Atacuri avansate impotriva institutiilor financiare

Metode de prevenire si raspuns

Teodor Cimpoesu, Cyber Security BU Director

Cyber Risks, Bucuresti, 9 Oct, 2014


Cum cred CSOs din fin/banking ca arata apararea lor cibernetica?

Hackers May Have Targeted at Least 13 Firms

Investigators Believe Another Firm Lost Data

Email Print 4 Comments

By EMILY GLAZER, DANNY YADRON AND DANIEL HUANG CONNECT

Updated Oct. 8, 2014 10:09 p.m. ET

Citi and others saw indications of activity but weren't breached. *Bloomberg News*

Investigators believe that the hackers who broke into J.P. Morgan Chase JPM +1.91% & Co. targeted at least 12 other financial-services companies, including Fidelity Investments, people familiar with the matter said, suggesting the cyberattack spree on

"Investigators believe that the hackers who broke into **J.P. Morgan Chase** targeted **at least 12 other financial-services companies** […] suggesting the cyberattack spree on Wall Street was broader than previously thought."

"Hackers appear to have originally breached J.P. Morgan's network via an **employee's personal computer**, people close to the investigation have said. From there, the intruders were able to **leapfrog** to additional data because the **machine** accessed **had administrative privileges**, the people said." (online.wsj.com)

Stagii de atac

1. • Colectarea de intelligence– OSINT, CYBINT, HUMINT
2. • Infectarea tintei – SE, BYOD, spear phishing, water holing
3. • Exploatarea sistemului– zero-day exploits, half-day exploits + RATs
4. • Cercetare/misiune interna – miscari laterate si de mentinere a controlului
5. • Exfiltrare de date – peste FTP/HTTP, sau protocoale cunoscute/false

