Zabezpiecz swoje dane przed mailami phishingowymi na temat koronawirusa i atakami typu zero-day

Damian Przygodzki
Sophos System Engineer

SOPHOS

Co wiemy i jak się dowiadujemy?

SOPHOS

Co wiemy i jak się dowiadujemy?

- https://www.worldometers.info/coronavirus/

Coronavirus Cases:

111,401

view by country

Deaths:

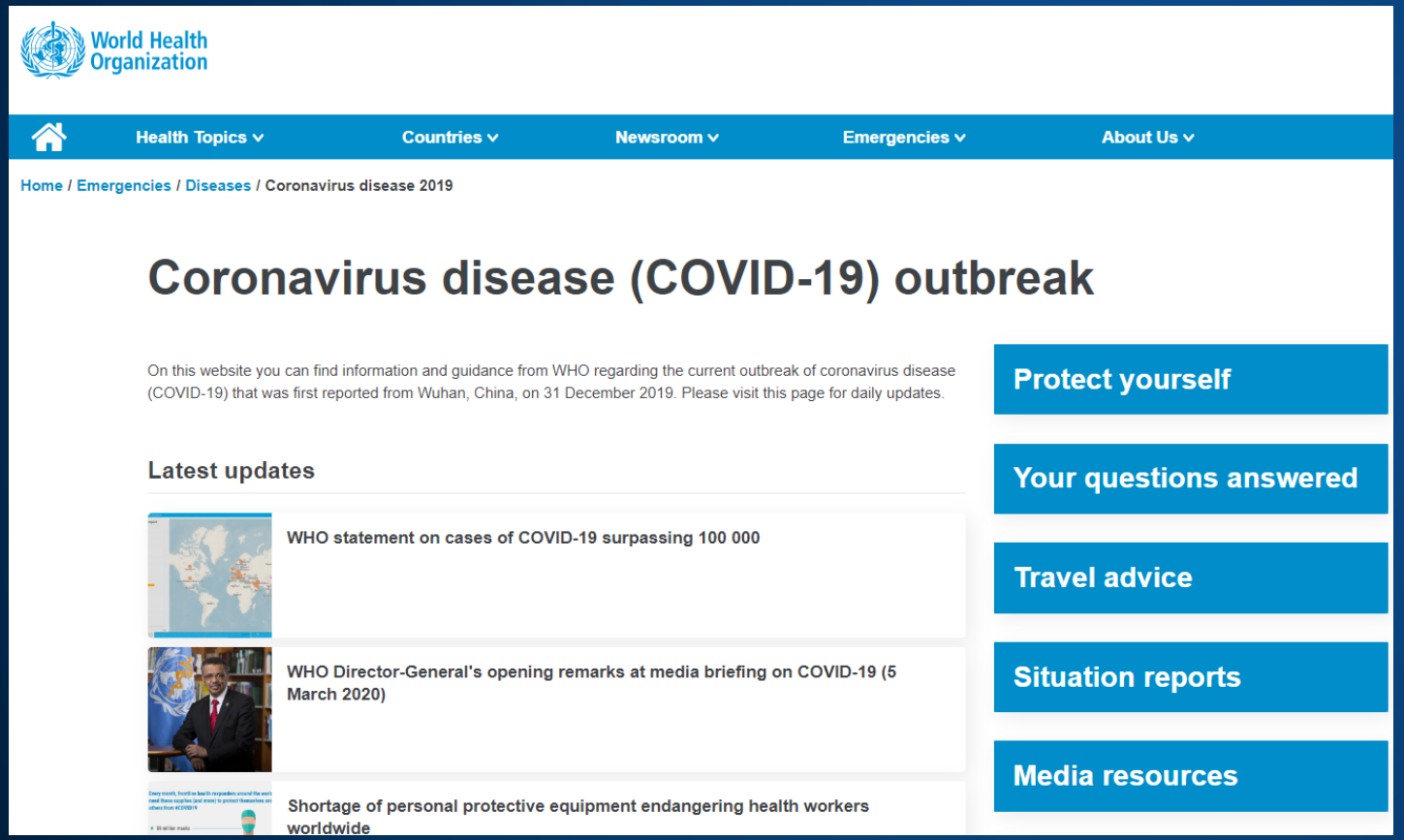
3,882

Recovered:

62,671

Co wiemy i jak się dowiadujemy?

- https://www.who.int/emergencies/diseases/novel-coronavirus-2019



Na co musimy uważać?

SOPHOS

Na co musimy uważać?

ZDNet

PAIN MORE

UN News | Global perspective Human stories

Search

Advanced Search

HOME | TOPICS | IN DEPTH | SECRETARY-GENERAL | MEDIA

Africa | Americas | Asia Pacific | Middle East | Europe | History Corner | UN Art and Gifts

AUDIO HUB | SUBSCRIBE

UN health agency warns against coronavirus COVID-19 criminal scams

etails.

Usługi spamerskie - jaki jest koszt

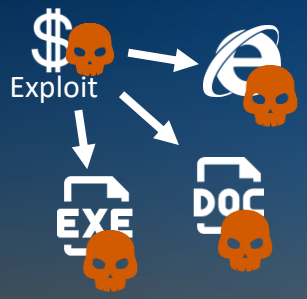
- Spam e-mail jest podstawym wektorem lub metodą dystrybucji wykorzystywaną przez atakujących w celu rozprzestrzeniania wszystkich form złośliwego oprogramowania od Trojanów po Ransomware

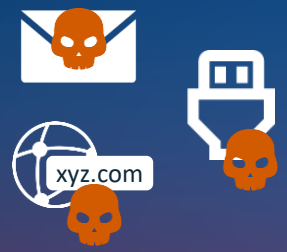
Service	Actor A	Actor B	Actor C	Actor D	Actor E
Pricing	$200/20 million US only $150/25 million—DE, FR, IT, UK and US $75/5 million—RU	SMTP servers $8-10	Sends html page emails Sends attachments Sends spoofed email address from any address Email lists provided $25	Standard: 100 bots $1000/mo. Pro Package: 500 bots $1400/mo. Additional bots: 100—$330 500—$750 1000—$1000	Price: • minimum order $40 for 50k sent • $70 per 100k • more than 100k is considered individually
Average monthly cost	$14	$9	$25	$1200	$500
Note - monthly costs for Actor A based on per million emails					

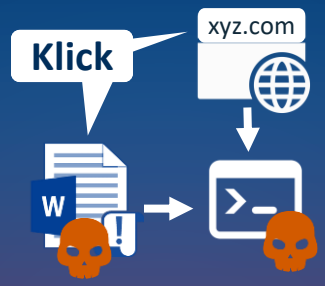
Jak zabezpieczyć organizacje?

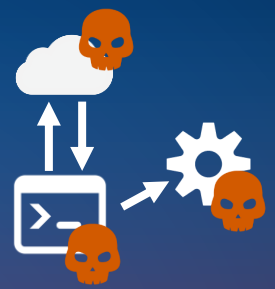
SOPHOS

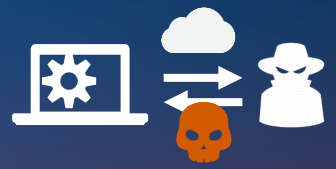
Cykl życia zagrożenia - jak przerwać łańcuch

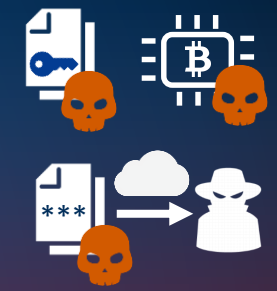












Rozpoznanie

Zbieranie:
- Adresy e-mail
- Nazwy
- Publiczne adresy IP
- Dostępne usługi
- Używane AV

Uzbrojenie

Połączenie exploita z backdoorem do dostarczanej zawartości:
- Dokumenty
- Treść stron internetowych
- Pliki wykonywalne

Dostawa

Dostawa uzbrojonej paczki:
- E-mail
- Strona internetowa

Wykorzystanie Exploita

Wykorzystanie podatności lub funkcji by wykonać kod exploita:
- Makra w pakiecie Office
- Aktywne treści na stronach internetowych
- PowerShell

