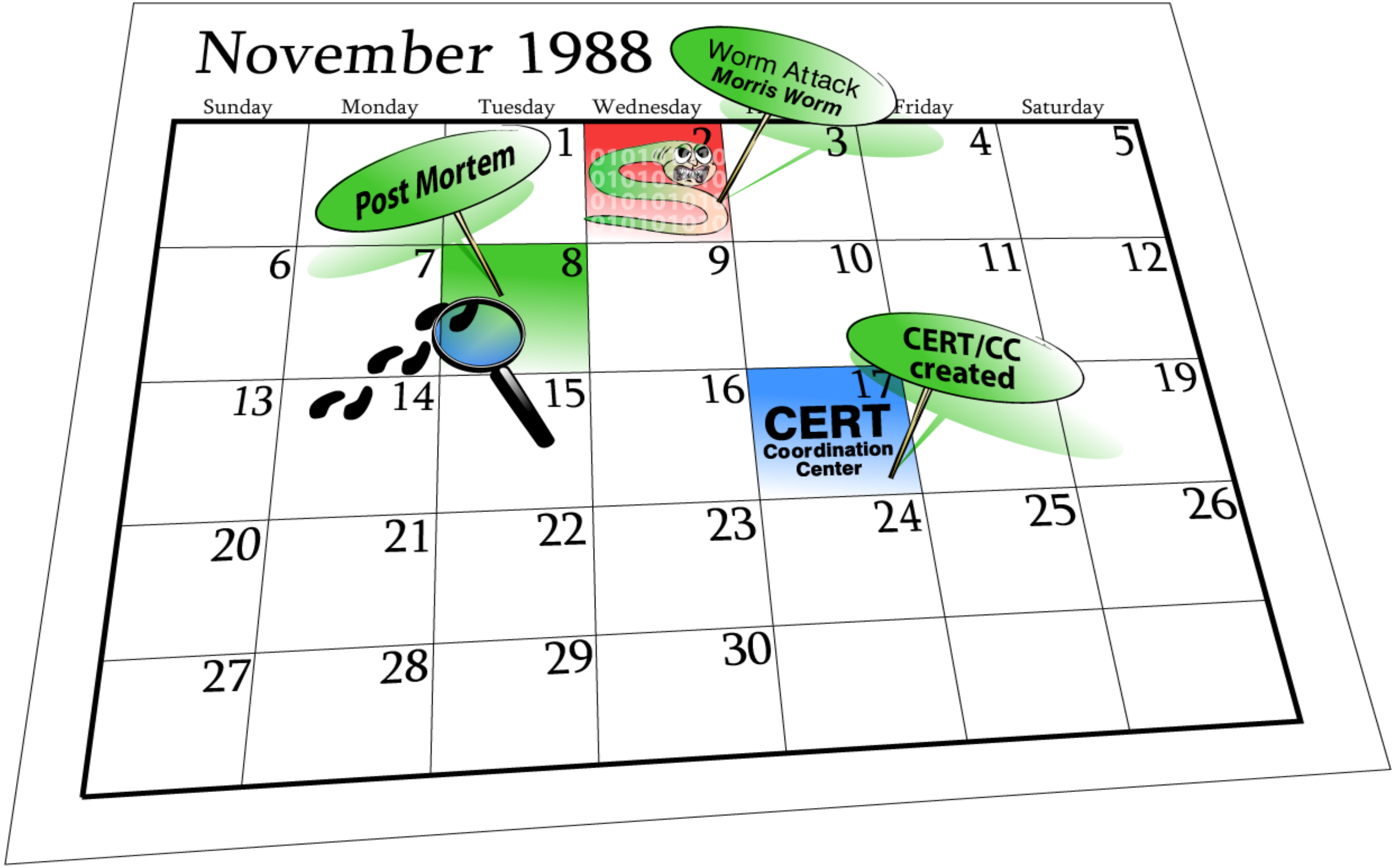
Perspectives of incident response practitioner

Koichiro Sparky Komiyama
Global Coordination Division
JPCERT/CC

Jan 24, 2019 ECSO-EUNITY Workshop, Brussels

Morris Worm and the first CSIRT was made



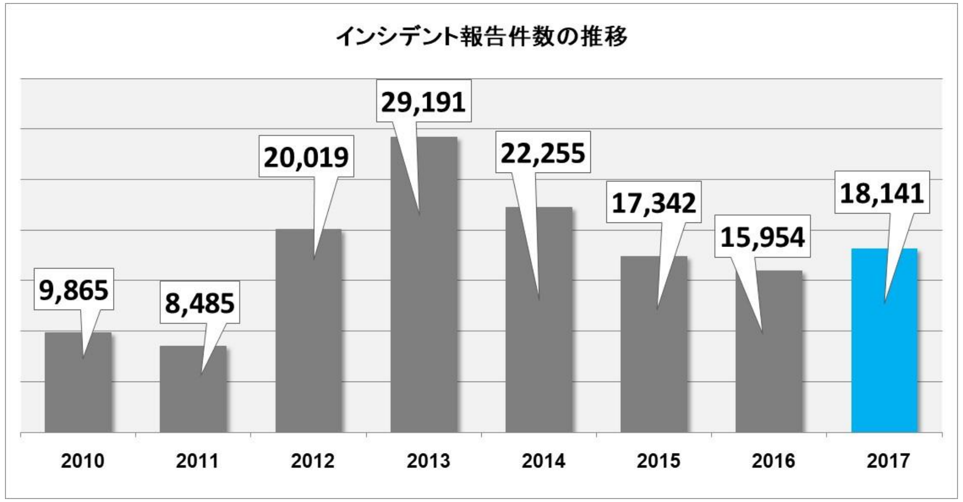
CSIRT’s mission

- Provides a single point of contact (POC)
  - info@jpcert.or.jp for reporting incident
  - office@jpcert.or.jp for general contact
- Assists the constituency and community in preventing and handling computer security incidents
- Share information and lesson learned with other CSIRT / response teams and appropriate organizations and sites.

