



STORMSHIELD

FIREWALL TO ZA MAŁO. JAK SKUTECZNIE CHRONIĆ URZĘDOWĄ SIEĆ W DOBIE ATAKÓW TYPU APT I RANSOMWARE?



Aleksander Kostuch
Inżynier wsparcia sprzedaży
Aleksander.Kostuch@Stormshield.eu

Hakerzy okradli Jabłonna. Władze SZPZOZ o zaszyfrowaniu bazy danych pacjentów

I.O., pszl | publikacja: 10.06.2015 | aktualizacja

📅 22 Września 2016

💬 Komentarzy: 3

📍 Jabłonna

👤 Redakcja



Prokuratura zaznacza, że namierzenie osz

20 tys. zł przelał za pośrednictwem pracowników Powiatowego Urzędu dziwnego, gdyby nie to, że pieniądze planowano. Urząd padł ofiarą ataku prokuratura.



KRAJOBRAZ BEZPIECZEŃSTWA POLSKIEGO INTERNETU

ISSN 2084-9079

2015

NASK

Raport roczny z działalności CERT Polska

- 08-18 Wyciek danych z serwisu Ashley Madison⁴⁰
- 08-19 Wyciek danych klientów Play⁴¹
- 08-25 Phishing ukierunkowany wykorzystujący dokumenty MS Word – początek działalności fiat126pteam⁴²
- 08-27 Publikacja analizy SmokeLoadera używanego przez fiat126pteam⁴³

- 06-08 Ujawnienie włamania do Plusbanku³¹
- 06-09 Zbigniew Stonoga publikuje akta afery taśmowej³²
- 06-11 Phishing ukierunkowany na polskie instytucje publiczne³³
- 06-12 Doxxing Plusbanku³⁴
- 06-20 Atak na LOT³⁵
- 06-25 Wyciek dokumentów z Citibanku³⁶

- 10-02 Kampania phishingu kierowanego udającego faktury Orange⁵¹
- 10-02 Publikacja analizy GMBota⁵²
- 10-07 Wyciek danych klientów Komputronika i phishing kierowany wykorzystujący te adresy⁵³
- 10-13 Aresztowanie Polsilvera, administratora największego polskiego podziemnego forum⁵⁴
- 11-12 MAiC publikuje opracowaną przez NASK ekspertyzę „System bezpieczeństwa cyberprzestrzeni RP”⁵⁸
- 11-17 Kampania phishingu kierowanego udającego wezwania do zapłaty⁵⁹
- 11-17 Publikacja analizy droppera Dridex⁶⁰
- 11-20 Wyciek danych z Kinoman.tv⁶¹
- 11-30 Atak DDoS na serwery root DNS⁶²
- 11-30 Ujawnienie włamania do systemu pocztowego MON⁶³

PRZEGLĄDARKI TOR

The Onion Router

- **ANONIMIZACJA**

Pierwszy serwer proxy podmienia przy tym adres IP paczki na własny. Na każdym następnym przystanku oznaczenie zmienia się kolejny raz

- **SZYFROWANIE**

Tor wysyła zaszyfrowane zapytania i adresy IP użytkownika do operatora strony. Każdy serwer proxy w łańcuchu rozszyfrowuje dane poprzedniego proxy i szyfruje je ponownie dla następnego.

- **ZASADA PRZYPADKU**

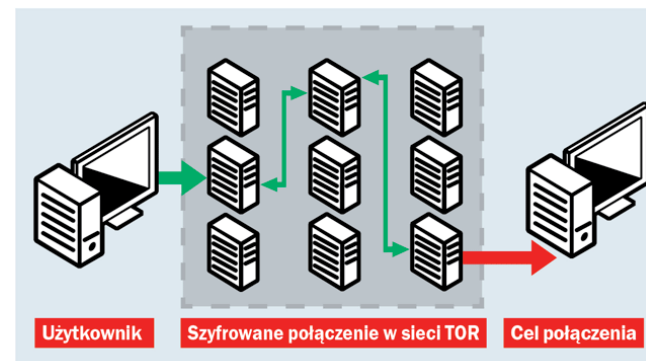
Co dziesięć minut wybierana jest nowa, przypadkowa droga przez sieć serwerów proxy.

