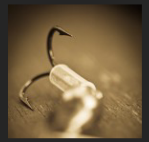
Skuteczne zabezpieczenie danych przed nieznanymi zagrożeniami

aleksander_kroszkin@trendmicro.com
9.05.2017

Uwaga na wyjątkowo perfidny atak phishingowy na konto Google

Adam dodał 3 maja 2017 o 22:46 w kategorii Prywatność, Socjo, Włamania z tagami: atak • Google • OAuth • phishing • token

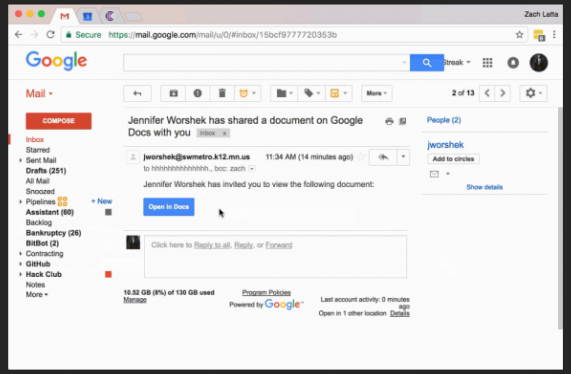


(źródło: Nomadic Lass)

Oglądamy codziennie różne ataki. Czasem gorsze, czasem lepsze. A czasem takie, że sami, patrząc na zrzuty ekranów, mówimy „Gdyby przyszedł do nas to trudno powiedzieć, czy na pewno byśmy rozpoznali". To właśnie jeden z nich.

Atak, który zrobił na nas takie wrażenie, pojawił się w skrzynkach użytkowników na całym świecie kilka godzin temu. Na początek pokażemy Wam, jak wygląda ekran po ekranie, a potem opiszemy, co tak naprawdę dzieje się pod spodem i jakich sztuczek użyli przestępcy. Do zobrazowania ataku wykorzystujemy film nagrany przez Zacha Latta.

Zaczyna się od zwykłej wiadomości z prośbą o zapoznanie się z dokumentem Google Docs.



Jeśli klikniecie w guzik „Open in Docs" traficie na prawdziwą stronę Google, z prawdziwym ekranem pytającym Was o to, którego konta chcecie użyć.

Najlepsze w tym miesiącu

- Uwaga na wyjątkowo perfidny atak phishingowy na konto Google
- Więźniowie zbudowali komputer, ukryli w suficie i użyli do oszustw finansowych
- Historia apokalipsy Windowsów, która była tuż tuż – i niespodziewanie zniknęła
- Rosyjski operator na kilka minut przejął ruch sieciowy wielu firm – w tym polskiego banku
- Zdalne wykonanie kodu w WordPressie odkryte przez Polaka (tylko do wersji 4.7)

Trzymaj rękę na pulsie

Adres email zapisz

Wyszukiwanie

Szukasz czegoś? szukaj

Co się stało?

Przez cały czas trwania ataku przebywaliście tylko na stronie Google. Domena była prawidłowa, prawidłowy był certyfikat SSL. Przestępcy wykorzystali jednak bardzo sprytną sztuczkę, opisaną kilka dni temu przez firmę Trend Micro. Polega ona na kradzieży tokenu OAuth zamiast zwyczajowej kradzieży hasła. Token ten pozwala użytkownikom pozwolić aplikacji na dostęp do ich danych bez konieczności podawania jej swojego hasła. Przestępcy najpierw tworzą aplikację, którą nazywają na przykład Google Docs. Następnie zgłaszają ją do Google by mogła poprosić użytkowników o tokeny OAuth w celu uwierzytelnienia. W kolejnym kroku wysyłają phishing, w którym wskazują na link prowadzący do procesu uwierzytelnienia aplikacji. Link wygląda wiarygodnie, ponieważ prowadzi do serwerów Google. Aplikacja wygląda wiarygodnie, ponieważ ma „Google" w nazwie. Jeśli ktoś zgodzi się przyznać jej dostęp do swojej poczty, przestępcy dostają token OAuth, za pomocą którego mogą kontrolować pocztę ofiary.

Niestety oznacza to, że gdy ofiara ataku zmieni swoje hasło, to przestępcy nadal mają dostęp do jej konta. Dodatkowo dwuskładnikowe uwierzytelnienie nie chroni przed tym atakiem – sam właściciel konta daje dostęp do niego przestępcom. Aby faktycznie zabezpieczyć swoje dane trzeba odwiedzić listę aplikacji, które mają dostęp do konta Google, a następnie usunąć z niej wszystkie podejrzane pozycje (lub usunąć wszystkie a następnie dodać te potrzebne z zaufanych źródeł).

