Forcepoint - Sinn für menschliches Verhalten: der Schlüssel zu moderner Cybersicherheit

Frank Limberger
Insider Threat Detection Specialist

Michael Stanik
Senior Sales Engineer

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

UNDERSTANDING USER INTENT

ACCIDENTIAL INSIDER		COMPROMISED INSIDER		MALICIOUS INSIDER	
Poorly communicated policies and user awareness	Data where it shouldn't be, not where it should be	Phishing targets, breaches, BYOD contamination	Credential exfiltration, social engineering, device control hygiene	Leaving the company, poor performance review	Corporate espionage, national espionage, organized crime

Frustrated User

User logs into a different corporate laptop

Sends email with confidential data

A confidential file is copied to USB

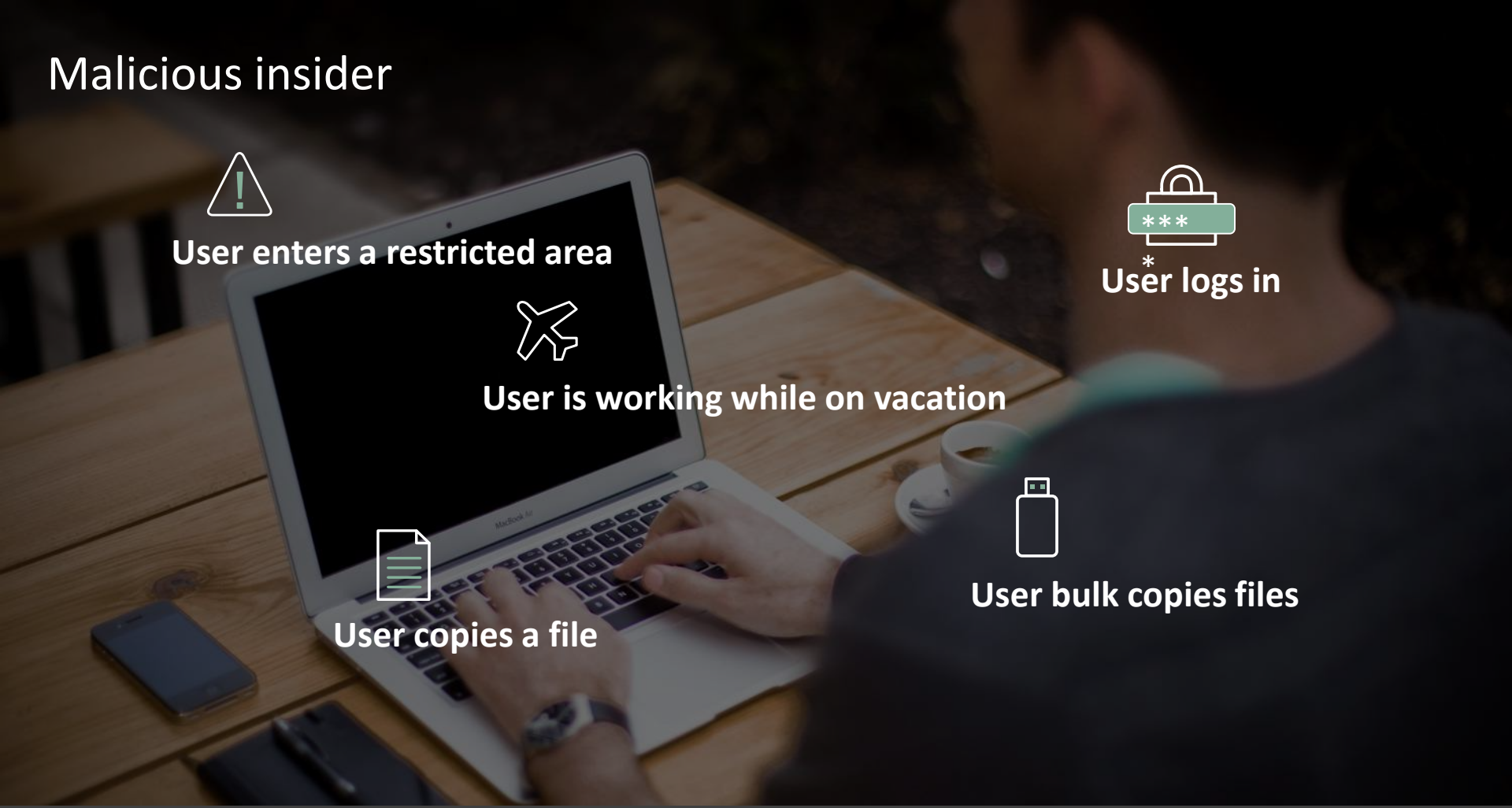
User stores data in his private cloud

BOX CASE

Security researchers have found dozens of companies inadvertently leaking sensitive corporate and customer data because staff are sharing public links to files in their **Box** enterprise storage accounts that can

Techcrunch March 2019

Malicious insider



Dokumentenmissbrauch

"Handfester Skandal" bei Airbus?