- **OTWARTOŚĆ**

trasowanie cebulowe

Open Source

Zacieranie cyfrowych śladów w Internecie



ilustracja: Komputer Świat

DARKNET

- Dysydenci
- Organizacje medialne
- Nielegalne materiały
- Dane dostępne
- Dane kart kredytowych
- Broń

Płatność: Bitkoiny



ilustracja:

<https://www.deepdotweb.com/2015/04/15/so-you-want-to-be-a-darknet-drug-lord/>

Anonimowa droga przekazywania informacji

WYNAJMĘ HAKERA

- włamania na konto społecznościowe,
- hackowanie scammera,
- odzyskiwanie pieniędzy,
- przywrócenie hasła,
- poprawa stopni w elektronicznym dzienniku,
- sprawdzenie bezpieczeństwa strony internetowej.

• TOR

- wykupienie profesjonalnej internetowej aplikacji
- przeprowadzenie własnego ataku z wykorzystaniem ransomware

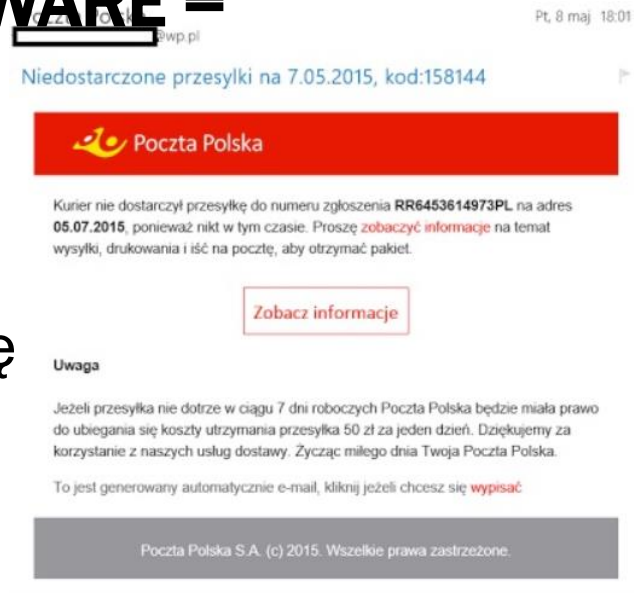


Ilustracja:komputerwfirmie.org

Korzyści są sprawiedliwie dzielone pomiędzy klienta i sprzedawcę usługi:
Malware as a Service

RANSOM (OKUP) + SOFTWARE = RANSOMWARE

- Przestępcy podszywali się pod powiadomienia wysyłane przez Poczta Polską
- Link przekierowywał użytkownika na stronę będący złośliwą aplikacją dla systemu Windows lub Android
- Zabezpieczone hasłem pliki zip oraz dokumenty ze złośliwymi makra pobierającymi i instalującymi złośliwe oprogramowanie.
- Program partnerski internetowych kasyn, reklamowanych w spamowych wiadomościach
- Szyfrowanie danych użytkownika dla okupu



CRYPTOWALL/ CONFICKER / CRYPTOLOCKER/ OPFAKE

- Szyfrowania ważnych dla użytkownika plików
- Prosi o zapłacenie grzywny
- .docx, .pdf, .txt, .img, .gif, .mp3, .mp4, .flv

HELP_YOUR_FILES.TXT
HELP_YOUR_FILES.HTML
HELP_YOUR_FILES.PNG

Cannot you find the files you need?

Is the content of the files that you have watched not readable?

It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!

You have become a part of large community CryptoWall.

[...]

For your attention, the software to decrypt the files (as well as the private key that come fitted with it) is a paid product.



