2014 FIRST Symposium

October 14-16, 2014

Tbilisi

CERT-UA practice in ensuring the country's cybersecurity

Vizniak Roman vrb@cert.gov.ua





What will be discussed?

- •CERT-UA. Who we are and what we do?
- •Incident Response. The main goal to prevent the incident.
- Problem of coordination. Our solutions.

Who fight against cyber threats of GOV organizations in Ukraine?

Security Service of Ukraine



Department of
Counterintelligence
Protection of State's
Interests in the Sphere
of Information Security

State Service of Special Communication and Information protection of Ukraine



State Center of
Protection of
Information and
Telecommunication
Systems

Ministry of Internal Affairs of Ukraine



Department on Combating Cybercrimes

State Center is responsible for:

- National System of Confidential Communication
- System of Protected Internet Access
- Computer Emergency Response Team of Ukraine (CERT-UA)

CERT-UA. Our mission

- to protect government information resources
- to provide security of Ukrainian segment of the Internet

CERT-UA works in 5 sectors:

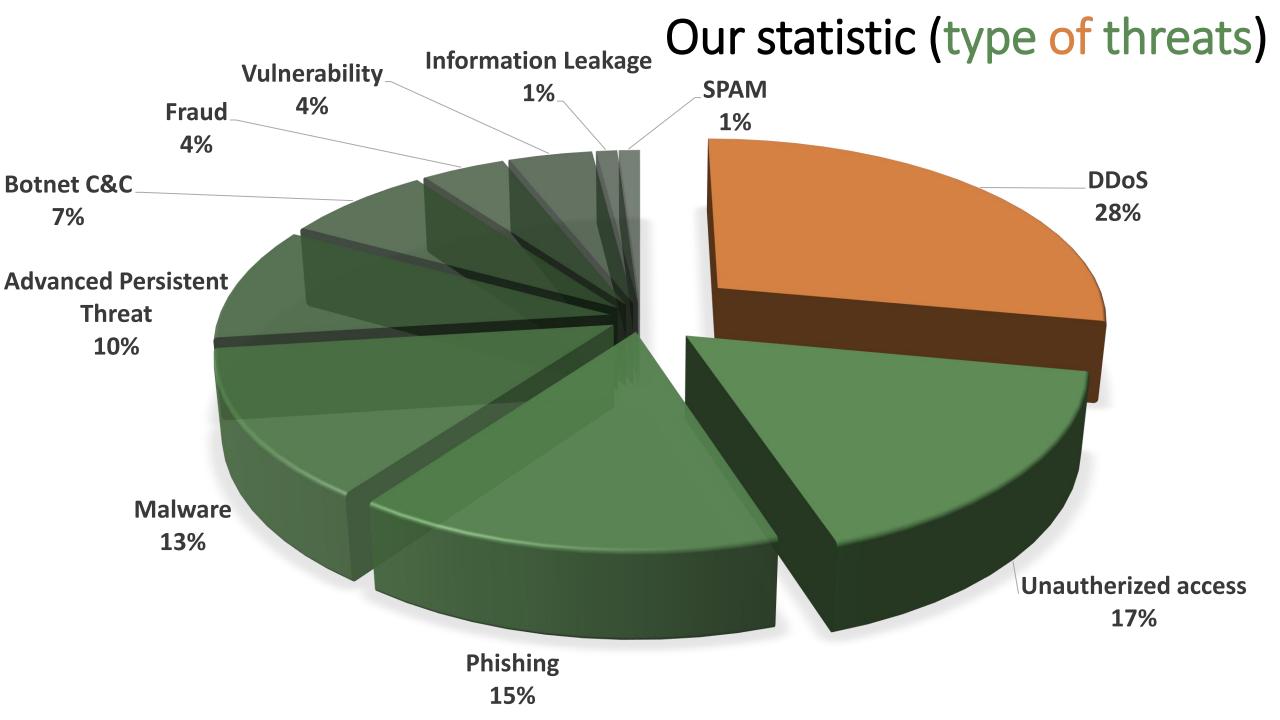
UAGOV

UACTZ

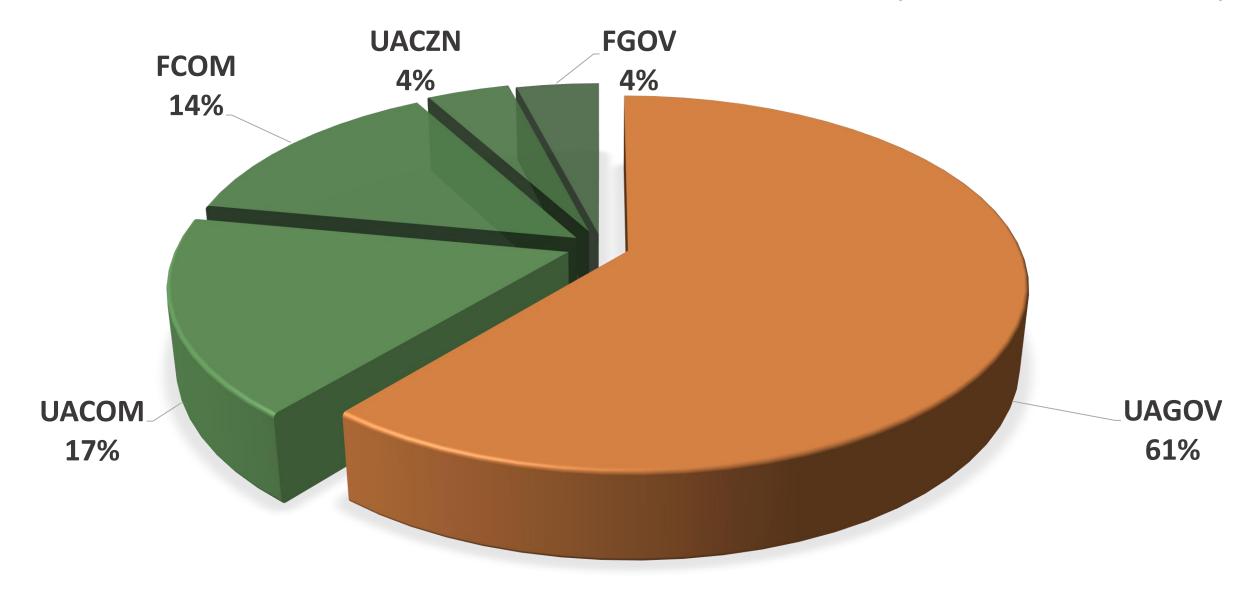
UACOM

FGOV

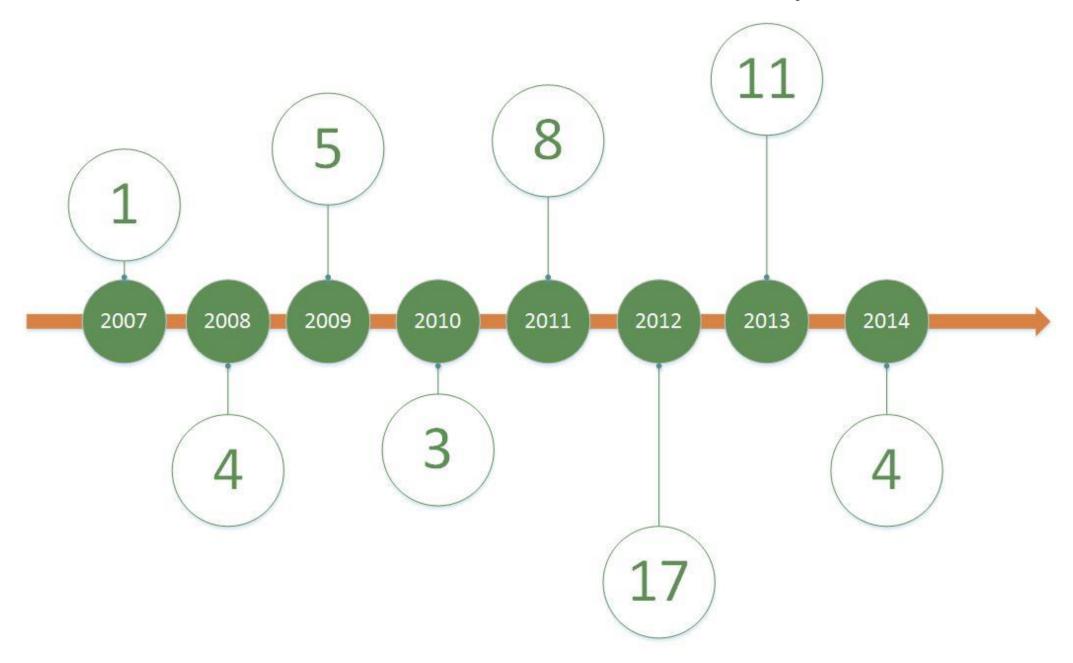
FCOM



Our statistic (attacked zones)



