2018-8376.Memory.Corruption
MS.Edge.Chakra.Scripting.Engine.CVE-2018-8583.Memory.Corruption
MS.Windows.Kernel.CVE-2018-0963.Privilege.Elevation

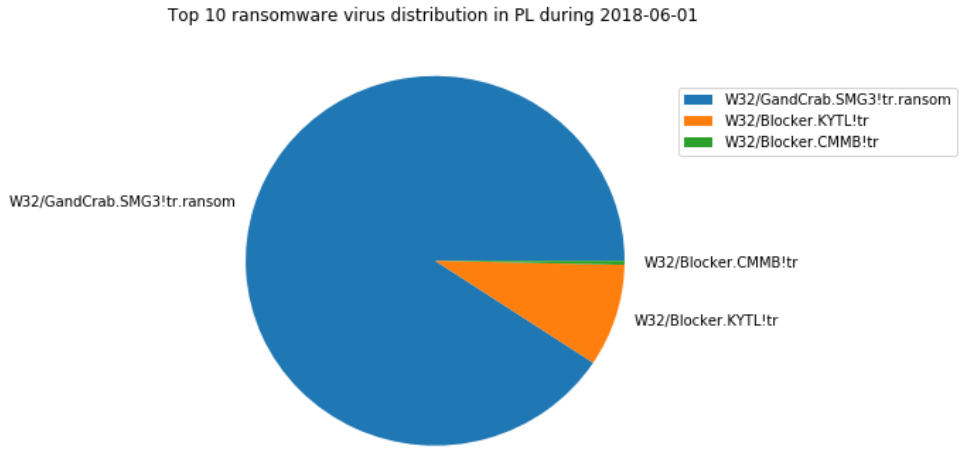
Cryptominer

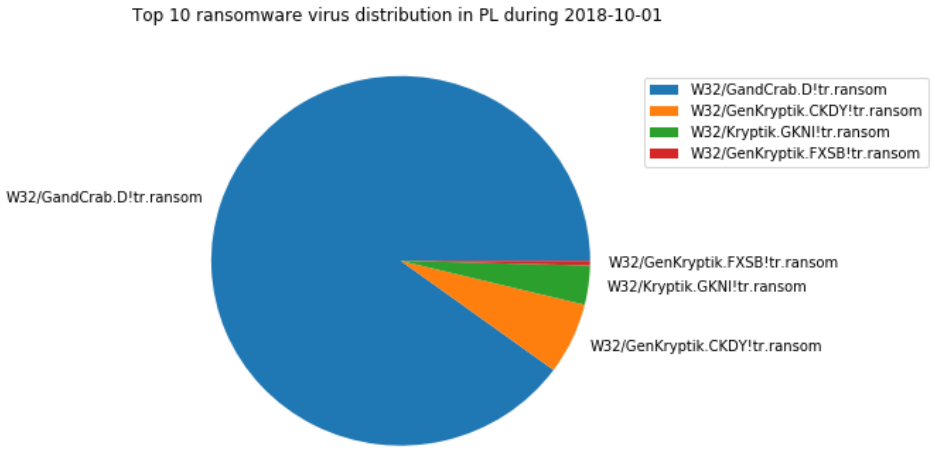
https://www.fortinet.com/blog/industry-trends/bitcoin-mining-is-more-popular-than-ever.html





