

NAGY SÁV, NAGY VÉDELEM A KIBERBIZTONSÁG MODERN FAKTORAI

Keleti Arthur
Kecskemét, 2014.10.08

 T-systems



TEMPÓ SÁVSZÉLESSÉG KOMPLEXITÁS



Wanted by the FBI

Home • Most Wanted • Cyber's Most Wanted

Cyber's Most Wanted

Select the images of suspects to display more information.



SUN KAILIANG



HUANG ZHENYU



WEN XINYU



WANG DONG



GU CHUNHUI



BJORN DANIEL SUNDIN



ALEXANDR SERGEYEVICH BOBNEV



CARLOS ENRIQUE PEREZ-MELARA



ANDREY NABILEVICH TAAME



NOOR AZIZ UDDIN

Show All



EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer... more →

Evgeniy Mikhailovich Bogachev, using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims' computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information necessary to log into online banking accounts. While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised web sites. Victims who visited these web sites were infected with the malware, which Bogachev and others utilized to steal money from the victims' bank accounts. This online account takeover fraud has been investigated by the FBI since the summer of 2009. Starting in September of 2011, the FBI began

SUMMARY
ALIASES
DESCRIPTION
MORE PHOTOS

- GET POSTER
- HA PYCKKOM
- SUBMIT A TIP

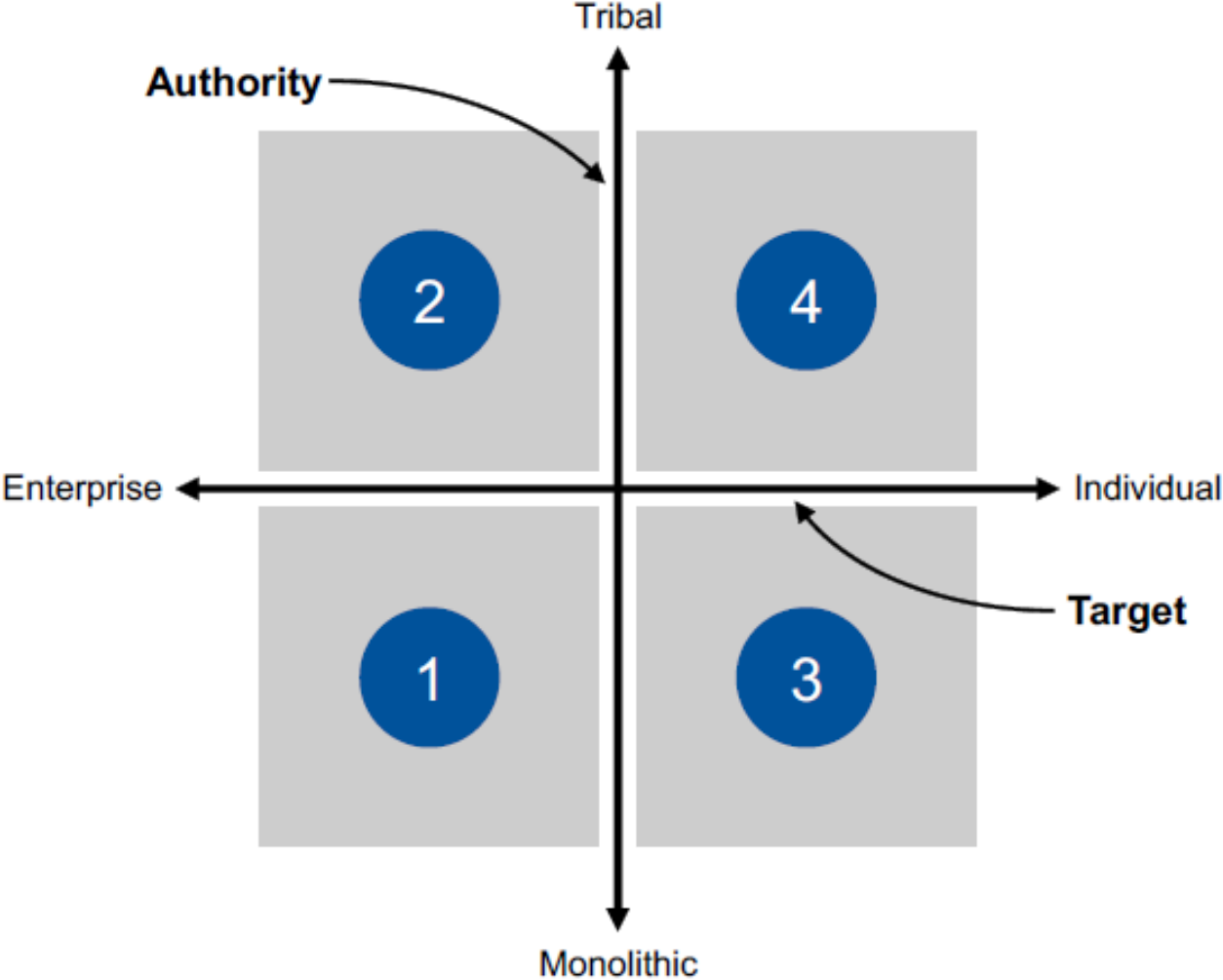


A KÍNAIAK JOBBAN CSINÁLJÁK



HOVA LETT A „RÉGI” HACKER? ÉRTJÜK A MOTIVÁCIÓKAT?

Figure 1. The Gartner Security and Risk Management Scenario

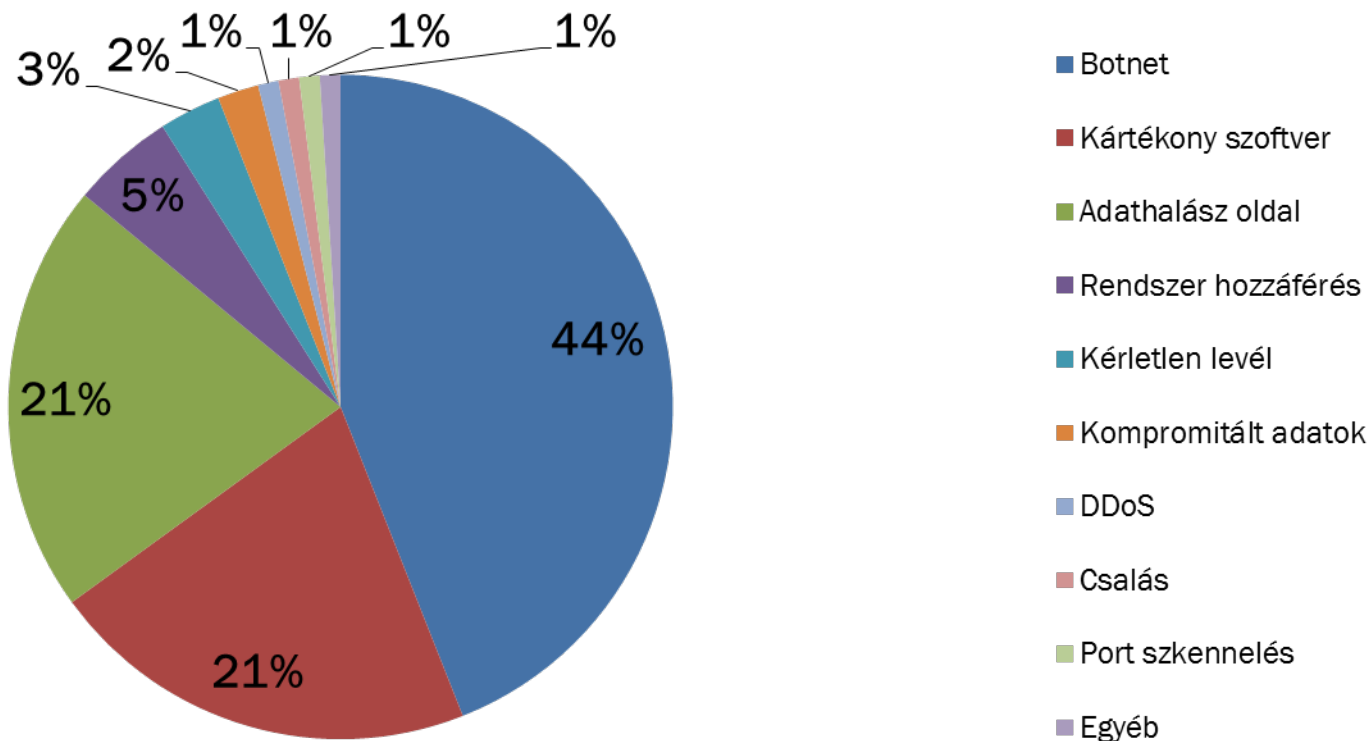


Source: Gartner (May 2013)