AWARIE BANKOMATÓW

- Sieć Bankomatów, podobnie jak w 2013
- IB, rosyjska grupa zajmująca się cyberbezpieczeństwem, przekazała, że problemy z bankomatami, które wystąpiły w Polsce, Holandii, Wielkiej Brytanii, Armenii, Estonii, Rosji i Hiszpanii
- Wypłaty zlecone przez ludzi były księgowane w bankach, jednak bankomaty pieniędzy nie wydawały
- Konkretnie bankomaty, wybrane przez hakerów, w tym samym momencie wypłacały pieniądze, które wcześniej powinny wydać użytkownikom



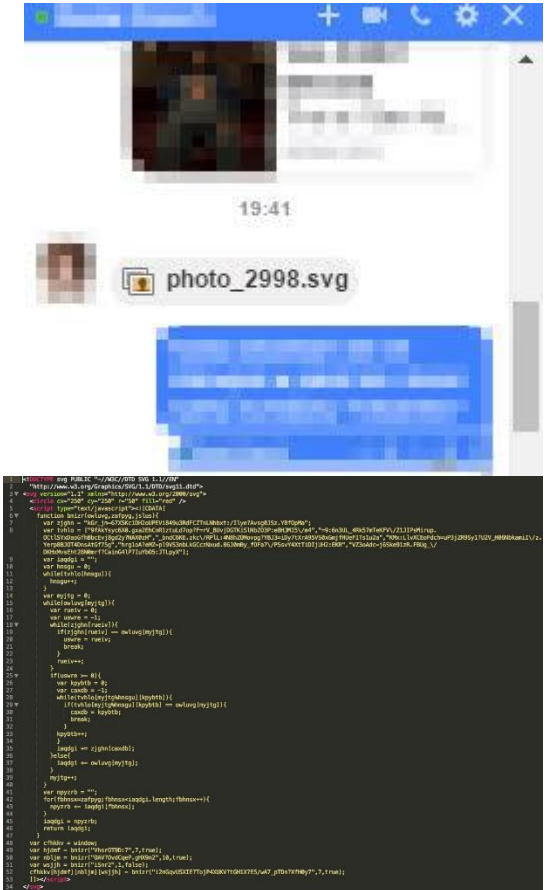
Ilustracja: fotolia (Wprost)

18.11.2016
touchless jackpotting

20.11.2016

SCAM - POPRZEZ CZAT NA FACEBOOKU

- Oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy
- Jest to plik .svg, który po pobraniu i uruchomieniu w przeglądarce ofiary uruchamia następujący skrypt
- Do zobaczenia filmu potrzebny jest odpowiedni “kodek video”
- Dysk twardy jest szyfrowany



ROZWIĄZANIA OCHRONY DLA KAŻDEJ SIECI

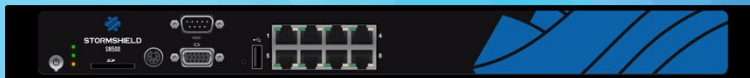
MAŁE ORGANIZACJE, ODDZIAŁY (1-70 UŻYTKOWNIKÓW)



DUŻE SIECI, DATACENTER (700-15 000 UŻYTKOWNIKÓW)