Instalacja

Instalacja / pobieranie złośliwego oprogramowania

Serwer Command & Control

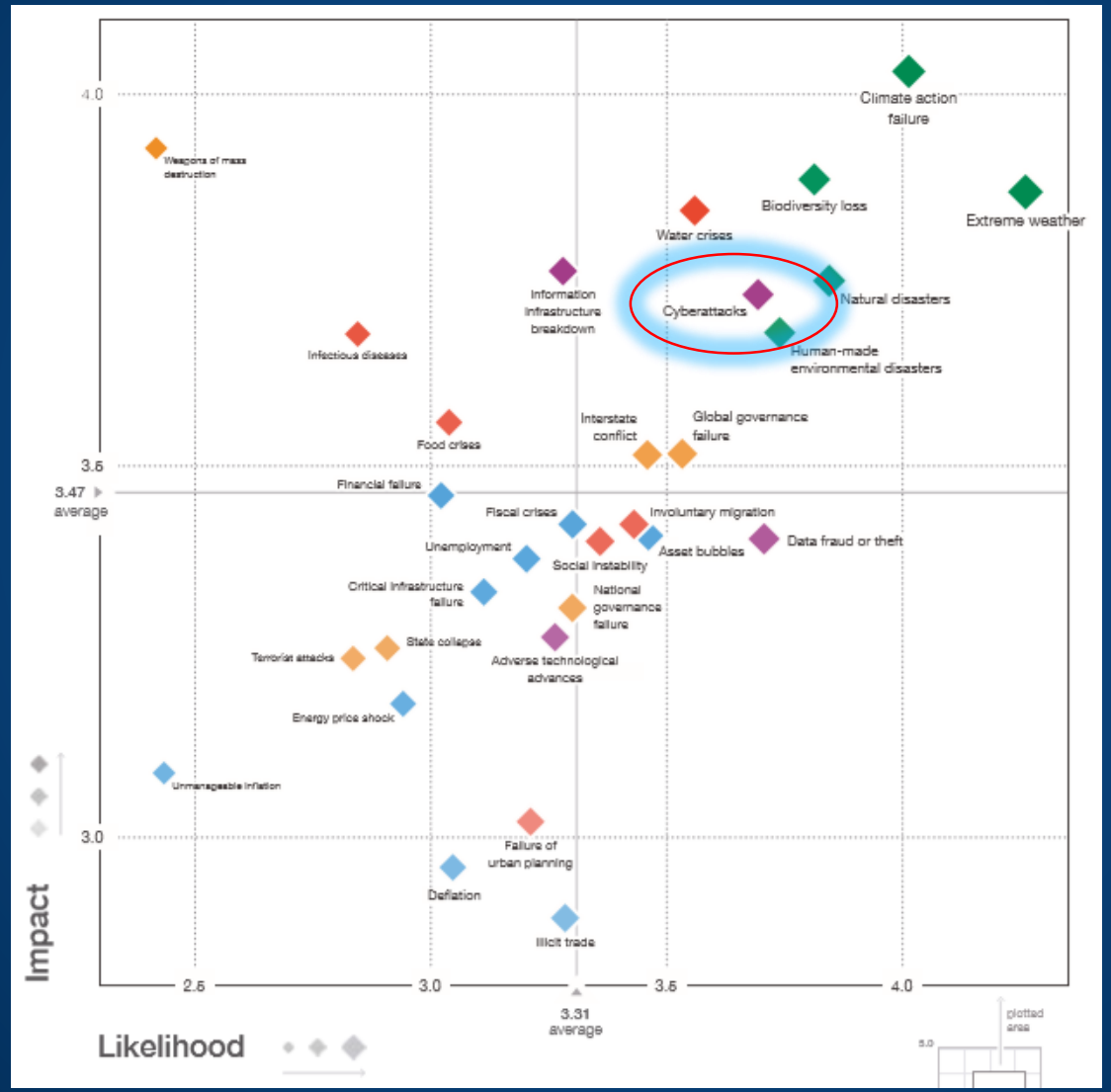
Przesyła polecenia do zdalnej manipulacji:
- Polecenia
- Dane
- Klucze
- Oprogramowanie / Payload

Działanie i ukierunkowany atak

Dzięki dostępowi „do klawiatury” intruzi osiągają swój cel:
- Ransomware
- Cryptojacking
- Kradzież danych
- Trojany bankowe
- itp

SOPHOS

Dlaczego tak ważne jest zerwanie łańcucha?



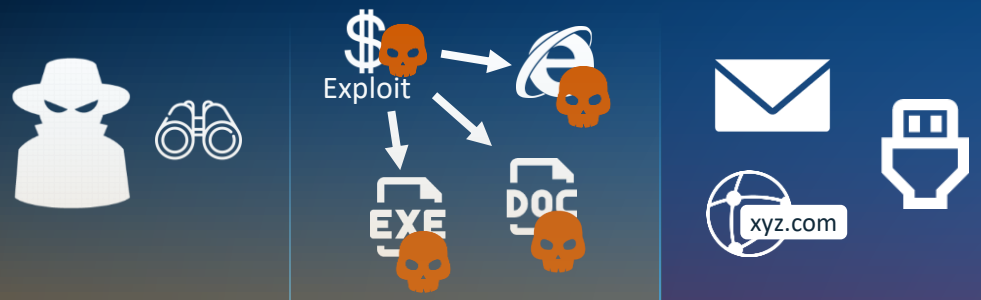
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The Global Risks Report 2020
15th Edition

SOPHOS

Cykl życia zagrożenia - jak zerwać łańcuch



Rozpoznanie → **Uzbrojenie** → **Dostawa**

ŚWIADOMOŚĆ UŻYTKOWNIKÓW

OCHRONA POCZTY

FIREWALL

SOPHOS

Świadomość Użytkowników

SOPHOS

Dlaczego świadomość użytkowników jest ważna?

https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes

Sophos Phish Threat

Centralne zarządzanie użytkownikami
Włącznie ze wspólną listą użytkowników z Sophos Central i synchronizacją AD

Międzynarodowe centra danych
Dostępność w USA, a teraz w Irlandii i we Frankfurcie w regionach AWS

Obsługa wielu języków
Interfejs użytkownika, szablony wiadomości e-mail i szkolenia przetłumaczone na dziewięć języków

Ulepszone Kampanie
Usprawniony kreator tworzenia kampanii i ulepszona infrastruktura SMTP

Pulpit i Analityka
Krótkie podsumowanie kampanii i wszystkie nowe „czynniki świadomości”, aby zrozumieć ogólną postawę