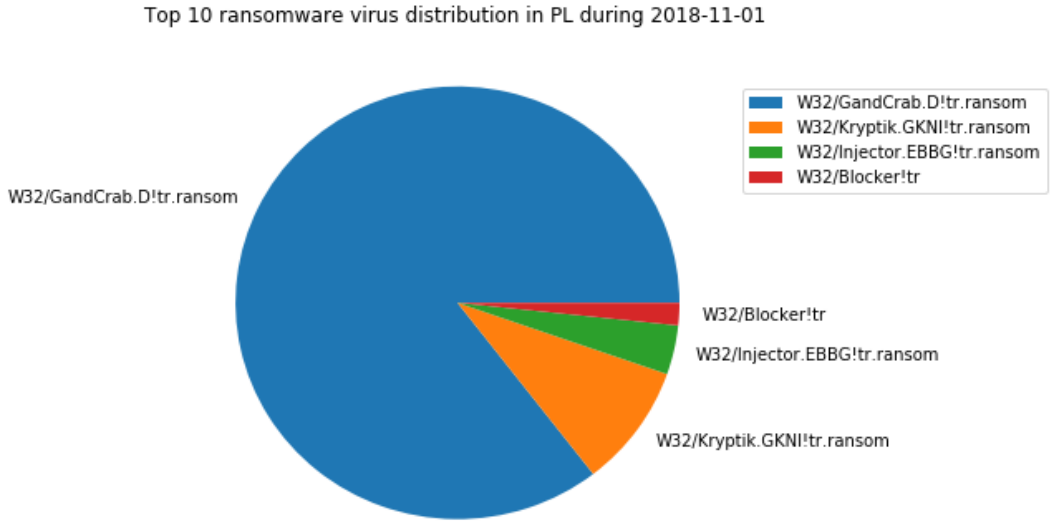
Ransomware





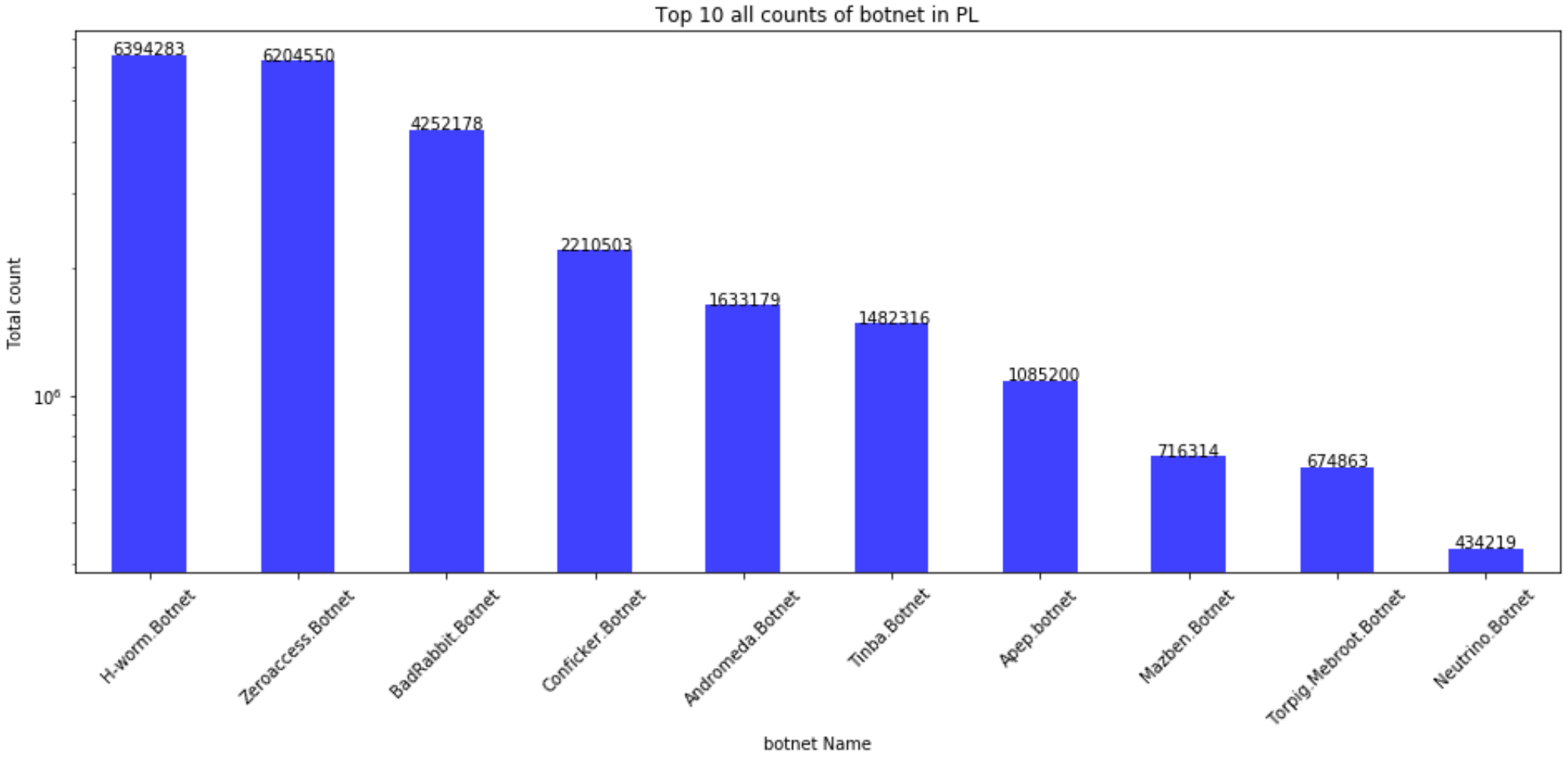
Network Communication

Figure 1 Malware sends Info to list of compromised websites



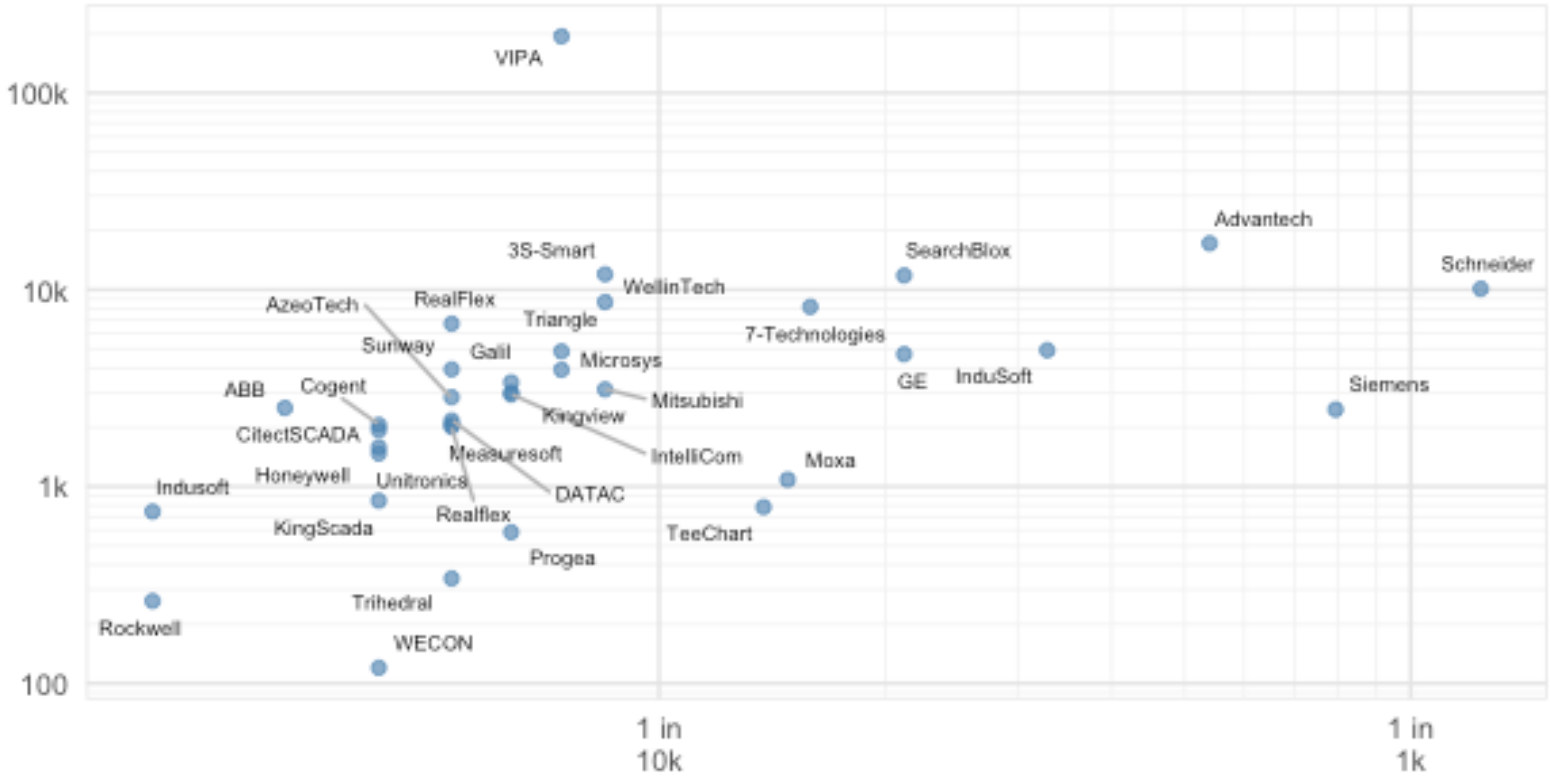
https://www.fortinet.com/blog/threat-research/gandcrab-v4-1-ransomware-and-the-speculated-smb-exploit-spreader.html

Botnet



Krajobraz zagrożeń: exploit'y ICS i SCADA

- ICS/SCADA – mały wolumen ataków (oczekiwane) – jednocześnie poważny wpływ na działanie systemów
- Ataki zaburzają procesy biznesowe, wnikają w infrastrukturę krytyczną, mogą zagrażać życiu ludzi
- Badania przeprowadzone przez Forrester pokazują, że ok. 60% firm używających ICS/SCADA doświadczyło skutecznego ataku w ostatnim roku
- Platformy te powinny być traktowane priorytetowo przy zabezpieczaniu i aktualizacji



Rozpowszechnienie i wolumen exploit'ów ICS/SCADA

Kluczowe tematy i trendy: Rekomendacje

	REKOMENDACJE
Infiltracja Adware	