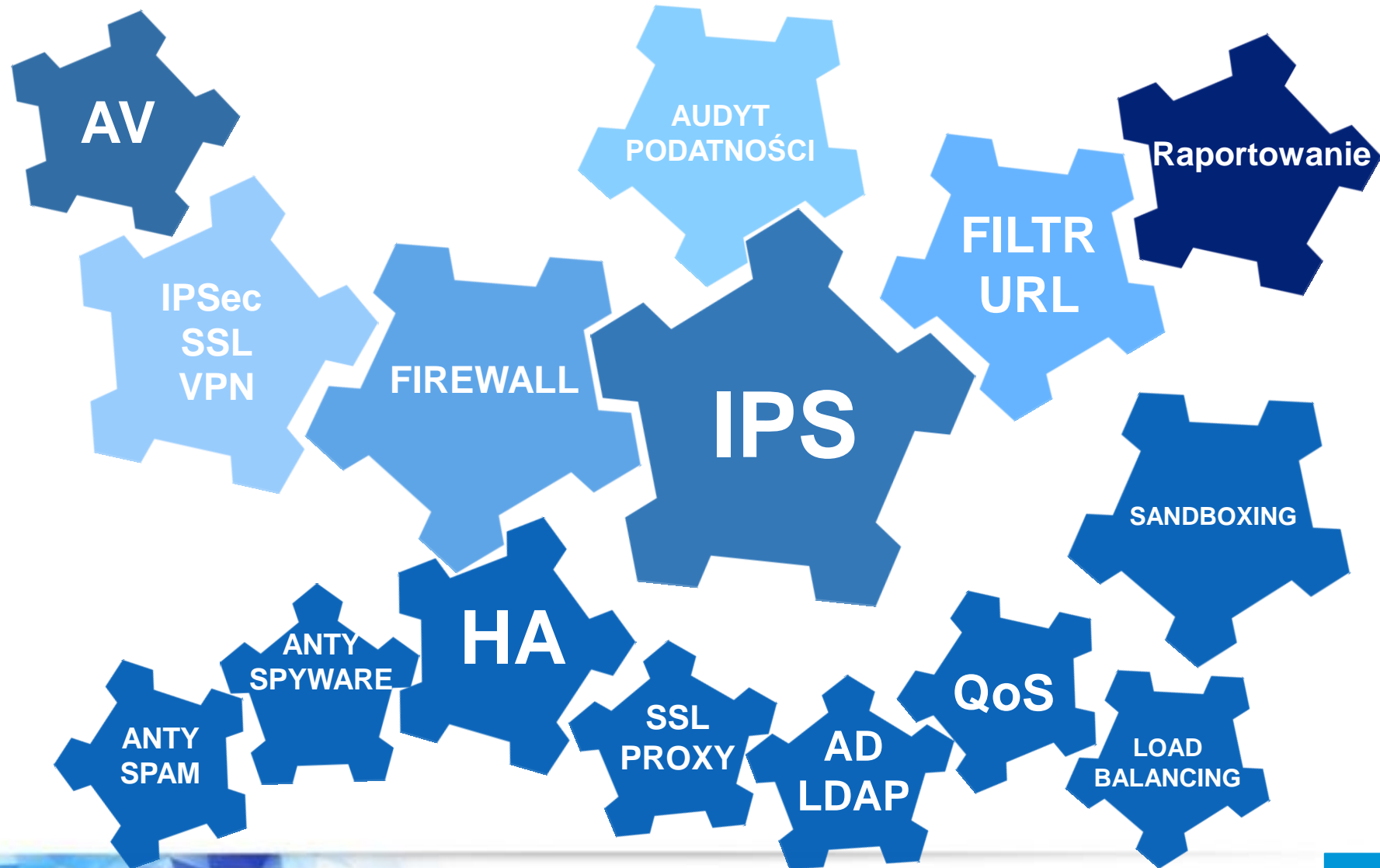
SIECI ŚREDNIEJ WIELKOŚCI (70-700 UŻYTKOWNIKÓW)



WIRTUALNE URZĄDZENIA I UTM W CHMURZE








CO OFERUJEMY - ZABEZPIECZENIA



STORMSHIELD

KIM JESTEŚMY

-  Firma francuska, powstała w 1998, w Polsce od 2007
-  Producent rozwiązań zabezpieczających do sieci
-  Europejskie certyfikaty bezpieczeństwa
-  Kilka tysięcy urzędzeń wdrożonych w Polsce
-  Polski interfejs, dokumentacja i wsparcie