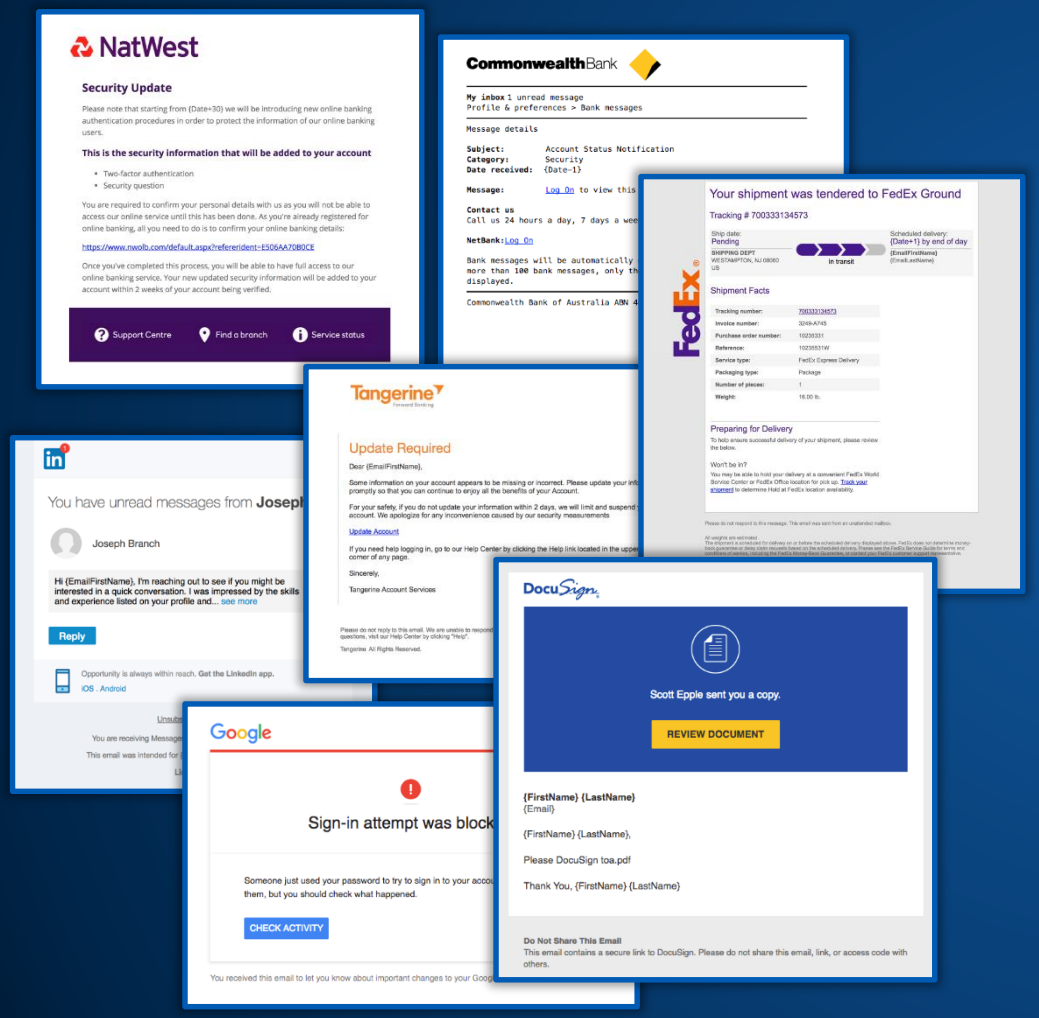
Phish Threat Campaigns

Personalizowana treść i marka

	Attack Email	*Caught Email*	*Training Enrollment Email*	*Attack Landing Page*	*Reminder Email*	*Caught User Landing Page*	*Training Landing Page*
 **KAMPANIE Z LINKAMI TYPU PHISHING** Zwab pracownika, aby kliknął link w wiadomości e-mail	✓				✓	✓	✓
 **KAMPANIE ZBIERANIA POŚWIADCZEŃ** Namów do wprowadzenia danych logowania online	✓			✓	✓	✓	✓
 **KAMPANIE Z ZAŁĄCZNIKIEM** Symuluj atak obejmujący złośliwy załącznik pakietu Office	✓	✓			✓	✓	✓
 **KAMPANIE SZKOLENIOWE** Wygeneruj bezpośrednie zaproszenie na szkolenie bez symulacji			✓		✓		✓

SOPHOS

100 dostosowywanych szablonów ataków



Wiele scenariuszy

- Dostępnych 9 języków
- Realistyczne symulacje
- Biblioteka szablonów od początkującego do eksperta

Rosnąca biblioteka treści

- Plain text business updates
- Australian Federal Police
- Amazon
- DVLA
- Canada Post
- New Zealand Inland Revenue Department
- Parcelforce
- Apple

Ponad 60 modułów szkolenia pracowników

Tamty o bezpieczeństwie

- Wyłudzanie informacji
- Zbiór poświadczeń
- Vishing (phishing telefoniczny)
- Inżynieria społeczna
- Ransomware
- Bezpieczne korzystanie z mediów społecznościowych
- Publiczne Wi-Fi
- Złośliwe załączniki
- Hasła
- Uwierzytelnianie dwuskładnikowe
- Zasada najmniejszych uprawnień
- Bezpieczeństwo fizyczne i ochrona danych

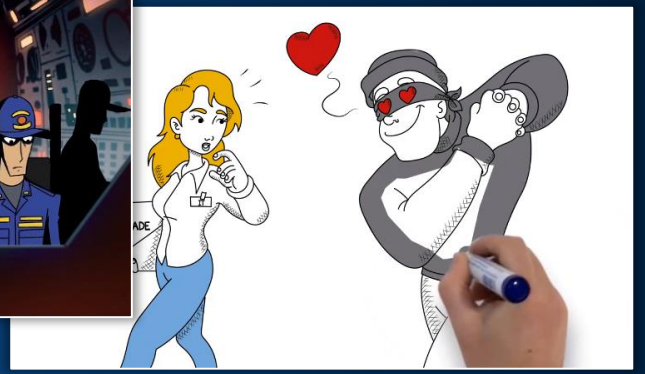
Tematy Zgodności

- Ogólne rozporządzenie UE w sprawie ochrony danych (RODO)
- Ustawa Gramm-Leach-Bliley (GLBA)
- Ustawa o przenośności i rozliczalności ubezpieczeń zdrowotnych (HIPAA)
- Karta płatnicza Standard bezpieczeństwa danych branżowych (PCI DSS)

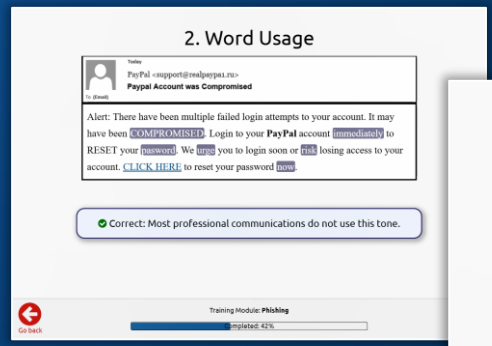
Sprawdzenie wiedzy

- Interaktywny quiz po każdym kursie
- Pełne raportowanie ukończenia kursu

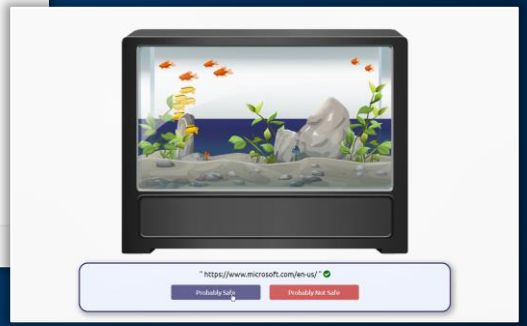
Różne style wideo



Interaktywne moduły



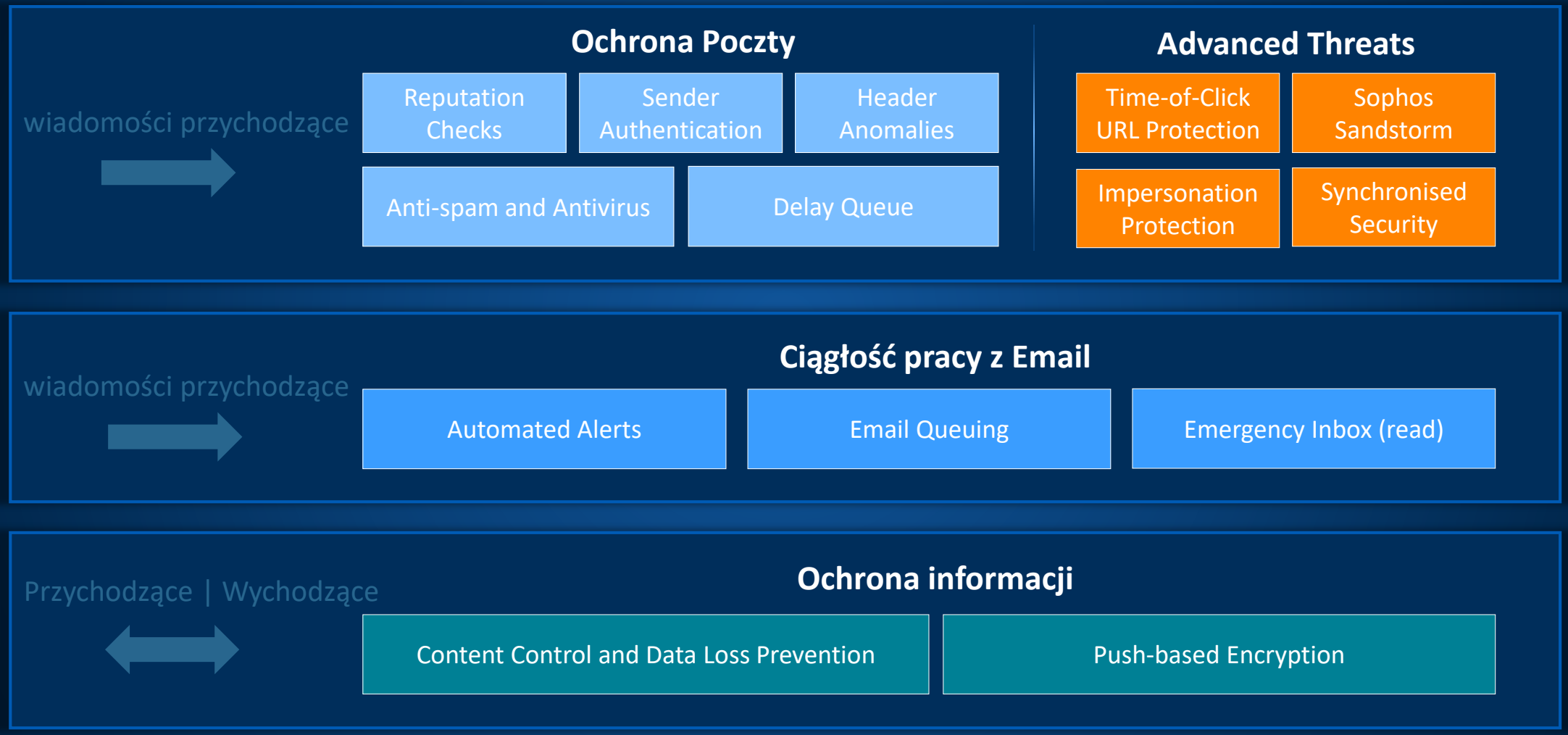
Gamifikacja



Ochrona Poczty

SOPHOS

Sophos Email - ochrona w jednym



Zatrzymywanie zaawansowanych zagrożeń

Ulepszone wykrywanie zachowania + głębokie uczenie (Deep Learning)