A DOLGOK INTERNETE

NMHH RIPORT - ENISA EZ VOLT 1,5 ÉVE – MI LEHET MOST?

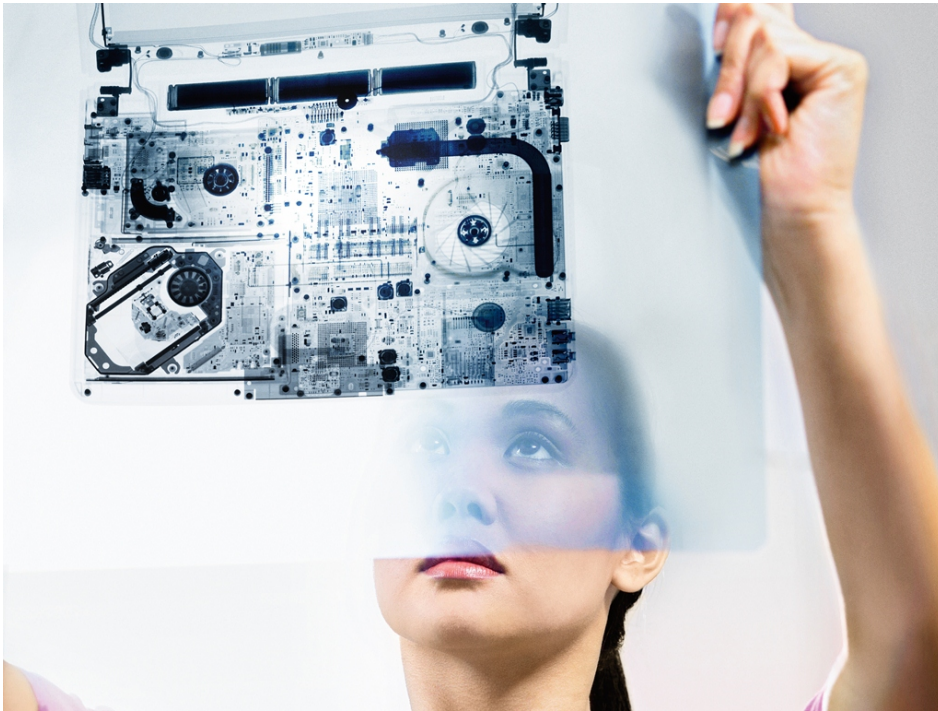


Forrás: NMHH riport az ENISA és a Bizottság számára, 2013. március



A FEL- ÉS BEISMERÉS HIÁNYA

GYÁRTÓK A STRATÉGIÁK EREDŐJE



Big Data biztonság

Mobil? VoIP?

Titkosítás?

Hálózati adatelemzés

Alkalmazás biztonság

Malware kezelés

Incidens kezelés,
SOC



A SZOLGÁLTATÓ DOLGA?

ÉS A JÖVŐ?