Stormshield

W pełni należy do Airbus Defence and Space Cybersecurity



AIRBUS
DEFENCE & SPACE

AIRBUS
GROUP



WYBRANE REFERENCJE W POLSCE



Śląskie.
Pozytywna energia



SZPITAL POWIATOWY
w Limanowej
Imienia Miłosierdzia Bożego



URZĄD PATENTOWY
RZECZYPOSPOLITEJ POLSKIEJ

fadom
siła w precyzji



POWIAT
ZGORZELECKI
możliwości bez granic



Regionalny Zarząd
Gospodarki Wodnej
we Wrocławiu

Dbamy o przyszłość naszych wód



POWIATOWY
URZĄD PRACY
DLA POWIATU NOWOSADECKIEGO



Łomża



SĄD OKRĘGOWY w LEGNICY



WYBRANE REFERENCJE W POLSCE



CERTYFIKATY



Vendor	Origin *	CC / cert. country	NATO Restricted	French Qualification	EU Restricted
Astaro/Sophos	UK/US	EAL4+	No	No	No
Check Point	Israel	EAL4+	Yes	No	No
Cisco (ASA)	USA	EAL4+	Yes	No	No
Cyberoam/Sophos	UK/US	EAL4+	No	No	No
Fortinet	USA	EAL4+	No	No	No
Genua	Germany	EAL4+	Only unclassified level	No	No
Juniper	USA	EAL4+	Yes	No	No
Netgear	USA	No	No	No	No
Palo Alto	USA	EAL4+	Yes	No	No
Stonesoft/McAfee	USA	EAL4+	No	Elementary	No
Sonicwall/Dell	USA	EAL4	No	No	No
Watchguard	USA	EAL4+	No (except borderware)	No	No
Stormshield/Airbus DS	FR/GE	EAL4+	Yes	Standard	Yes

* Origin of the group if the company is a subsidiary.

Strongly dependent on US interests



POLSKI INTERFEJS UŻYTKOWNIKA

STORMSHIELD SN500 SN500A14H0215A7 2.3.2 demo
Uprawnienia: modyfikacja/zapis...

Wyślij | Pobierz pakiet Administracyjny

INTERFEJSY

Szukaj... + Dodaj Usuń | Widok mieszany | Filtr: brak | Sprawdź

ULUBIONE
MODUŁY

- PANEL KONTROLNY
- USTAWIENIA SYSTEMOWE
- KONFIGURACJA SIECI
- Interfejsy**
- Interfejsy wirtualne
- Routing
- Routing multicast
- Dynamiczny DNS
- Serwer DHCP
- Proxy DNS
- OBIEKTY
- UŻYTKOWNICY
- POLITYKI OCHRONY
- Firewall i NAT
- Filtrowanie URL
- OBIEKTY
- UŻYTKOWNICY I GRUPY

bridge

- in
- dmz1
- dmz2**
- dmz3
- dmz5
- out
- dmz4
- WAN

OGÓLNE ZAAWANSOWANE

Nazwa : dmz2
Opis :
Identyfikator (numer portu) : dmz2(4)
VLANy zdefiniowane na interfejsie :
Kolor :
Typ interfejsu : wewnętrzny (LAN, DMZ)