Ransomware
Zatrzymany

10% więcej
Zatrzymanych EXE Malware

Przesyłanie Pliku

- Wykryj podejrzane pliki
- Wybierz środowisko wykonywania

Odtwarzanie Ataku

- Rejestrowanie zdarzeń
- Ekstrakcja Payload
- Zapobieganie oszustwom

Analiza Zachowania

- CryptoGuard i WipeGuard
- Zasady i wzory
- Korelacje zdarzeń

Analiza Deep Learning

- Wykryj nieznane zagrożenia wykonywalne
- Ciągly adaptacyjny model uczenia się

Sophos Sandstorm

Microsoft Office 365 Direct Access

Sophos Email
Office 365
Direct Access

Licencjonowanie Sophos Email

Sophos Email

- Cloud-based
- Licencjonowanie per-użytkownik
- Inclusive feature set

Sophos Central

- Jedna konsola zarządzająca
- Synchronized Security

Email Security License Features		Sophos Email Advanced Email security and ATP for cloud or on-premises
Mail Handling	Inbound / Outbound Message Scanning	✔
	Domain, Group and User Level Policies	✔
	Admin and User Quarantine	✔
	24/7 Emergency Inbox	✔
Spam, phishing and antivirus	Anti-Spam Filters	✔
	Antivirus Filters	✔
	Message Header Anomaly Checks	✔
	Inbound SPF, DKIM and DMARC	✔
	Delay Queue	✔
Information Protection	Push-based Encryption	✔
	Enforced TLS encryption	✔
	Data Loss Prevention	✔
	Content Control and DLP	✔
Active Threat Protection (ATP)	Sophos Sandstorm	✔
	Time-of-Click URL Protection	✔

Ochrona Firewall

SOPHOS

XG Firewall

Najlepsza widoczność, ochrona i reakcja

SOPHOS
XG 750 Firewall SFOS v17.5
NEXT GENERATION FIREWALL
NSS LABS
RECOMMENDED
JULY 2019

1. Eksponuje ukryte ryzyka

- ✓ Dashboard i bogate raporty on-box
- ✓ Zidentyfikuj ryzykownych użytkowników i podejrzane pli
- ✓ Zidentyfikuj nieznane aplikacje chmurowe i sieciowe
- ✓ Doskonała identyfikacja aplikacji i kontrola SSL

2. Zatrzymuje nieznane zagrożenia

- ✓ Pełny pakiet ochrony - łatwy w zarządzaniu
- ✓ Deep Learning AI Ochrona przed Zero-Day
- ✓ Najskuteczniejszy silnik IPS (Cisco Talos)
- ✓ Dywersyfikacja AV (Sophos, Avira)
- ✓ Silnik Xstream DPI z TLS 1.3

3. Izoluje zainfekowane systemy

- ✓ Unikalny Security Heartbeat ™
- ✓ Automatycznie izoluj zainfekowane systemy
- ✓ Zatrzymuje naruszenia bezpieczeństwa

Zalety wdrożenia w sieci XG Firewall

Prostota i wydajność

1. Elastyczna możliwość połączenia

- ✓ Zintegrowane funkcje SD-WAN
- ✓ Moduły z portami miedzianymi, światłowodowymi lub LTE
- ✓ Opcja redundancji WAN z monitorowaniem łącza

2. Uproszczona mozliwość zdalnych połączeń

- ✓ SD-RED - niedrogie, proste urządzenia do oddziałów
- ✓ Proste narzędzia do zestawiania VPN
- ✓ Hmurowe zarządzanie

3. Zoptymalizowana wydajność aplikacji

- ✓ Synrchronized App Control w celu identyfikacji 100% aplikacji
- ✓ Xstream FastPath dla zaufanego ruchu
- ✓ Synchronized SD-WAN dla zoptymalizowanego routingu aplikacji

XG Firewall – modele licencjonowania

Features (as listed above)		FullGuard Plus (included in TotalProtect Plus)				
			FullGuard (included in TotalProtect)			
		EnterpriseGuard Plus (included in EnterpriseProtect Plus)				
			EnterpriseGuard (included in EnterpriseProtect)			
	Base Firewall	Sandstorm Protection	Network Protection	Web Protection	Email Protection	Web Server Protection
General Management (incl. HA)	●					
Firewall, Networking and Routing	●					
Base Traffic Shaping and Quotas	●					
Secure Wireless	●					
Authentication	●					
Self-Serve User Portal	●					
Base VPN Options	●					
Sophos Connect IPSec Client	●					
Sandstorm Protection		●				
Intrusion Prevention (IPS)			●			
ATP and Security Heartbeat™			●			
Remote Ethernet Device (RED) VPN			●			
Clientless VPN			●			
Synchronized Application Control				●		
Web Protection and Control				●		
Application Protection and Control				●		
Cloud Application Visibility				●		
Web and App Traffic Shaping				●		
Email Protection and Control					●	
Email Quarantine Management					●	
Email Encryption and DLP					●	
Web Application Firewall Protection						●
Logging and Reporting	●	●	●	●	●	●

Cykl życia zagrożenia - jak przerwać łańcuch

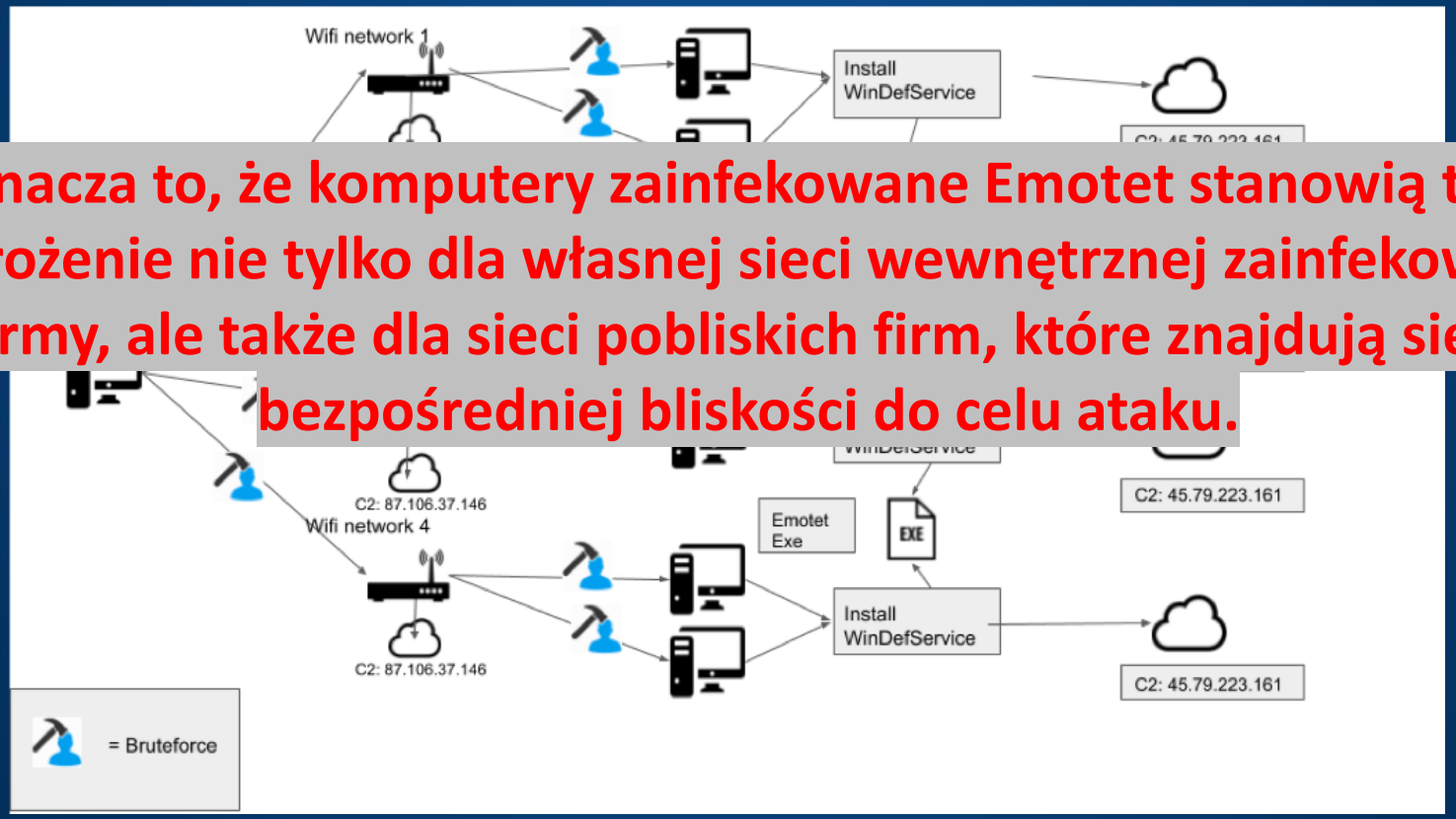
Rekonesans | Uzbrojenie | Dostawa | Wykorzystanie Exploita | Instalacja | Serwer Command & Control | Działanie i ukierunkowany atak