Jeśli otrzymaliście email z podobnym linkiem, dajcie nam znać.

Aktualizacja 23:00

Docierają do nas informacje, że złośliwa aplikacja, gdy już zdobędzie dostęp do Waszego konta, pobiera książkę adresową i wysyła wiadomości z Waszego konta do Waszych kontaktów – dlatego tez atak na Wasza skrzynkę może przyjść od kogoś, kogo znacie i komu ufacie. Przestępcy wykorzystują w ataku dziesiątki różnych domen typu docscloud|g-cloud|g-docs|gdocs.download|info|win|pro.

Podobne wpisy

- Jak Wiadomości TVP okłamują widzów w sprawie afery KNF
- Spowodował atak epilepsji przez Twittera, wpadł przez swoją głupotę
- Polacy rządzą wśród łowców błędów w usługach i produktach Google

komentarzy 48

The data center has evolved
faster than everyone imagined…

…and many are encountering
challenges because their approach
to security did not evolve.

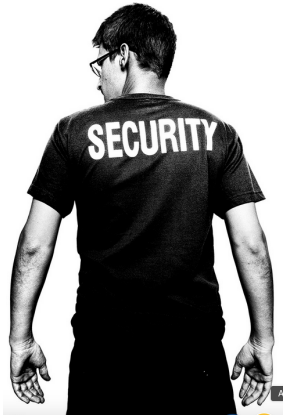
Data Center Security Options

Secure Perimeter

vs.

Zero-Trust Pervasive Security

What does Pervasive Security look like?



Secure Perimeter

vs.

Granular Per-Tenant Security

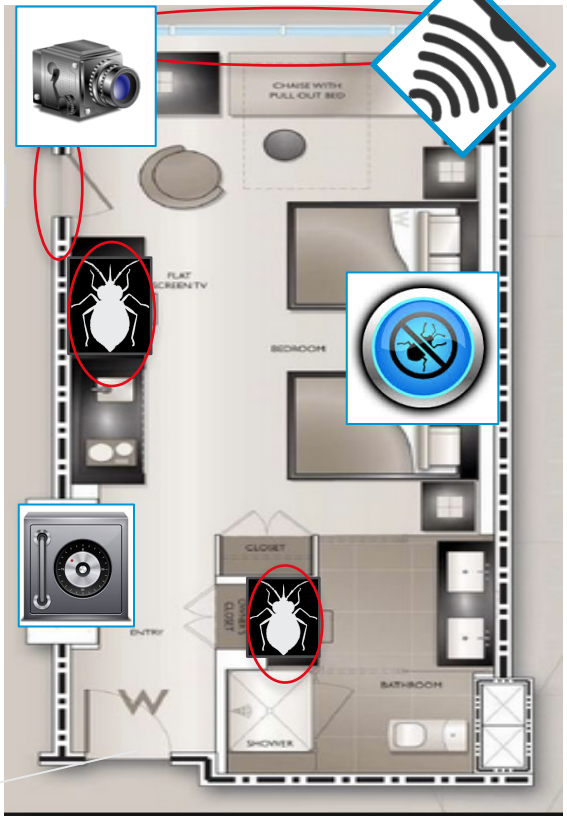
What do we need at the endpoint?