Konfiguracja sieciowa interfejsu

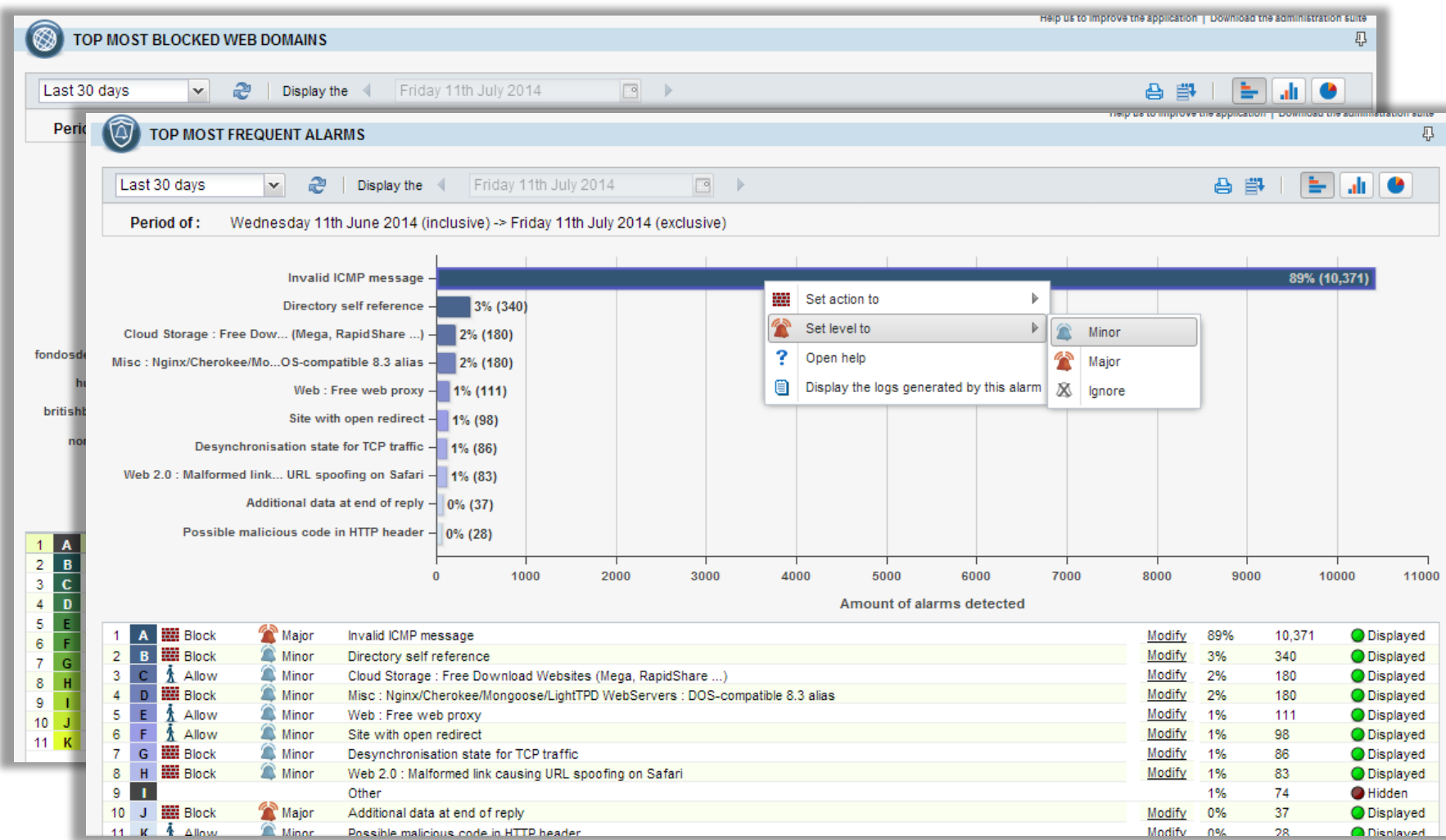
Wyłącz interfejs
 Pobierz adres z DHCP
 Interfejs należy do bridge
bridge
 Konfiguracja statyczna

+ Dodaj - Usuń

Adres	Maska	Opis
-------	-------	------

Zastosuj Anuluj

BEZPŁATNE RAPORTOWANIE



AUDYT PODATNOŚCI



BRAK WPŁYWU NA WYDAJNOŚĆ SIECI

WYSZUKIWANIE SŁABYCH PUNKTÓW
STANOWIĄCYCH ZAGROŻENIA

SUGEROWANIE SPOSOBU ROZWIĄZANIA
WYKRYTYCH PODATNOŚCI

WYKRYWANIE NIEDOZWOLONEGO RUCHU

ANALIZA RYZYKA

TOP CLIENT VULNERABILITIES

[help us to improve the application](#) | [Download the administration suite](#)