ŚWIADOMOŚĆ UŻYTKOWNIKÓW
OCHRONA POCZTY
FIREWALL

SOPHOS

Na co musimy uważać?

- **Trojan Emotet ewoluuje, rozprzestrzeniać się za pośrednictwem połączeń WiFi**



Oznacza to, że komputery zainfekowane Emotet stanowią teraz zagrożenie nie tylko dla własnej sieci wewnętrznej zainfekowanej firmy, ale także dla sieci pobliskich firm, które znajdują się w bezpośredniej bliskości do celu ataku.

https://www.zdnet.com/article/emotet-trojan-evolves-to-spread-via-a-wifi-connection/

Ochrona punktu końcowego

SOPHOS

Sophos Intercept X

Ochrona punktów końcowych nowej generacji

OCHRONA PRZED NIEZNANYMI ZAGROŻENIAMI

SOPHOS

INTERCEPT X

Niektóre techniki i ataki Exploit zatrzymane przez Intercept X

Enforce data execution prevention	Mandatory address space layout randomization	Bottom-up ASLR	Null page deference	Heap spray allocation	Dynamic heap spray	Stack pivot and stack exec (memory protection)
Stack-based ROP (caller)	Structured exception handling overwrite (SEHOP)	Import address table faltering (IAF)	Load library	Reflective DLL injection	Malicious shellcode	VBScript god mode
WOW64	Syscall	Hollow process	DLL hijacking	Squiblydoo Applocker bypass	APC protection (Double Pulsar / Atom Bombing)	Process privilege escalation
	Credential theft protection	Code cave mitigation	MITB protection (Safe Browsing)	Malicious traffic detection	Meterpreter shell detection	

Sophos Intercept X

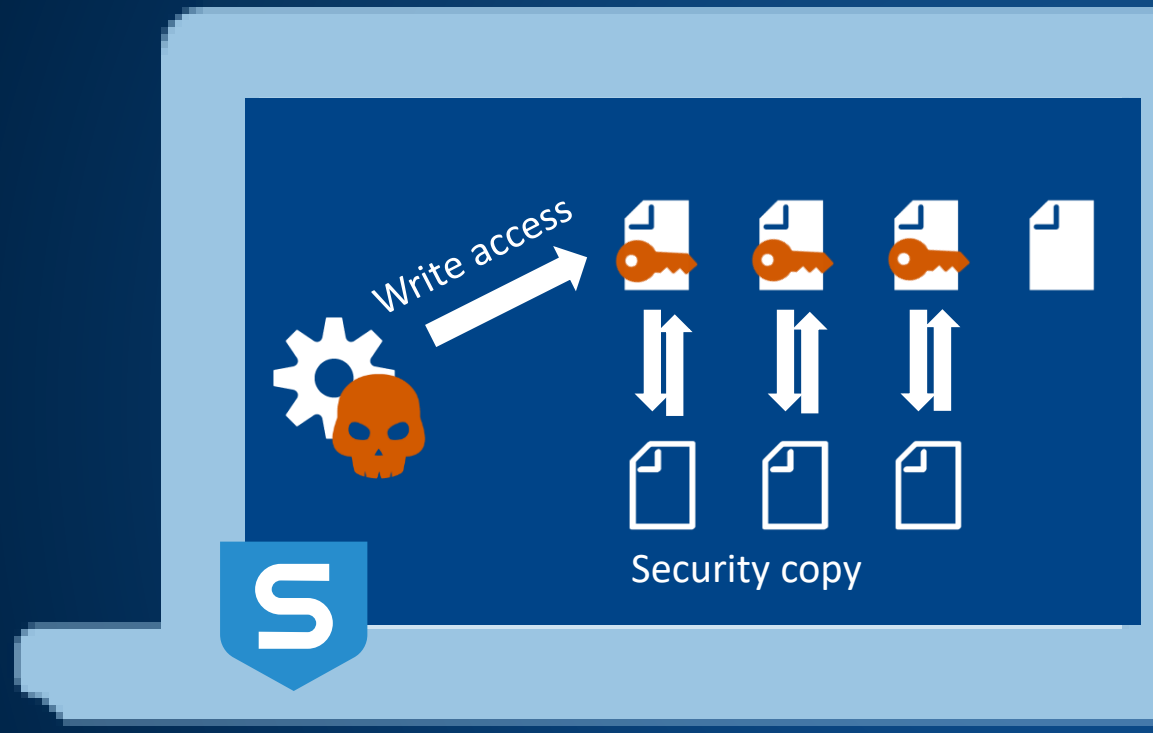
Ochrona punktów końcowych nowej generacji

OCHRONA PRZED NIEZNANYMI ZAGROŻENIAMI

OCHRONA PRZED RANDOMWARE

INTERCEPT X

CryptoGuard – Ochrona przed lokalnym ransomware



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7B	5C	72	74	66	31	5C	61	6E	73	69	5C	61	6E	73	69	{\rtf1\ansi\ansi
00000010	63	70	67	31	32	35	32	5C	64	65	66	66	30	5C	64	65	cpg1252\deff0\de
00000020	66	6C	61	6E	67	31	30	34	33	7B	5C	66	6F	6E	74	74	flang1043{\fontt
00000030	62	6C	7B	5C	66	30	5C	66	6E	69	6C	5C	66	63	68	61	bl{\f0\fnil\fcha
00000040	72	73	65	74	30	20	56	65	72	64	61	6E	61	3B	7D	7D	rset0 Verdana;}}
00000050	5C	72	5C	6E	5C	76	69	65	77	6B	69	6E	64	34	5C	75	\r\n\viewkind4\u
00000060	63	31	5C	70	61	72	64	5C	73	61	32	30	30	5C	73	6C	c1\pard\sa200\sl
00000070	32	37	36	5C	73	6C	6D	75	6C	74	31	5C	6C	61	6E	67	276\slmult1\lang
00000080	39	5C	66	30	5C	66	73	32	32	20	54	68	65	20	71	75	9\f0\fs22 The qu
00000090	69	63	6B	20	62	72	6F	77	6E	20	66	6F	78	20	6A	75	ick brown fox ju
000000A0	6D	70	73	20	6F	76	65	72	20	74	68	65	20	6C	61	7A	mps over the laz
000000B0	79	20	64	6F	67	2E	7D										y dog.}