5. “Tampering” protection:
CCTV

6. Tracking / Logging:
CCTV

4. Deeper Security:
Safe

1. Authorized Access:
Room Key



2. Intrusion Detection:
Motion Sensor

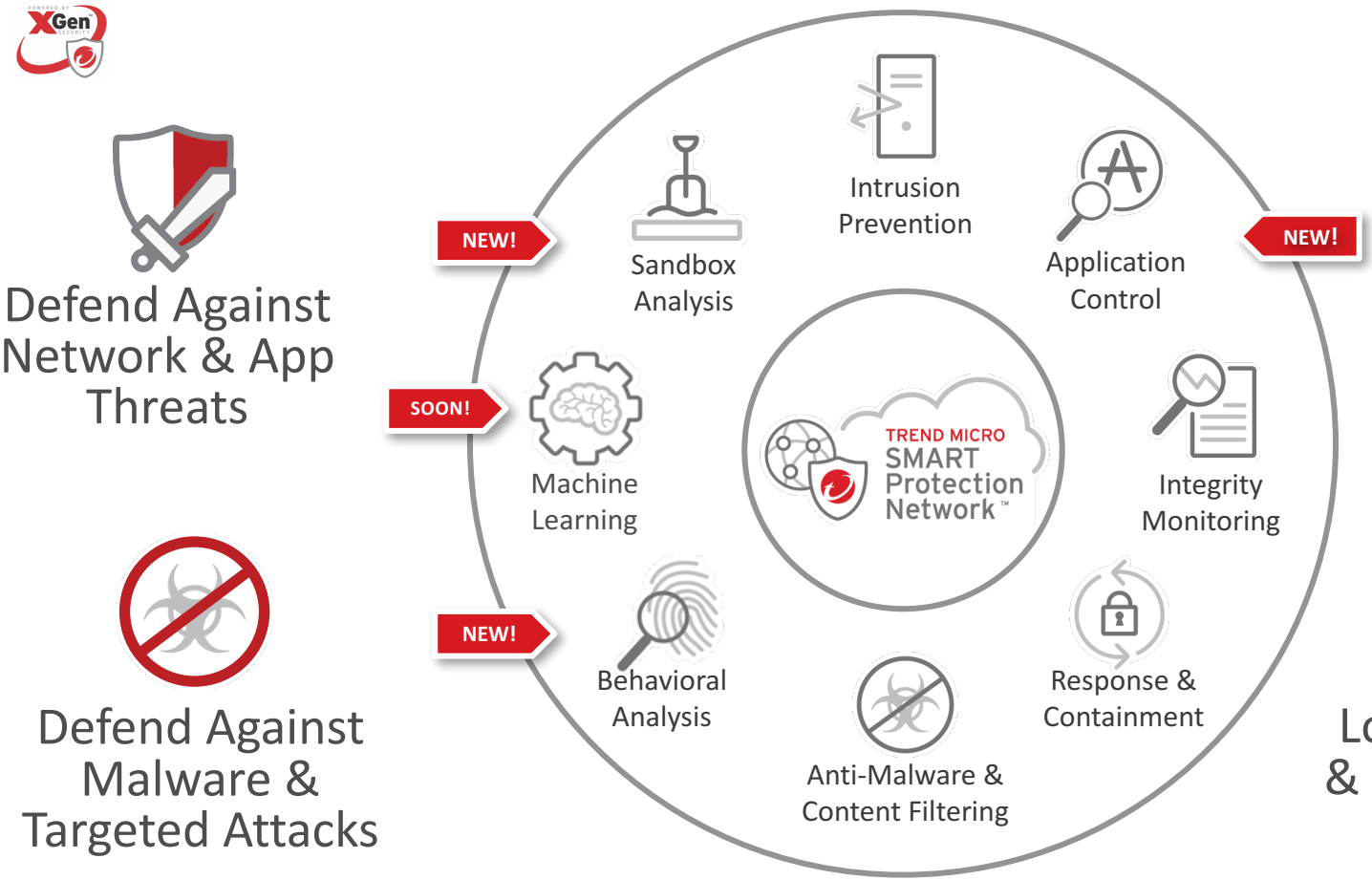
3. “Bug” Removal

TREND MICRO

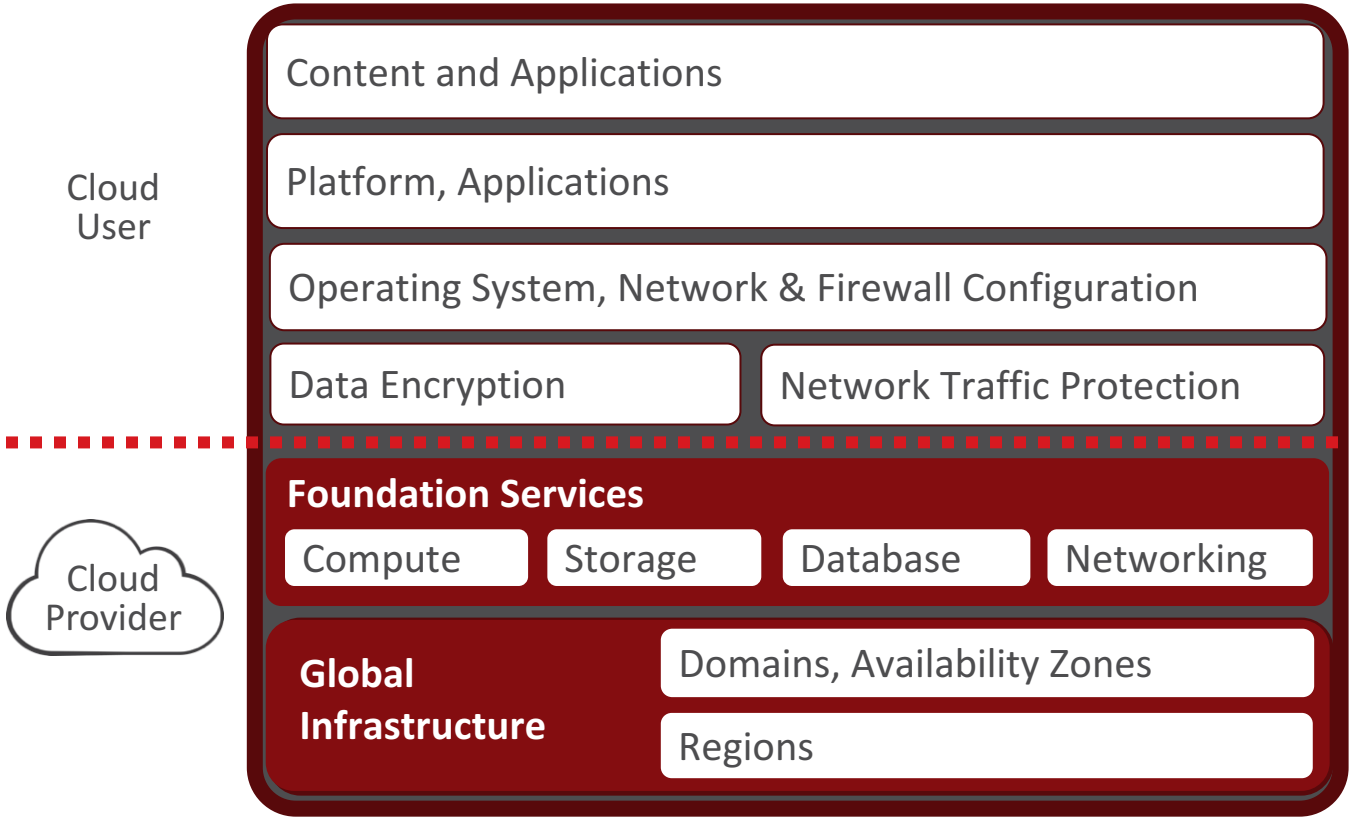
How does this map to Data Center Security?