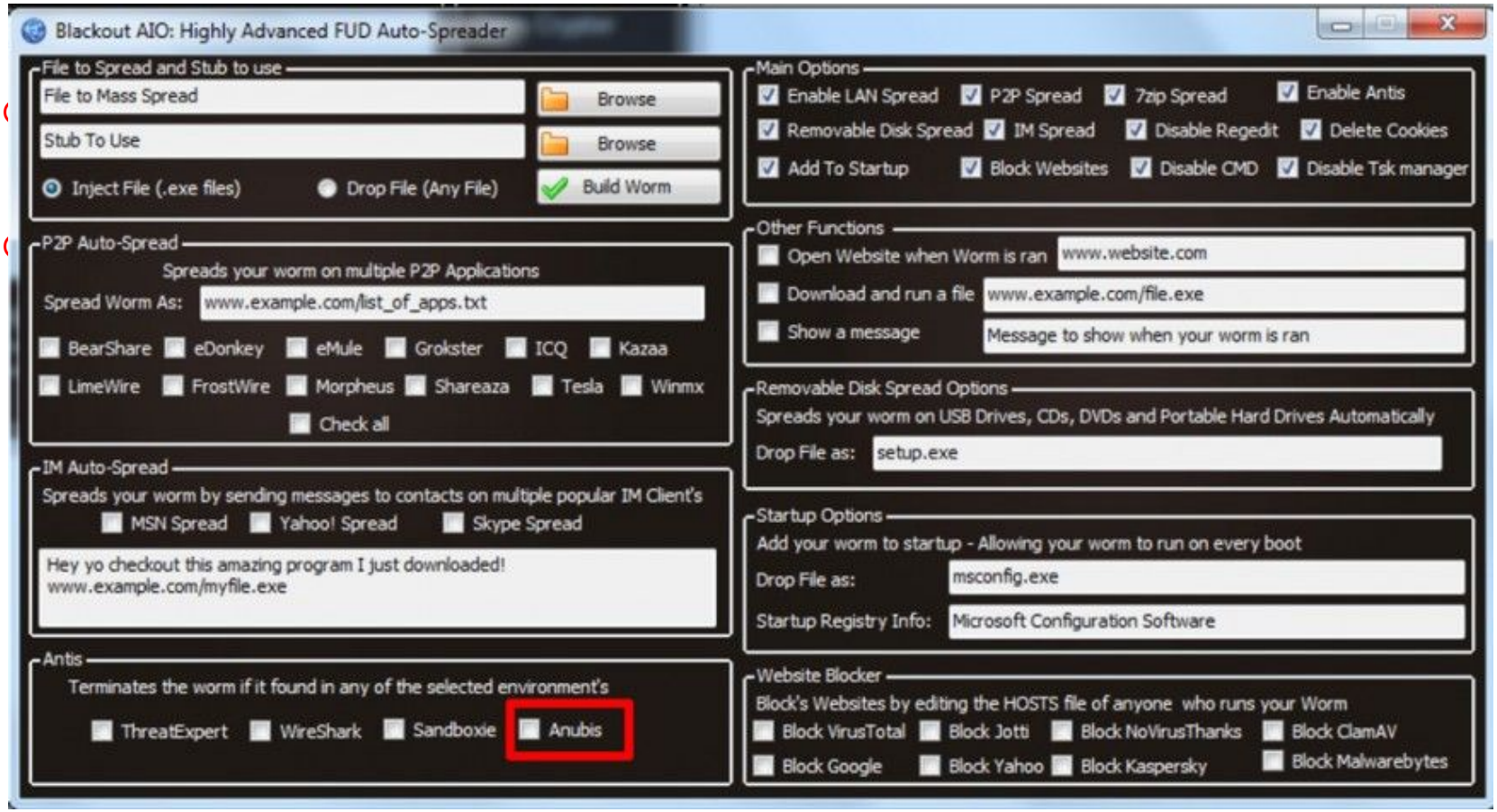
Atacuri targetate vs. APT

Tactic	Targeted cyber attacks	Advanced Persistent Threats
Deceptive	Yes	Yes
Stealthy	Yes	Yes
Exploits	Both known/unknown exploits	Primary zero days are used
Persistent	Depends on the design	Yes
Data exfiltration	Yes	Yes
Maintaining access	Yes (RATs)	Yes (RATs)
Intelligence reuse	Yes	Yes
Lateral movement	Depends on the design	Yes
Campaigns	Depends on the design	Are started as campaigns
State sponsored	Possible	More likely
Actors	Individual or group	Group

APT-urile nu sunt tactici de manual si nu se constituie in vectori binecunoscuti. Nu sunt limitate de capabilitati de atac sau de cyber intelligence. Nu au formula specifica. *Ele sunt campanii.*

Sursa: "Targeted Cyber Attacks – multi stage attacks driven by exploits and malware", Adita Sood (2014)

Tools of the trade



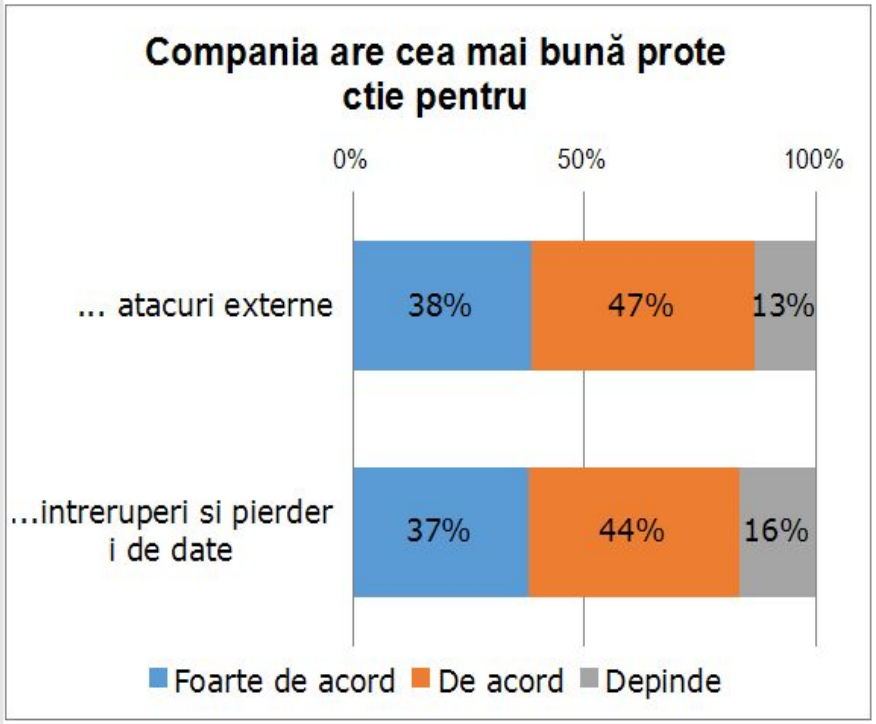
IT Security - Astazi

"There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don't know it" – Gartner Inc. (2012)