Plik niezaszyfrowany przed dostępem do zapisu

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7D	EB	10	B2	FD	8E	EB	B9	D1	F6	D8	DE	CC	9B	F6	CB	}ë.²ýŽë¹ÑöØÞÌ›öË
00000010	C4	D9	C3	F6	CB	C4	D9	C3	C9	DA	CD	9B	98	9F	98	F6	ÄÙÃöËÄÙÃÉÚÍ›˜Ÿ˜ö
00000020	CE	CF	CC	CC	9A	F6	CE	CF	CC	C6	CB	C4	CD	9B	9A	9E	ÎÏÌÌšöÎÏÌÆËÄÍ›šž
00000030	99	D1	F6	CC	C5	C4	DE	DE	C8	C6	D1	F6	CC	9A	F6	CC	™ÑöÌÅÄÞÞÈÆÑöÌšöÌ
00000040	C4	C3	C6	F6	CC	C9	C2	CB	D8	D9	CF	DE	9A	8A	FC	CF	ÄÃÆöÌÉÂËØÙÏÞšŠüÏ
00000050	D8	CE	CB	C4	CB	91	D7	D7	F6	D8	F6	C4	F6	DC	C3	CF	ØÎËÄË'××öØöÄöÜÃÏ
00000060	DD	C1	C3	C4	CE	9E	F6	DF	C9	9B	F6	DA	CB	D8	CE	F6	ÝÁÃÄÎžößÉ›öÚËØÎö
00000070	D9	CB	98	9A	9A	F6	D9	C6	98	9D	9C	F6	D9	C6	C7	DF	ÙË˜ššöÙÆ˜.œöÙÆÇß
00000080	C6	DE	9B	F6	C6	CB	C4	CD	93	F6	CC	9A	F6	CC	D9	98	ÆÞ›öÆËÄÍ"öÌšöÌÙ˜
00000090	98	8A	FE	C2	CF	8A	DB	DF	C3	C9	C1	8A	C8	D8	C5	DD	˜ŠþÂÏŠÛßÃÉÁŠÈØÅÝ
000000A0	C4	8A	CC	C5	D2	8A	C0	DF	C7	DA	D9	8A	C5	DC	CF	D8	ÄŠÌÅÒŠÀßÇÚÙŠÅÜÏØ
000000B0	8A	DE	C2	CF	8A	C6	CB	D0	D3	8A	CE	C5	CD	84	D7		ŠÞÂÏŠÆËÐÓŠÎÅÍ„×

Zaszyfrowany plik po zapisie

Analiza przyczyn

Rozszerzone czyszczenie dzięki Sophos Clean

SOPHOS

Sophos Intercept X

Ochrona punktów końcowych nowej generacji

OCHRONA PRZED NIEZNANYMI ZAGROŻENIAMI

OCHRONA PRZED RANDOMWARE

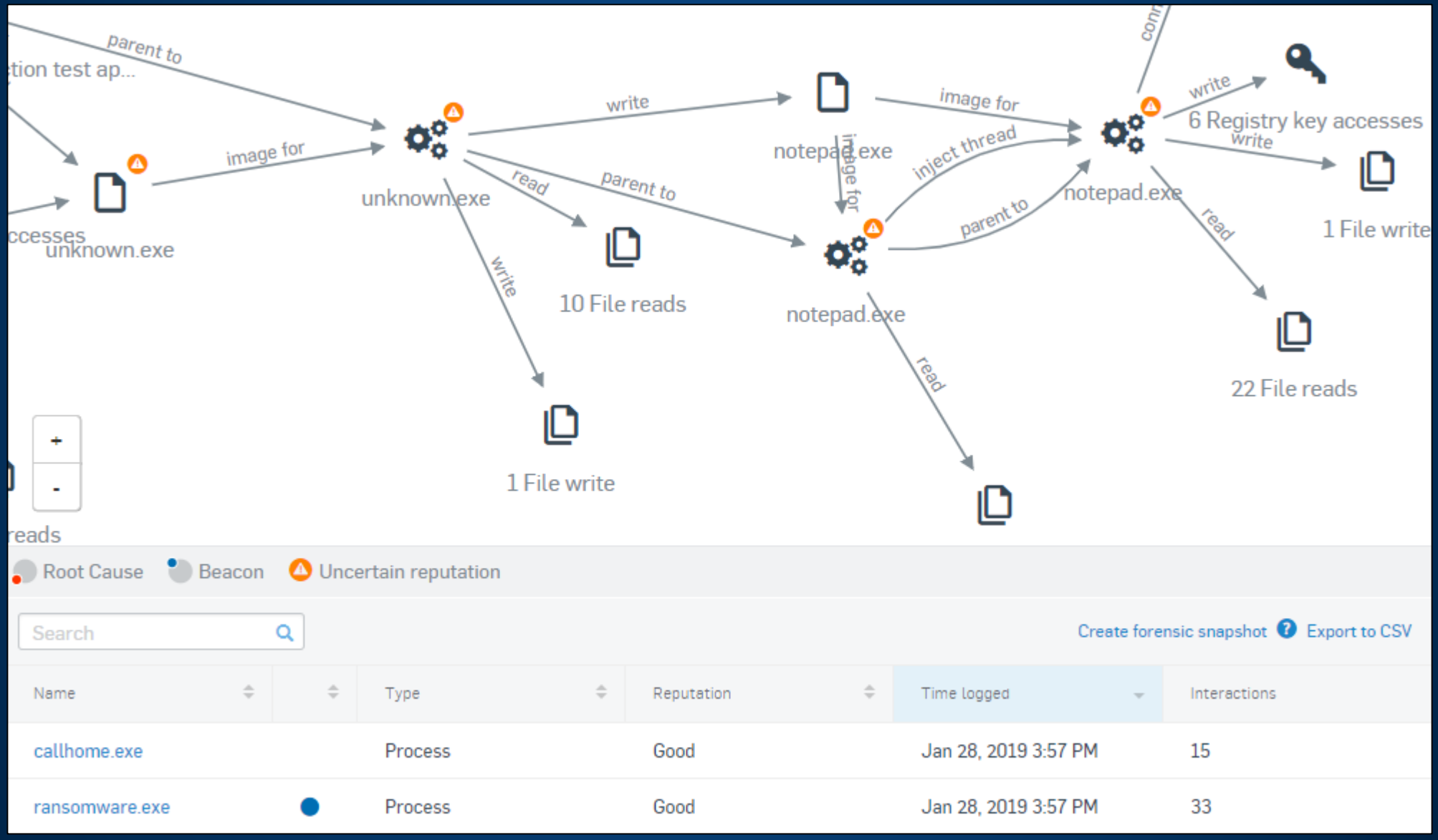
OCHRONA PRZED DZIAŁANIEM HAKERA

ROZSZERZONE CZYSZCZENIE

ANALIZA PRZYCZYNY ATAKU

INTERCEPT X

Analiza przyczyny ataku



Sophos Intercept X

Ochrona punktów końcowych nowej generacji

Oprócz ochrony punktu końcowego

OCHRONA PRZED NIEZNANYMI ZAGROŻENIAMI

OCHRONA PRZED RANDOMWARE

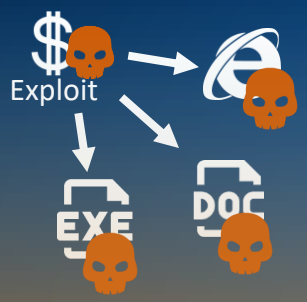
OCHRONA PRZED DZIAŁANIEM HAKERA

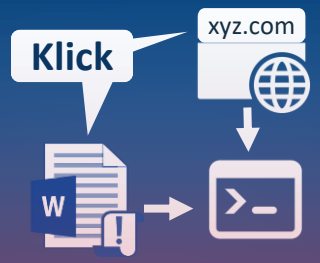
ROZSZERZONE CZYSZCZENIE

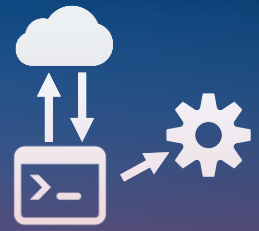
ANALIZA PRZYCZYNY ATAKU

INTERCEPT X

Protection modules in SOPHOS INTERCEPT X







Rekonesans → **Uzbrojenie** → **Dostawa** → **Wykorzystanie Exploita** → **Instalacja** → **Serwer Command & Control** → **Działanie i ukierunkowany atak**

Dostawa
- ŚWIADOMOŚĆ UŻYTKOWNIKÓW
- OCHRONA POCZTY
- FIREWALL

Wykorzystanie Exploita
- OGRANICZENIA KODU / PAMIĘCI / APC
- BLOKADA APLIKACJI
- LOCAL PRIVILEGE MITIGATION
- Kontrola Aplikacji