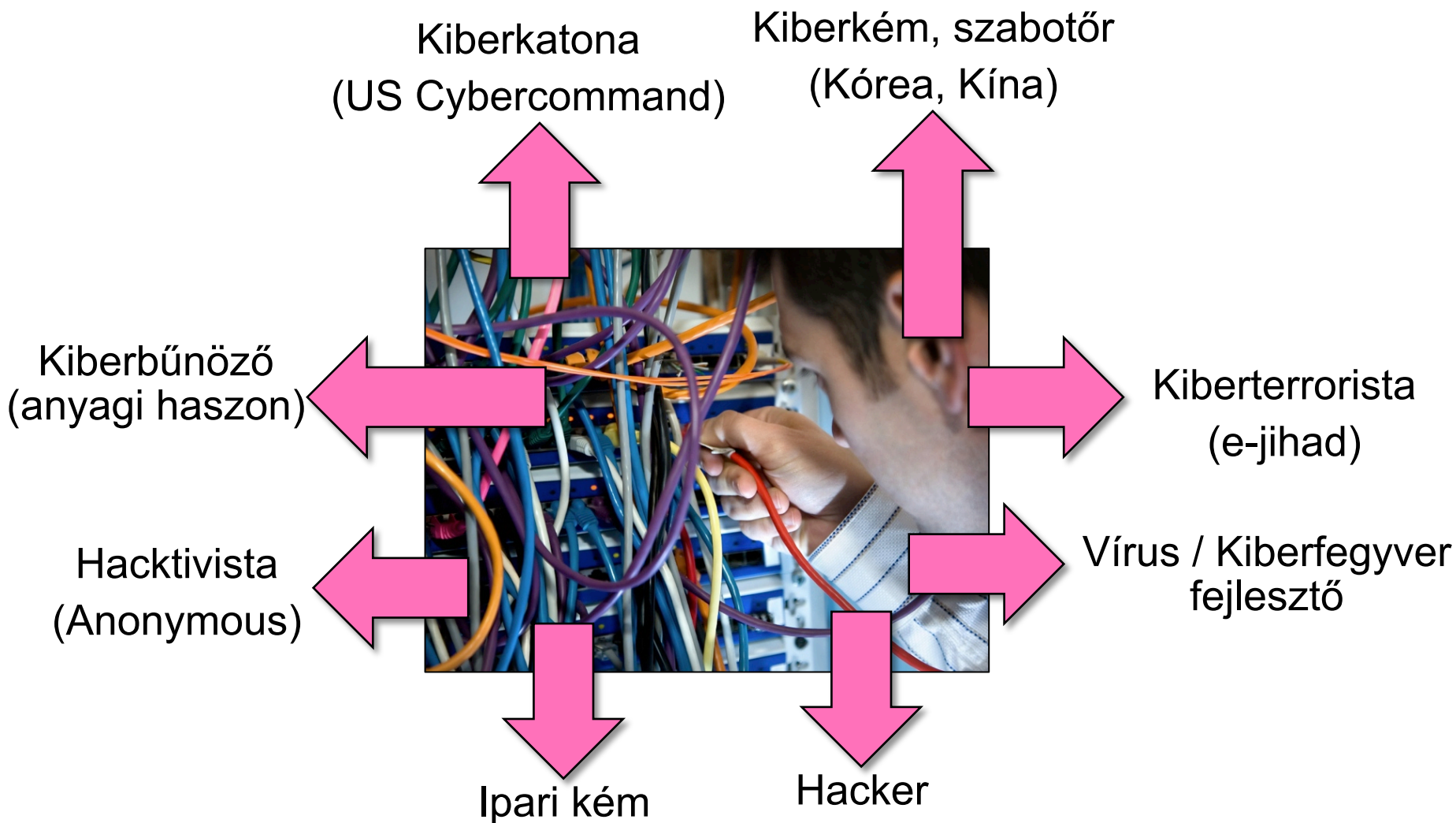
KÖSZÖNÖM!

Keleti Arthur

keleti.arthur@t-systems.hu

 T-Systems

MI LETT AZ „EGYSZERŰ” HACKERBŐL



KIBERTÉR VÍZIÓK MIT CSINÁLNAK A KORMÁNYOK



Kép forrás: Internet, <http://www.forbes.com>

- Pl. spy/malware-t írnak Androidra
- Tavaly tibeti aktivistákat célzó támadás
- Nem sokkal korábban a Kaspersky Lab is talált egyet
- Köthető a Kínai kormányhoz
- Komplex, célzott email és phishing támadás
- Amiket lop: kontakt adatok a telefonból és a SIM-ről, hívás adatok, SMS-ek, Geo lokációs adatok, telefon adatok
- A frissen talált verzió (képen) + telekommunikációs cégek adatai = pontos lokáció

KIBERTÉR VÍZIÓK GARTNER VARIÁNSOK – 2020-RA

Regulated Risk: (Szabályzott biztonság)

- Alapvetően tömbösít, a kormányzat előír
- A cégek + államigazgatás együtt, biztonsági csapat fókusz (kiberháborús lépések?)