1.	Authorized Access	= Micro-Segmentation
2.	Intrusion Prevention	= Host IPS
3.	Bug Removal	= Anti-Virus / Malware Removal
4.	Deeper Security	= Next-Gen Firewall
5.	Tampering Protection	= File Integrity Management
6.	Tracking/Logging	= Log Inspection
7.	Virtual Patching	= Protection of unpatched OSs

TREND MICRO


Defend Against Network & App Threats
Intrusion Prevention
NEW!
Sandbox Analysis
Application Control
NEW!
SOON!
Machine Learning
TREND MICRO
SMART Protection Network™
Integrity Monitoring
NEW!
Behavioral Analysis
Anti-Malware & Content Filtering
Response & Containment
Protect Against Vulnerabilities
(like Heartbleed, Shellshock etc.)
Defend Against Malware & Targeted Attacks
Lock Down Systems & Identify Suspicious Changes

Cloud Security is a Shared Responsibility



Cloud providers deliver a secure infrastructure.

But YOU need to protect what you put IN the cloud—your workloads.

Shared responsibility for compliance

Cloud
User

Facilities

Physical security of hardware

Network infrastructure

Virtualization infrastructure

- File & System integrity monitoring
- Intrusion detection & prevention
- Firewall
- Anti-malware
- Vulnerability scanning & updating

Securing a Multi-Cloud Strategy

Secure workloads in multiple cloud environments

Leverage same core advanced security controls in physical, virtual, cloud and hybrid environments

Future proof private cloud and data center security investments

Google Cloud Platform

Center for Internet Security®

SANS

Helping with

14 of 20

Critical Security Controls

SANS / CIS TOP 20 CRITICAL SECURITY CONTROLS	
1. Inventory of Authorized & Unauthorized Devices	11. Secure Configurations for Network Devices
2. Inventory of Authorized & Unauthorized Software	12. Boundary Defense
3. Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers	13. Data Protection
4. Continuous Vulnerability Assessment & Remediation	14. Controlled Access Base on the Need to Know
5. Controlled Use of Administrative Privileges	15. Wireless Access Control
6. Maintenance, Monitoring, & Analysis of Audit Logs	16. Account Monitoring & Control
7. Email and Web Browser Protections	17. Security Skills Assessment & Appropriate Training to Fill Gaps
8. Malware Defenses	18. Application Software Security
9. Limitation and Control of Network Ports, Protocols, and Services	19. Incident Response Management
10. Data Recovery Capability	20. Penetration Tests & Red Team Exercises

Build security into the application lifecycle

Security is enforced through every step of an application's lifecycle

- Deploy security service
- Create security groups and policies

- Dynamically assign security groups and policies

- Run periodic automated scans for threats
- Monitor applications for vulnerabilities
- Monitor and record system changes

- Address threats & vulnerabilities
- Respond to emergent attacks
- Adjust security policy as app changes over time

- Decommission security services
- Report compliance and generate audit logs

Udanego dnia!

aleksander_kroszkin@trendmicro.com