Instalacja
- MACHINE LEARNING (ML)
- OCHRONA PROCESÓW
- ANTI-VIRUS
- PUA
- HIPS
- WIPEGUARD

Serwer Command & Control
- NETWORK THREAT PROTECTION
- IPS

Działanie i ukierunkowany atak
- ANTI-RANSOMWARE
- CREDENTIAL THEFT PROTECTION
- RUNTIME HIPS
- THREAT CASE (RCA)
- SYNCHRONIZED SECURITY

SOPHOS

Sophos Endpoint Protection (per użytkownik)

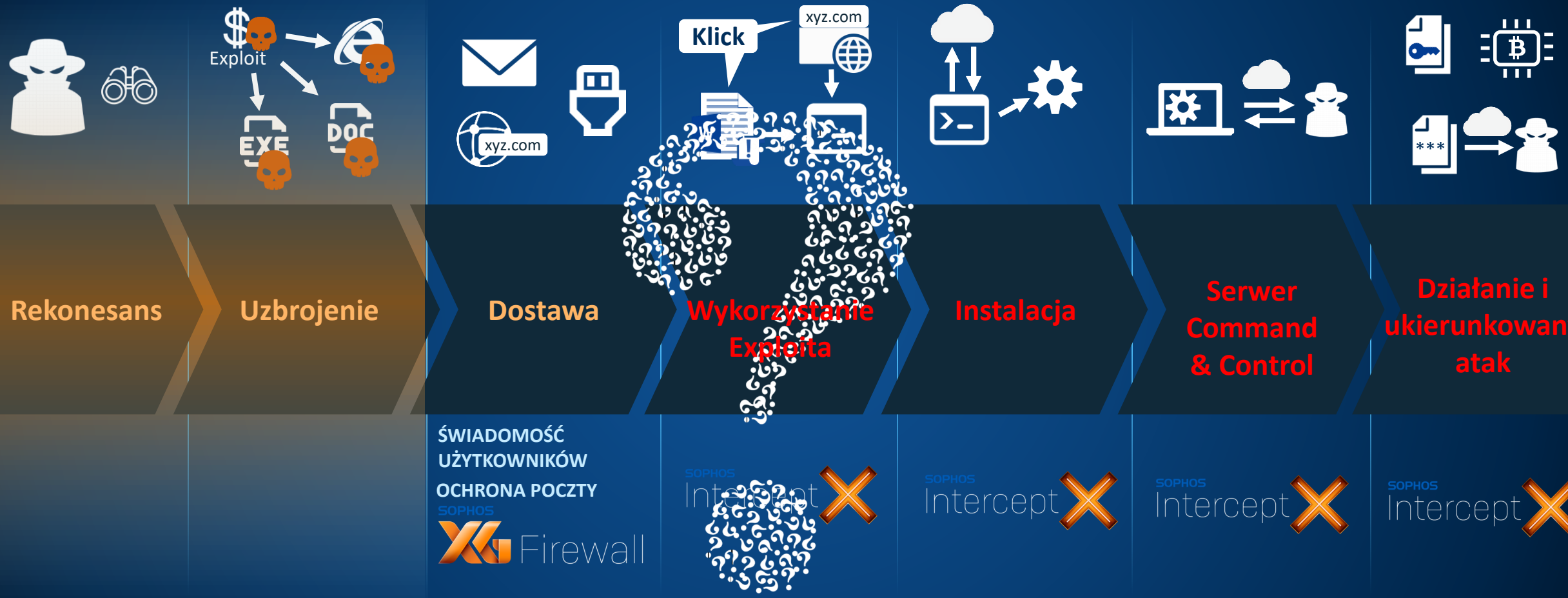
	Central Endpoint Protection	Sophos Intercept X	Sophos Intercept X Advanced	Sophos Intercept X Advanced with EDR
AV Signaturs / HIPS / Live Protection	✓	Competitors-Endpoint Protection	✓	✓
Device / Web / App Control	✓		✓	✓
Data Loss Protection (DLP)	✓		✓	✓
Malicious Traffic Detection (MTD)	✓	✓	✓	✓
Security Heartbeat	✓	✓	✓	✓
Deep Learning		✓	✓	✓
CryptoGuard		✓	✓	✓
WipeGuard		✓	✓	✓
Anti-Hacker-Technolies (CredGuard etc.)		✓	✓	✓
Exploit Protection		✓	✓	✓
Root cause analysis		✓	✓	✓
Automatic / Manual Client-Isolation	✓/-	✓/-	✓/-	✓/✓
Malware-Analysis by SophosLabs				✓
Search & contain threats				✓

SOPHOS

Sophos Server Protection (per serwer)

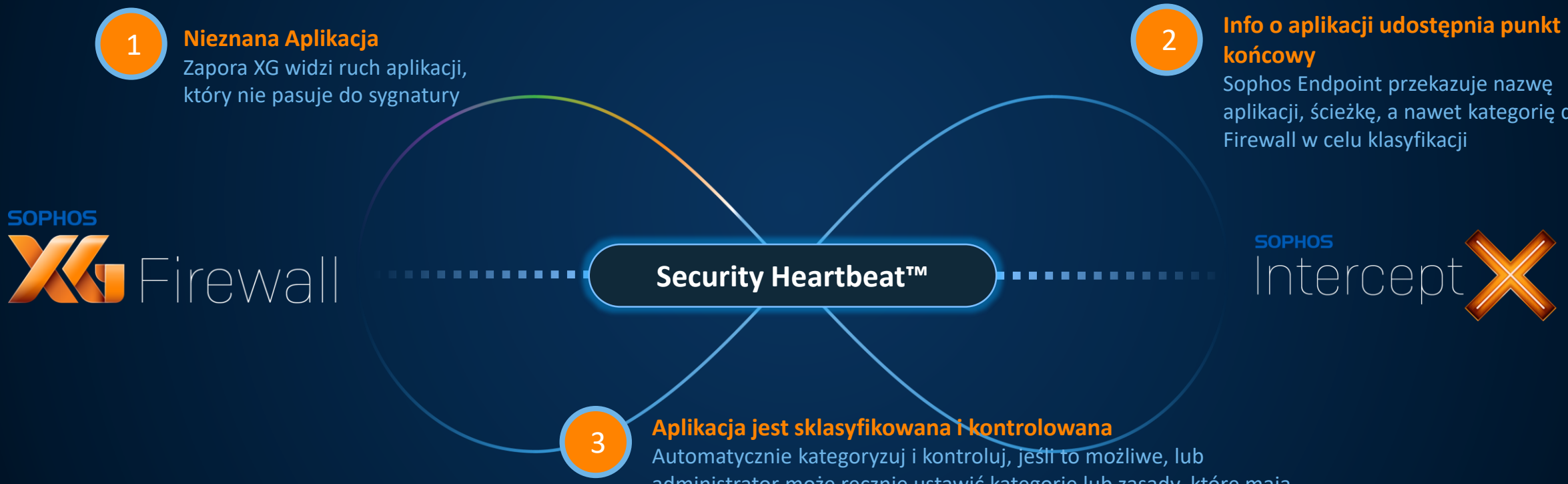
	Central Server Protection	SOPHOS Intercept X For Server	SOPHOS Intercept X For Server with EDR with EDR
AV Signaturs / HIPS / Live Protection	✓	✓	✓
Device / Web / App Control / DLP	✓	✓	✓
Automatic exclusions	✓	✓	✓
Cloud Workload Discovery	✓	✓	✓
Security Heartbeat	✓	✓	✓
Server Lockdown		✓	✓
Deep Learning		✓	✓
Anti-Ransomware (CryptoGuard, WipeGuard)		✓	✓
Anti-Hacker-Technologies (CredGuard etc.)		✓	✓
Exploit Protection		✓	✓
Root cause analysis		✓	✓
Automatic / Manual Client-Isolation	✓/-	✓/-	✓/✓
Malware-Analysis by SophosLabs			✓
Search & contain threats			✓

Cykl życia zagrożenia - jak przerwać łańcuch



Synchronized Application Control

Jak działa...