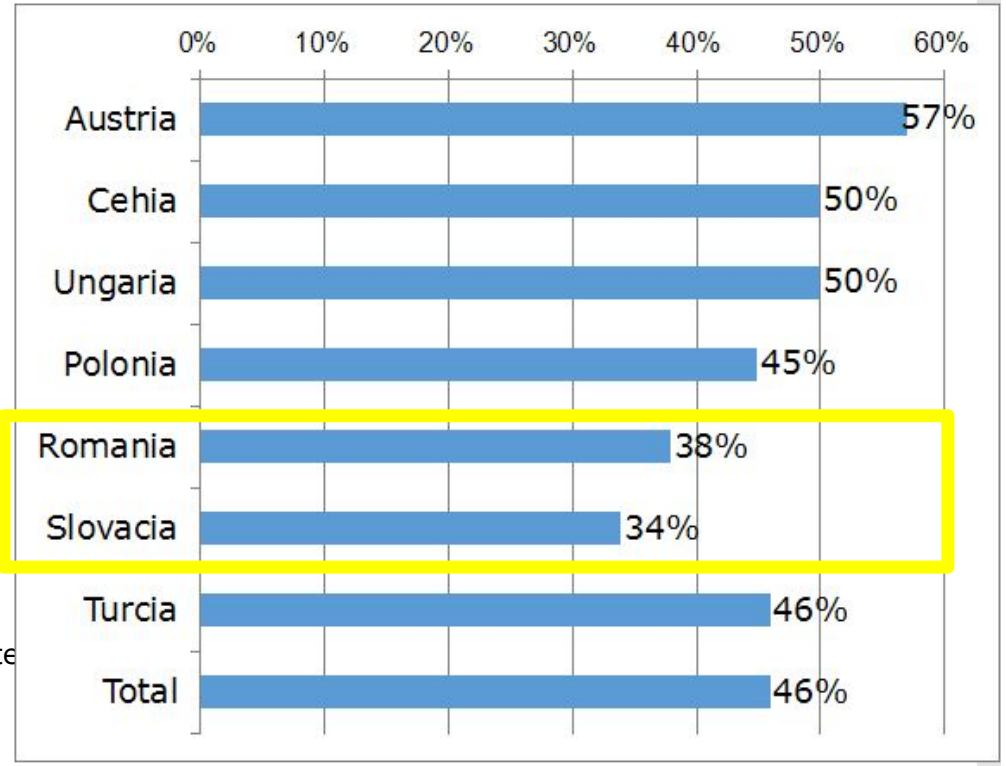
Impacts	Top Recommendations
The failure of traditional security tools to stop targeted attacks requires security organizations to balance technology investments and processes in all four stages of the security life cycle.	• Balance investments across the security life cycle. • Invest in hardening endpoints with policy- and process-based controls. • Invest in continuous monitoring tools and processes to reduce dwell time.
Security organizations must assume they are compromised and invest in detective capabilities that provide continuous infection monitoring.	• Track dwell time and time to recovery as key performance metrics. • Create infrastructure to store baseline information. • Create systems to monitor suspect changes in endpoints and the network.
Policy-based controls are highly effective and should be considered as the first line of defense against malware attacks.	• Invest in proactive application management. • Invest in "default-deny" application control solutions.

Source: Gartner whitepaper, *"Malware Is Already Inside Your Organization; Deal With It"* (2014)

Securitate cibernetică – stare curentă



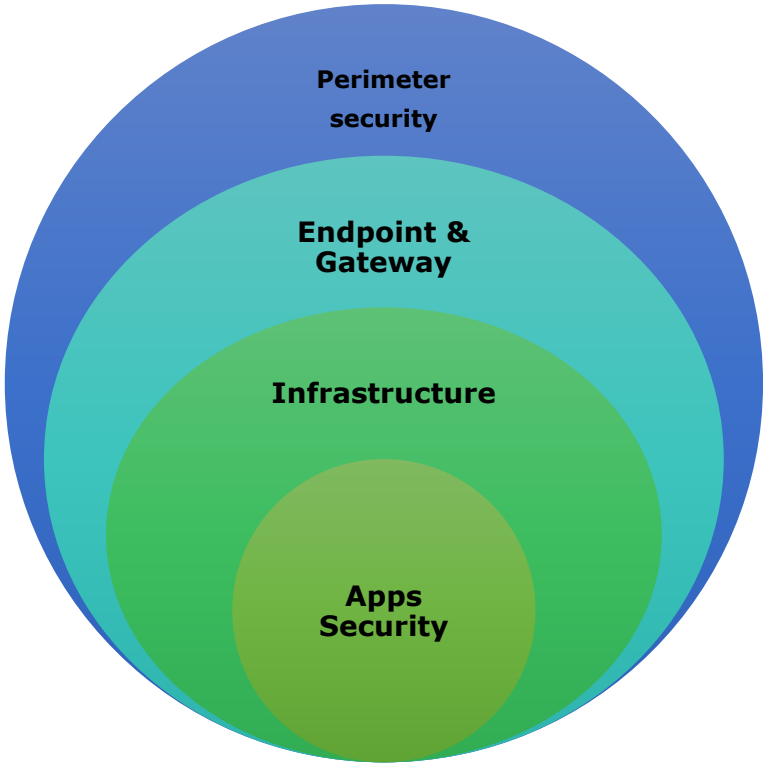
Verificări de securitate cu partener extern în ultimii 3 ani