Controlling Parent: (Irányító szülő)

- Az egyének a fő támadási célcsoport
- Kétes adatbányászati módszerek, privát szféra?
- A kormányzat erre reagálva szigorúan szabályoz ÉS megfigyel
- A kereskedelem reagál a vevők problémái miatt

Coalition Rule: (Céges összefogás)

- Az előírások és compliance hatástalan
- A cégek saját erőforrásaikra támaszkodnak
- Fekete piaci, földalatti kiberkartellek
- Nagy cégek koalíciót és jól védett

Neighborhood Watch: (Emberi összefogás)

- Anarchista jellegű helyzet
- A szabályzás és a kormányzati lépések nem működnek
- E-Polgárőrségek alakulnak a hacktivisták ellen
- Közösségi védelmi csapatok alakulnak

GYÁRTÓK STRATÉGIÁK ÉS MEGKÖZELÍTÉSEK (NÉHÁNY PÉLDA)

- Balabit – Naplózni és SCB már nem elég, komplex megközelítés
- Cisco – Hálózati védelemből a komplex APT védelem felé, Big Data
- Checkpoint – Hálózati szegmentáció és APT kell
- FireEye – Alkalmazás biztonság – APT védelem
- Fortinet – Hálózati biztonságból – alkalmazás biztonságba
- HP – Összetett adatbányászat és elemzés a naplóelemzés helyett
- IBM – Naplóelemzés, Big Data biztonság és ipari biztonság
- Juniper – Big Data, Data Center biztonság
- McAfee – Vírusírtó nem elég, APT védelem és hálózatelemzés kell

T Radware és Arbor – DDoS intelligencia képességek növelése

LEHETŐSÉGEK A NEHÉZSÉGEK KÖZEPETTE IS

- Adatvédelmi kérdéseket lehet kezelni (adatosztályozások, kockázatok, DLP)
- Elérhető árú megoldások a hálózatbiztonságban, napló- és hálózat elemzésben (pl. DDoS, NAC)
- Törvényi megfelelésségért lehet tenni
- Alkalmazások bizt. követelményei!
- Operatív és védelmi szinten: malware képességek, CERT tapasztalatok, „hacker” tudás beszerzése



T-SYSTEMS TAPASZTALATOK MIBS – TÁVFELÜGYELET

- Naponta több száz millió biztonsági esemény feldolgozása
- Havi szinten több mint 20 milliárd esemény
- Az ügyfelek, vállalatok több ezer informatikai eszköze produkálja
- A biztonsági központ szakemberei és etikus hackerei elemzik a nap 24 órájában
- Informatikai betörések, hacker vagy biztonsági incidensek esetén akár



MIBEN TUD SEGÍTENI A T-SYSTEMS VAGY ESETLEG JÓMAGAM?

A biztonságának a T-Systems-nél **6 fő** és **36 szakmai alterülete** van

Ami ma leginkább foglalkoztat minket:

- Adatszivárgás elkerülése (egyedülálló módszertan)
- Napló- és hálózat elemzés, felügyelet és incidens menedzsment
- Alkalmazás biztonság, APT/ Malware
- DDoS támadások elleni szolgáltatás



MIBEN TUD SEGÍTENI A CIVIL SZFÉRA ÉS A SZAKMAI KEZDEMÉNYEZÉSEK?



I N F O R M A T I K A I
B I Z T O N S Á G N A P J A

A régió legnagyobb
ingyenes biztonsági
rendezvénye

2500 szakember, 100
brand, 70 előadás és
workshop, trade show,
kapcsolatépítés, 2 nap



kibev

önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

Civilek a kiberbiztonságért
Magyarország első ilyen
kezdeményezése

Közös munkalehetőség

T · · Systems ·