Our statistic (information security audits)



Incident Response. Main steps (RFC 2350)

Incident triage

- Report assessment
- Verification

Incident coordination

- Information categorization
- Coordination

Incident resolution

- Technical Assistance
- Eradication
- Recovery

Coordination problem

We have to:

- try to get some basic info about incident from alternative(trusted) sources
- have much contact information of our ISPs, banks and other organizations (not GOV only)
- try to decentralize monitoring of theirs security status.

Our solutions

- Threat Monitoring System (passive mode)
- IP Guard (interactive system which called to create some kind of dialog between CERT-UA and subjects of information security)

Threat Monitoring System (passive mode)

DB contains info about IPs of compromised devices in UA Internet

Visualization works for UA GOV entities

GOV IPs gathering process:

- 3 official inquiries on behalf of Prime-Minister of Ukraine
- 5 mount for answers and data processing

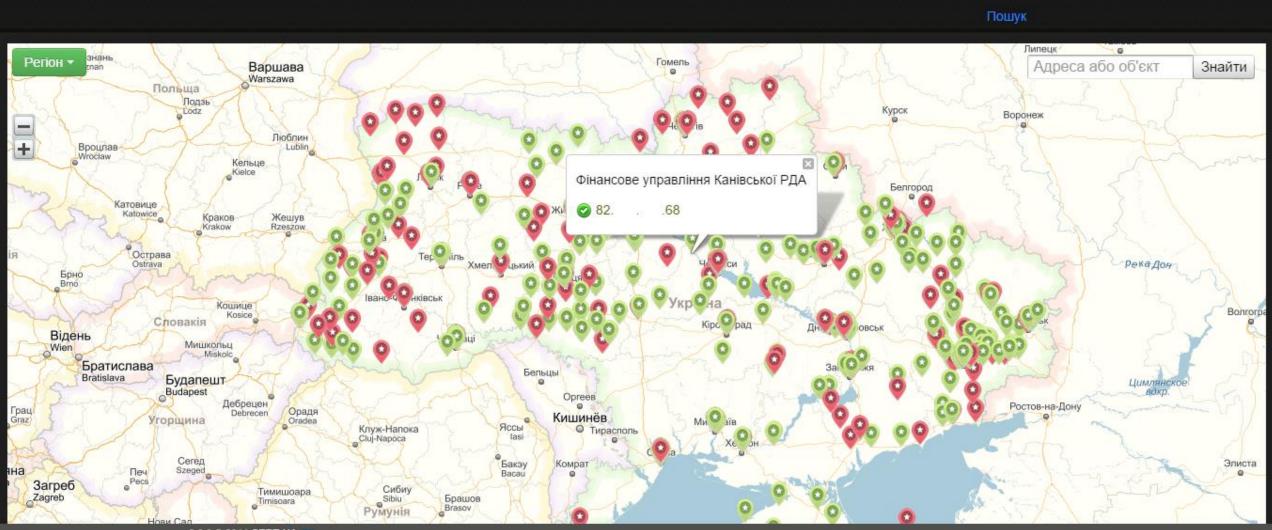
Finally:

Number of	Quantity	
Organizations	1523	411/6
IP-addresses	3045	
Compromised Org	605	
Compromised IPs	586	ARE COMPROMISED

Threat Monitoring System (passive mode)