Stand: 19.09.2019 13:21 Uhr

Mitarbeiter des Flugzeugbauers Airbus stehen im Verdacht, sich Planungsunterlagen der Bundeswehr beschafft zu haben. Mitglieder des Verteidigungsausschusses sind empört.

KORRESPONDENTIN

TECHNOLOGY

Former McAfee employees conspired to take 'secret sauce' to Tanium, lawsuit says

JUNE, 2019

Compromised Insider

Statt Erpressungstrojaner: Krypto-Miner auf dem Vormarsch

20.04.2018 11:42 Uhr – Dennis Schirrmacher

vorlesen

(Bild: Pixabay)

Malware-Autoren setzen vermehrt auf bösartige Mining-Software. Dieses Jahr hat es einem Sicherheitsunternehmen zufolge erstmals mehr Infektionen dieser Art als mit Ransomware gegeben.

https://www.heise.de/security/meldung/Statt-Erpressungstrojaner-Krypto-Miner-auf-dem-Vormarsch-4028279.html

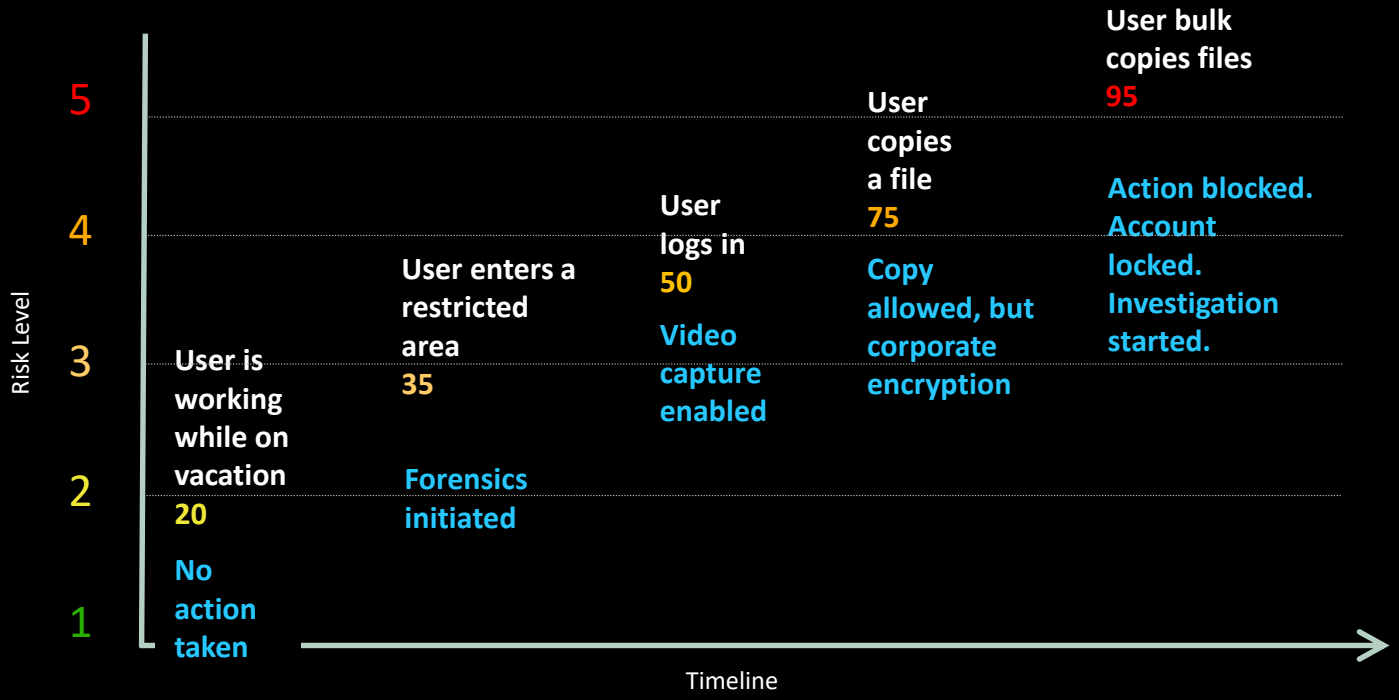
FORCEPOINT

Security Risk Sites Blocked by Date

Date Range: 2018-04-11 - 2018-04-11

Date	URL	Requests
2018-04-11		
	6images.cgames.de	1
	849715076759606.mateti.net	3
	a1.zanox.com	30
	af.stroeerdp.de	4
	ancensored.com	5
	aqt.adalliance.io	54
	box.r66net.com	1
	cdn1.jameda-elements.de	44
	cdn2.jameda-elements.de	6
	cdn3.jameda-elements.de	7
	coinhive.com	11,970
	confirm.orders-ticketbar.eu	1
	delivery.content-recommendation.net	2

with risk-adaptive protection



Risk-adaptive protection

Better with,
or without?

10.1 - 208

Thank you

michael.stanik@forcepoint.com