Adware jest wysoko w rankingu infekcji malware dla wszystkich regionów, dotyczy wszystkich platform	Mechanizmy ochrony muszą dotyczyć całej architektury – kluczem jest zintegrowana i zautomatyzowana ochrona
Automatyzacja exploit'ów	
Cyberprzestępcy używają automatyzacji i uczenia maszynowego w celu propagacji ataków	Konieczne jest zaadoptowanie usług bezpieczeństwa, w tym sandboxing'u w strategiach ochrony – Advanced Malware Protection Service przed znanymi i nieznanymi zagrożeniami
Zwiększająca się powierzchnia ataku	
Coraz więcej ataków wycelowane w urządzenia IoT	Program Monitoring & Risk Assessment pozwoli zrozumieć podatności i nadać priorytety w programach patch'owania
Cryptojacking	
18% firm doświadcza cryptojacking'u - zwiększenie adresowanych platform i wariantów	Monitoruj aktywność procesów | Używaj VPN do segmentacji | Zmień domyślne hasła | Inwentaryzuj IOT | Patch
Wzrost botnetów	
Te same 'STARE' Botnety – nowe triki, nowe kampanie, nowe cele	Konieczna jest ciągła i skuteczna ochrona, dobra cyber higiena, integracja i automatyzacja


FORTINET