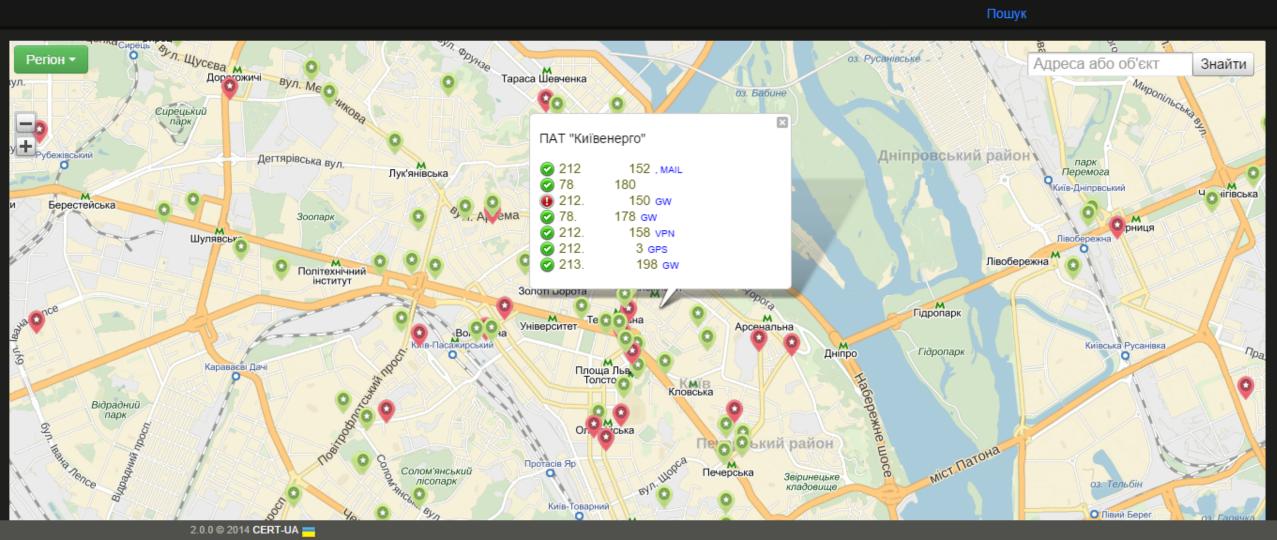
Система пасивного моніторингу загроз



Threat Monitoring System (passive mode)