Last 30 days
Display the

Friday 11th July 2014

Period of:

Monday 14th June 2014 (Friday) - Friday 14th July 2014 (Friday)

[help us to improve the application](#) | [Download the administration suite](#)

VULNERABILITIES

[help us to improve the application](#) | [Download the administration suite](#)

Customized time range
Refresh
Line view
Collapse elements

(New filter)

Save
Delete
Simple search
Reset columns

FILTER

any contains Mozilla Products Code Execution and Security Bypass Vulnerabilities

+ Add a criterion

SEARCH FROM - 06/11/2014 12:00:00 AM - TO - 07/11/2014 12:00:59 AM

Saved at	Date and time	Time ...	Source Na...	Source	Severity	Message	Exploit	Solution
06/25/2014 01:00:04 PM	06/25/2014 01:00:04 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 01:00:04 PM	06/25/2014 01:00:04 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 01:00:04 PM	06/25/2014 01:00:04 PM	+0200				Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 01:00:04 PM	06/25/2014 01:00:04 PM	+0200				Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 01:00:04 PM	06/25/2014 01:00:04 PM	+0200				Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:47 PM	06/25/2014 12:58:47 PM	+0200				Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:47 PM	06/25/2014 12:58:47 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:47 PM	06/25/2014 12:58:47 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:44 PM	06/25/2014 12:58:44 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:44 PM	06/25/2014 12:58:44 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:44 PM	06/25/2014 12:58:44 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:44 PM	06/25/2014 12:58:44 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:44 PM	06/25/2014 12:58:44 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:44 PM	06/25/2014 12:58:44 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution
06/25/2014 12:58:44 PM	06/25/2014 12:58:44 PM	+0200	dasda2	192.168.1.2	Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	Remote	Solution

1	A	Other
2	B	Mozill
3	C	Mozill
4	D	Mozill
5	E	Mozill
6	F	Mozill
7	G	Mozill
8	H	Mozill
9	I	Mozill
10	J	Mozill
11	K	Mozill