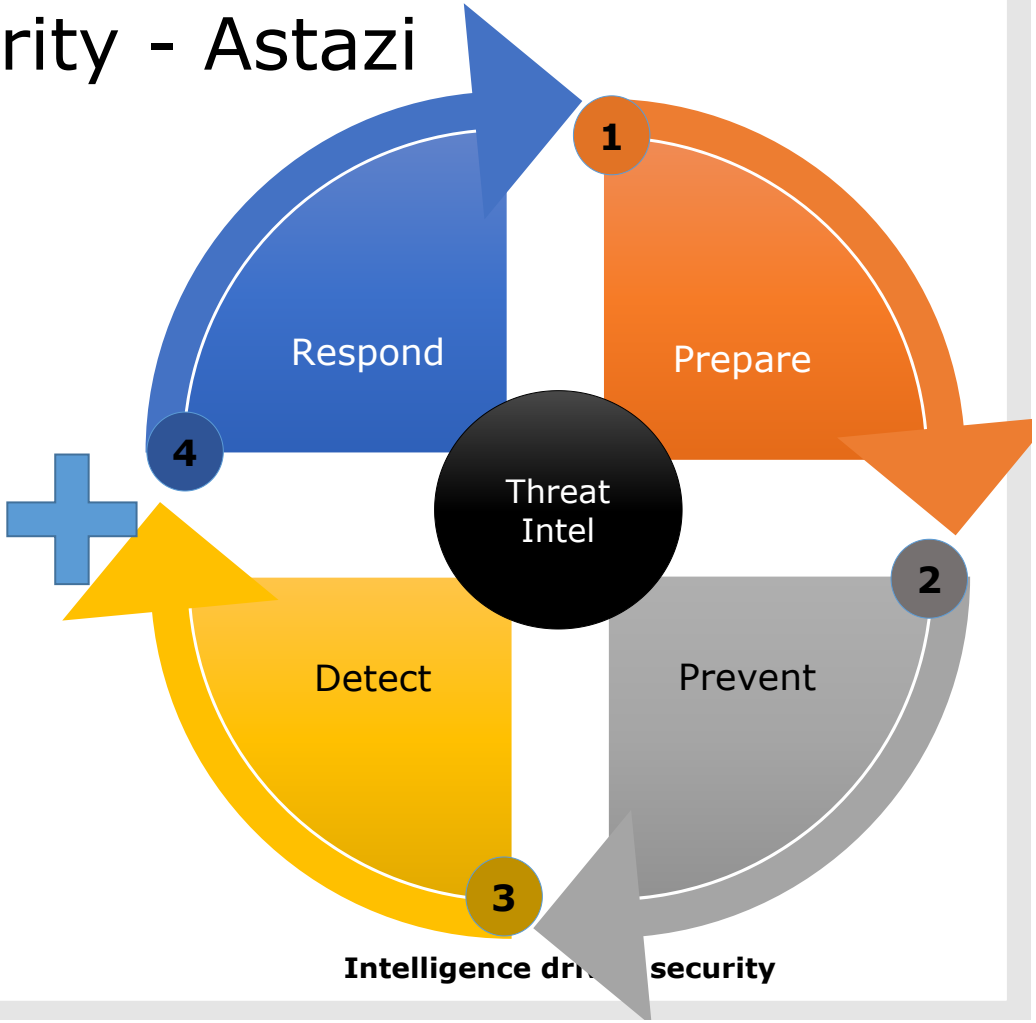
Deș i foarte multe companii nu au făcut verificări de securitate cu o parte terț ă – deci le-au făcut intern – încrederea este destul de ridicată privind statura de securitate ș i asigurarea celei mai bune protecț ii.