Система пасивного моніторингу загроз

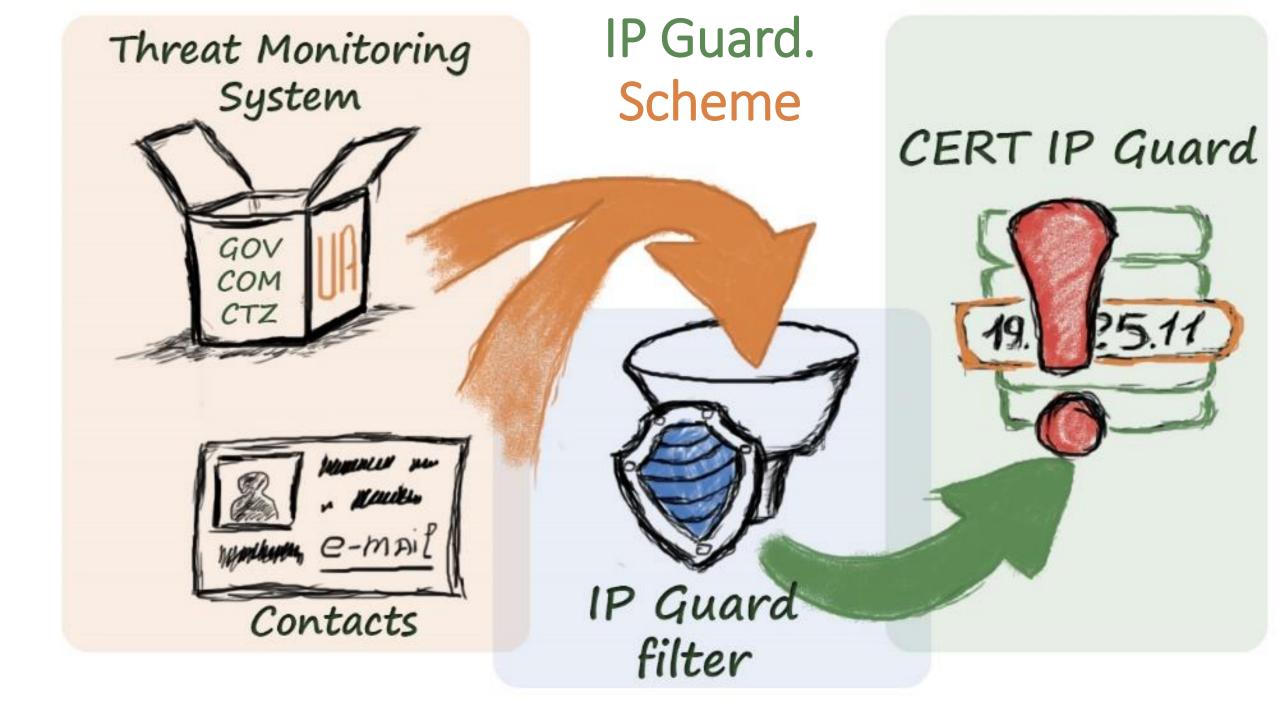


IP Guard. What we have...

Diagram of the system include:

- Threat Monitoring System (include all UA sectors UAGOV, UACOM, UACTZ)
- Information about user of IP Guard (basic info and contacts, which certainly will be checked by CERT-UA members)
- Information about users IPs or some range of IPs, which he interested in.

As a result.. you'll see what we know about requesting IPs



IP Guard. Looks like this

IP Guard bank@domain.com

Мій профіль

Вихід

Звіти 1

Налаштування мережі

Контактні дані

Звіти

Дата	Назва	Зміст звіту	Дії
2014-08-22 07:26:55	Sinkhole-HTTP- Drone	Звіт містить інформацію щодо IP-адрес, з яких генерувалось з'єднання до серверів управління бот- мережами. Процедура отримання контролю над бот-мережею шляхом підміни значень DNS/IP-адреса для серверів, що забезпечували її функціонування, називається «SINKHOLING». Сервери, які підставляються замість серверів зловмисників називається «SINKHOLE».	Детальніше
2014-10-01 19:39:55	Sinkhole-HTTP- Drone	Звіт містить інформацію щодо IP-адрес, з яких генерувалось з'єднання до серверів управління бот- мережами. Процедура отримання контролю над бот-мережею шляхом підміни значень DNS/IP-адреса для серверів, що забезпечували її функціонування, називається «SINKHOLING». Сервери, які підставляються замість серверів зловмисників називається «SINKHOLE».	Детальніше
2014-09-18 07:26:55	Sinkhole-HTTP- Drone	Звіт містить інформацію щодо IP-адрес, з яких генерувалось з'єднання до серверів управління бот- мережами. Процедура отримання контролю над бот-мережею шляхом підміни значень DNS/IP-адреса для серверів, що забезпечували її функціонування, називається «SINKHOLING». Сервери, які підставляються замість серверів зловмисників називається «SINKHOLE».	Детальніше
2014-09-18 07:26:55	Sinkhole-HTTP- Drone	Звіт містить інформацію щодо IP-адрес, з яких генерувалось з'єднання до серверів управління бот- мережами. Процедура отримання контролю над бот-мережею шляхом підміни значень DNS/IP-адреса для серверів, що забезпечували її функціонування, називається «SINKHOLING». Сервери, які підставляються замість серверів зловмисників називається «SINKHOLE».	Детальніше
2014-09-18 07:26:55	Sinkhole-HTTP- Drone	Звіт містить інформацію щодо IP-адрес, з яких генерувалось з'єднання до серверів управління бот- мережами. Процедура отримання контролю над бот-мережею шляхом підміни значень DNS/IP-адреса для серверів, що забезпечували її функціонування, називається «SINKHOLING». Сервери, які підставляються замість серверів зловмисників називається «SINKHOLE».	Детальніше
« 1 2 »			CERT-U

What we are trying to achieve. Global

- Raise coordination level
- Raise awareness level in information security of each citizen of Ukraine.

What we are trying to achieve. Developing

- Add some visualization to IP Guard (some statistic)
- Bring some mobility to IP Guard
- Try to make our Internet safer

THANKS A LOT FOR YOUR ATTENTION

CERT-UA

Roman Vizniak vrb@cert.gov.ua