Sieciowy Autopilot - zautomatyzowana reakcja na zagrożenia

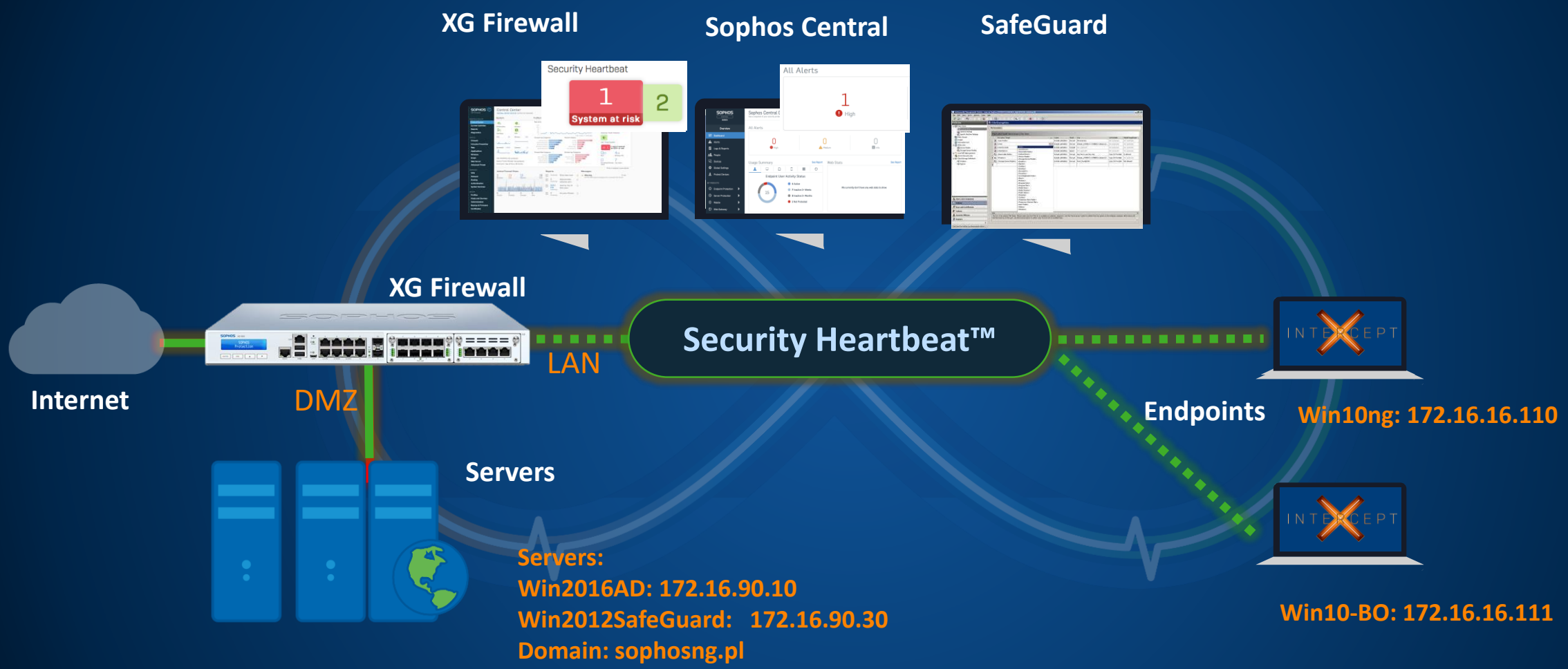
Automatyczne izolowanie zainfekowanych systemów

Unikalne dla Sophos: w pełni zautomatyzowana reakcja na zagrożenia 24/7

Zobaczyć oznacza wierzyć – live demo

SOPHOS

DEMO environment



Jeden, aby rządzić wszystkimi, jeden, aby wszystkie znaleźć

Sophos Central

Endpoint and Server Protection

Intercept X

Mobile Protection

Encryption

Server Protection

Cloud Protection

Cloud Optix

Network Protection

Sophos Wireless

XG Firewall

Email

Phish Threat

Sophos Email

Unikalne dla Sophos: jedno rozwiązanie do zarządzania całym Cyberbezpieczeństwem

SOPHOS

Zmierzając do podsumowania...

SOPHOS

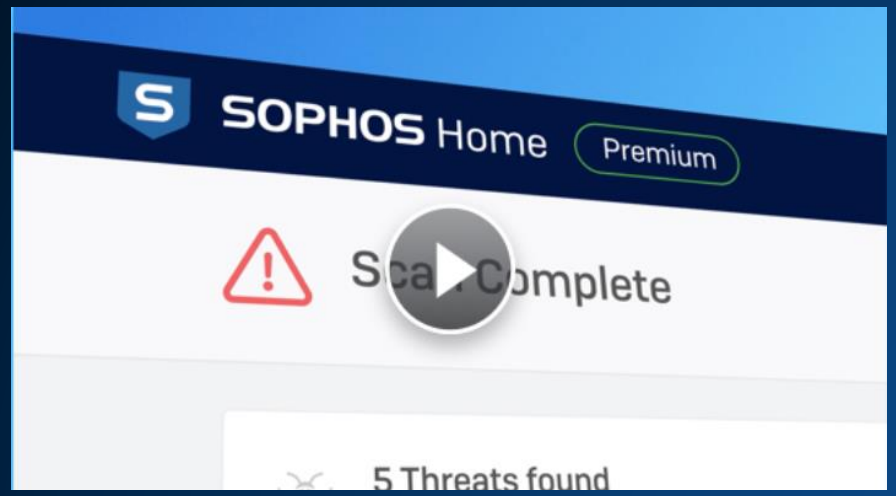
Złote zasady

- Wiadomości Phishing’owe poproszą o:
  - podaj poufne informacje, takie jak nazwy użytkowników lub hasła
  - kliknij w złośliwy link
  - otwórz złośliwy załącznik
- Złote zasady dla użytkowników:
  - zweryfikuj nadawcę, sprawdzając jego adres e-mail
  - sprawdź link przed kliknięciem
  - zachowaj ostrożność przy podawaniu danych osobowych
  - nie spiesz się, nie poddawaj się presji

Chroń swoją organizację

- Sprawdź świadomość użytkowników (Sophos Phish Threat)
  - Ochrona najsłabszego punktu wejścia
  - Świadomy użytkownik może zatrzymać KAŻDY atak phishingowy
- Zaimplementuj Sophos Email
  - Ochrona przed spamem i phishingiem
  - Time-of-Click ochrona URL
- Sprawdź ruch w sieci za pomocą XG Firewall
  - Ochrona AV i Sandbox
  - Filtrowanie URL z Xstream SSL Inspection
  - Ochrona IPS i ATP
  - Opcjonalnie: ochrona Antispam/Anti-Phishing
- Chroń swoje komputery za pomocą Sophos InterceptX Advanced z EDR
  - Ochrona Anti-Ransomware
  - Ochrona przed Exploit'ami
- Synchronized Security
  - Izolacja klienta
  - Kontrola aplikacji

SOPHOS



Sophos Home for Commercial Use za darmo

Sophos Home Commercial Use Edition to DARMOWA wersja Sophos Home Premium z obsługą bazy wiedzy

Jak otrzymać?

- Skontaktuj się z Sophos LUB z Partnerem z prośbą o SHFCU i daj znać jaką liczbę licencji potrzebujesz

- Nie jesteś jeszcze klientem Sophos? - kup DOWOLNE Rozwiązanie Sophos i uzyskaj bezpłatne licencje na ochronę swoich urządzeń w domu

Ta oferta jest przeznaczona dla WSZYSTKICH klientów Sophos, niezależnie od używanego produktu Sophos.
Więcej info- https://home.sophos.com/en-us/landing/commercial-use.aspx

Co dalej?

Date	Topics
30 Marzec 2020	Koronawirus a praca zdalna: co powinieneś wiedzieć

Zarejestruj się teraz i dowiedz się, jak wdrożyć bezpieczną pracę zdalną udostępnij link rejestracyjny znajomym i współpracownikom: https://attendee.gotowebinar.com/register/2051810049240329485

Co dalej ?

Bezpieczna praca zdalna

W tym czasie ważne jest zwiększenie świadomości na temat bezpieczeństwa cyfrowego, ponieważ zaobserwowaliśmy już wzrost liczby ataków phishingowych.

Zdalna praca na skalę, której doświadczamy, zwiększa ryzyko cybernetyczne, jak nigdy dotąd, cała ta zmiana online ułatwiła hakerom wykorzystanie oszustwa w celu uzyskania dostępu do systemów

Jednak praca zdalna nie musi być ryzykowna, dołącz do już w poniedziałek, aby uzyskać szczegółowy informacje:

- Jak ułatwić zdalną pracę
- Uwierzytelnianie wieloskładnikowe
- Ustanowienie bezpiecznych i szyfrowanych tuneli VPN dla pracowników zewnętrznych

SOPHOS

Cybersecurity evolved.