Sursa: *ICT Business Trends & Challenges in Austria, CEE and Turkey,* Pierre Audoin Consultants (2014)

IT Security - Astazi



Security in-depth

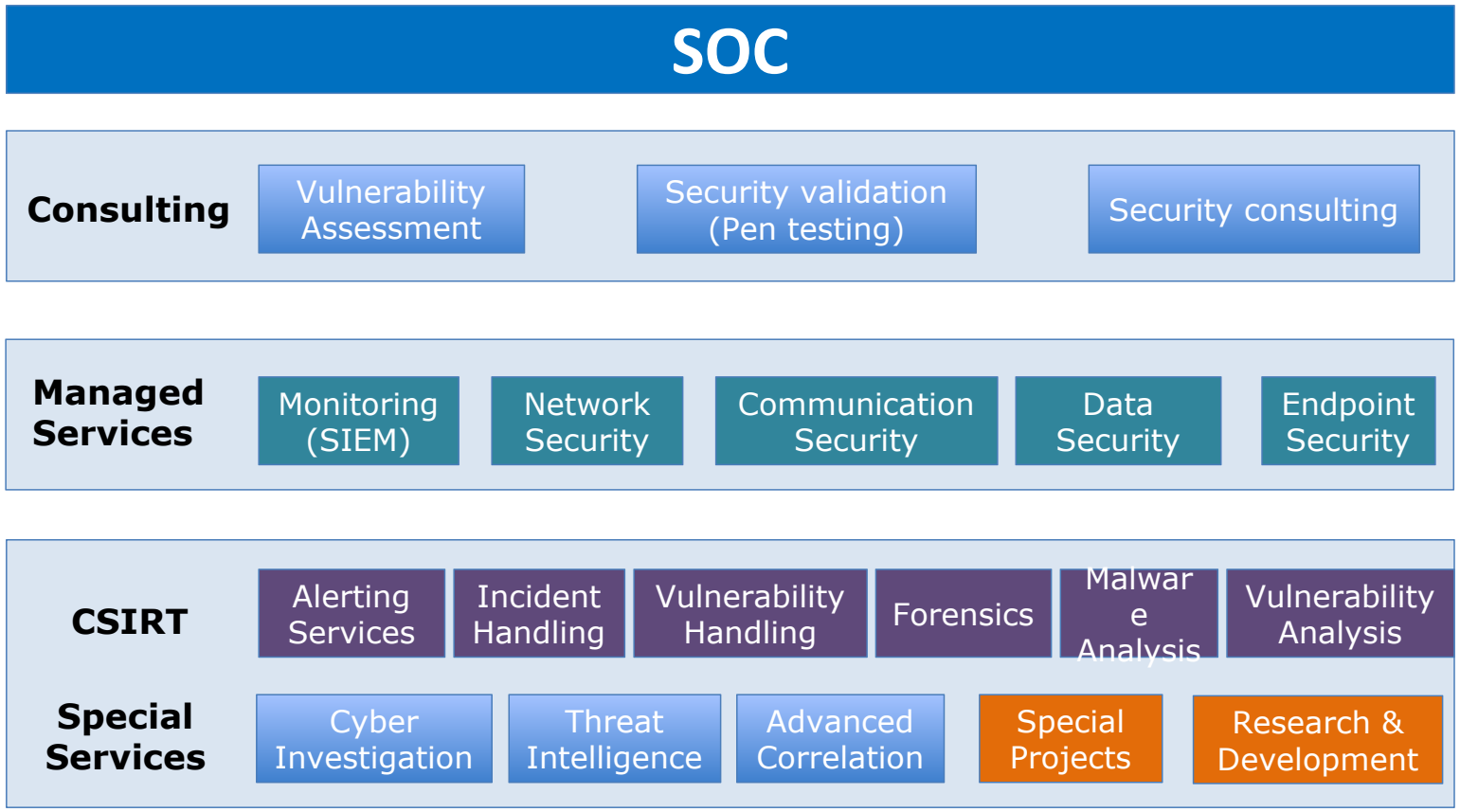


Intelligence dri security

The kill chain

Source: "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Eric M. Hutchins et al.
Image: http://www.digitalbond.com/blog/tag/cyber-kill-chain/

certSIGN – MSSP & CSIRT



Teodor.Cimpoesu@certsign.ro
@cteodor
+40724.039.254

csirt@certsign.ro