+ Add the host to the Object base

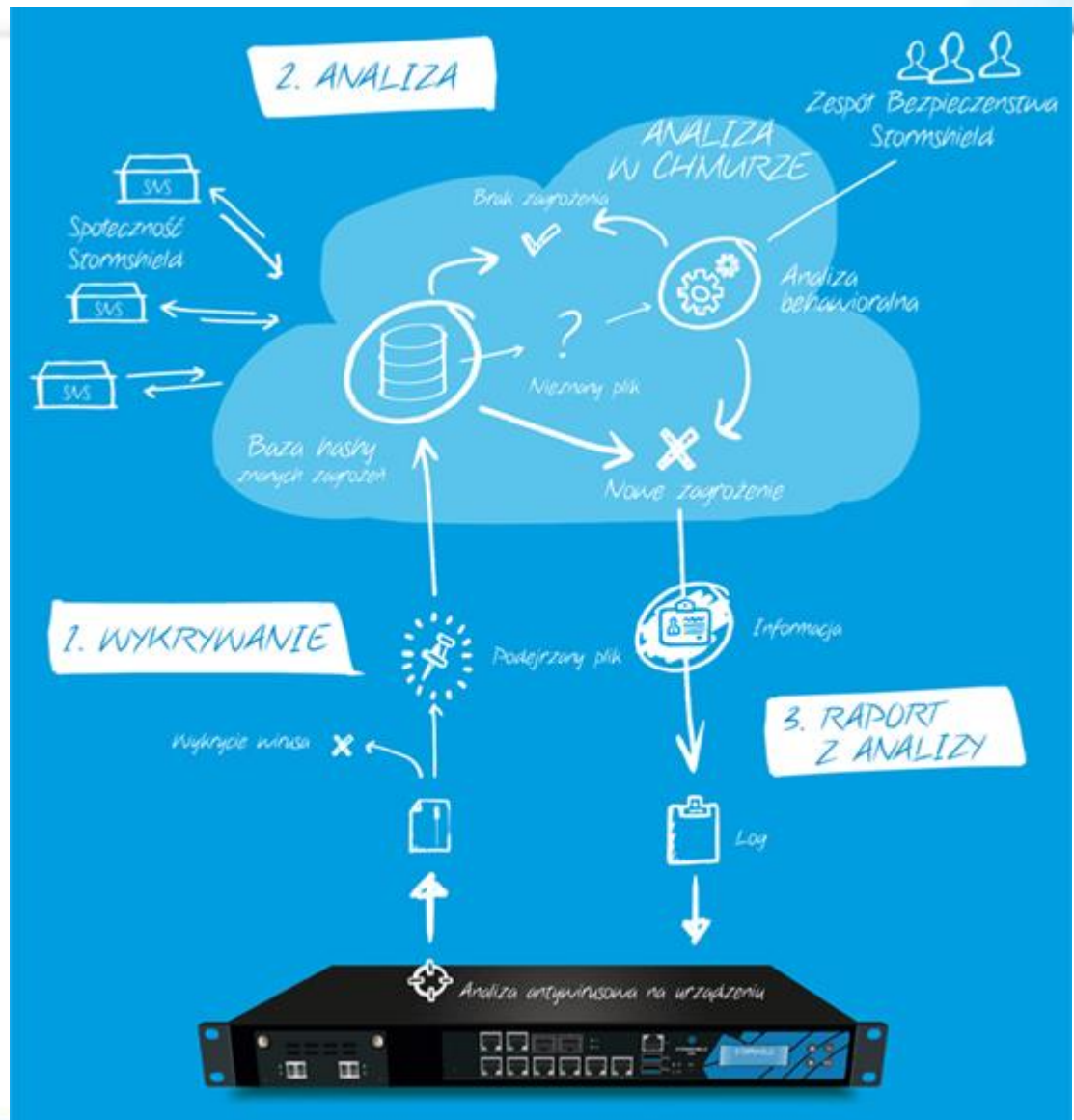
+ Add an equality criterion to this value

+ Add a difference criterion to this value

+ See the entire line

STORMSHIELD

21



KONFIGURACJA

PROTOCOLS

sandboxing

- HTTP
- SMTP
- POP3

(1) http_01 | Edit | Go to global configuration

IPS PROXY ICAP ANALYZING FILES **SANDBOXING ANALYSIS**

Sandboxing

State	File type	Max. size of the analyzed files (KB)
-------	-----------	--------------------------------------






pass	Pc-JO via SSL proxy	Internet	pop3s smtps	IPS Antivirus Sandboxing
pass	Network_bridge via SSL proxy	Internet	ssl_srv	IPS Antivirus Sandboxing URL filter: URLFilter_00

Application inspection

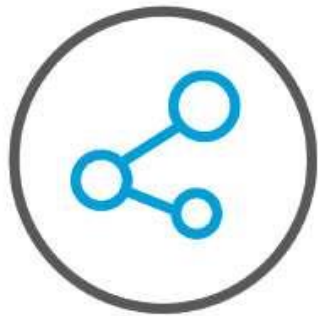
Antivirus ? : On

Sandboxing ? : On

CO OFERUJEMY:

-  Najszybszy IPS z firewall'em na rynku
-  Polskie: interfejs użytkownika, wsparcie techniczne i dokumentacja
-  2 moduły raportujące oraz filtr www w cenie serwisu podstawowego
-  Po wygaśnięciu licencji moduły nadal działają
-  Bezagentowy skaner podatności w sieci

PRODUKTY DO OCHRONY



Network
Security



Endpoint
Security



Data
Security

ZAPRASZAMY DO KONTAKTU

ALEKSANDER.KOSTUCH@STORMSHIELD.EU