No Accreditation or Certification body for CSIRT

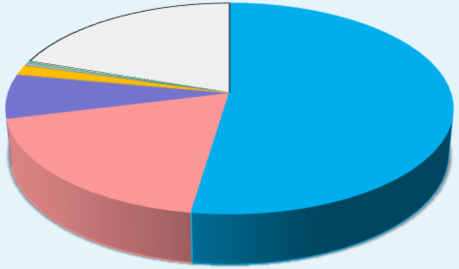
Incidents（Apr 2017 - Mar 2018）

- Reported Incidents
  - Incoming Report
    18,141
  - Incoming Incidents
    18,768
- Coordinated Incidents
  8,891



Source:
https://www.jpcert.or.jp/ir/report.html

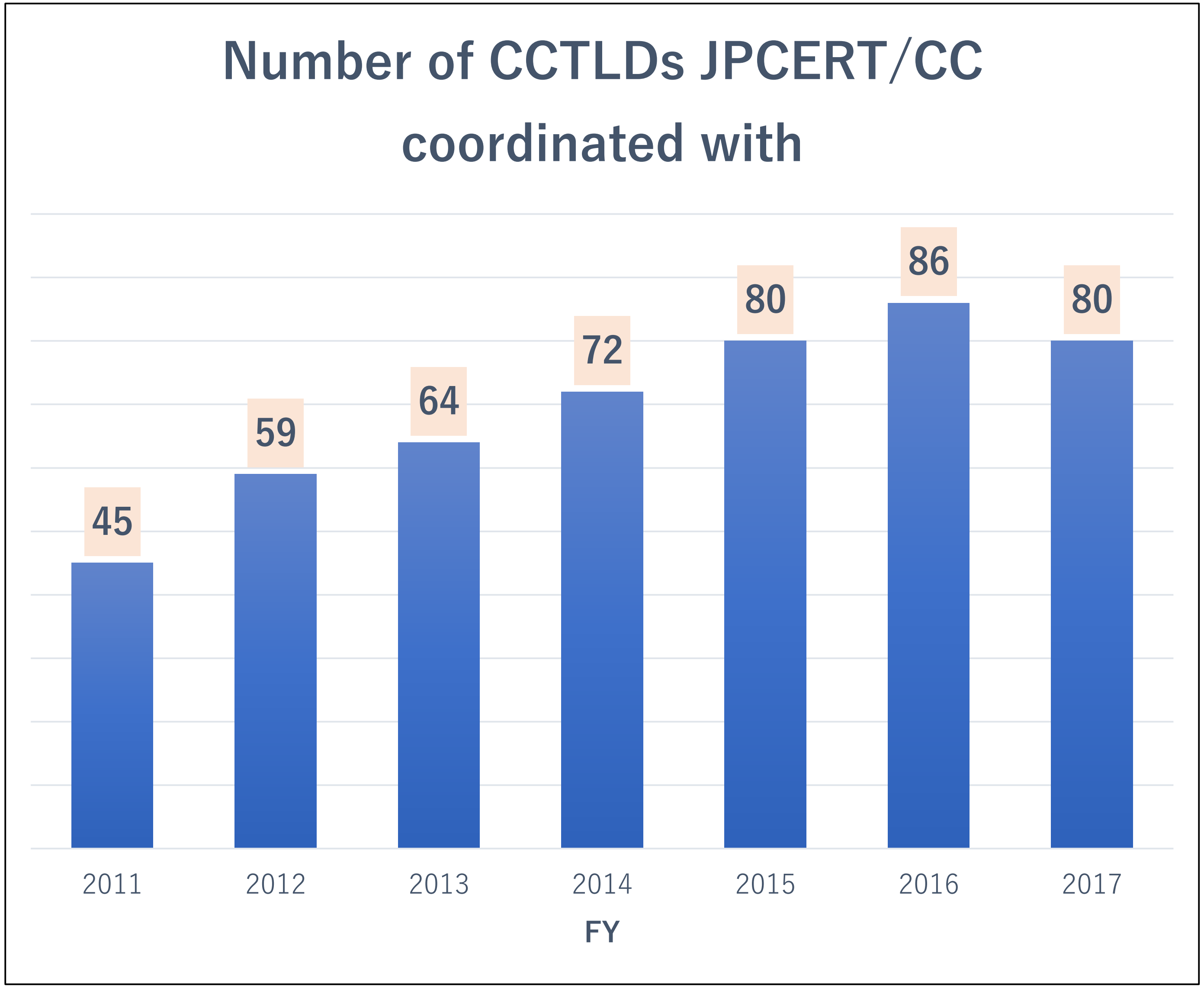
Incidents by Category



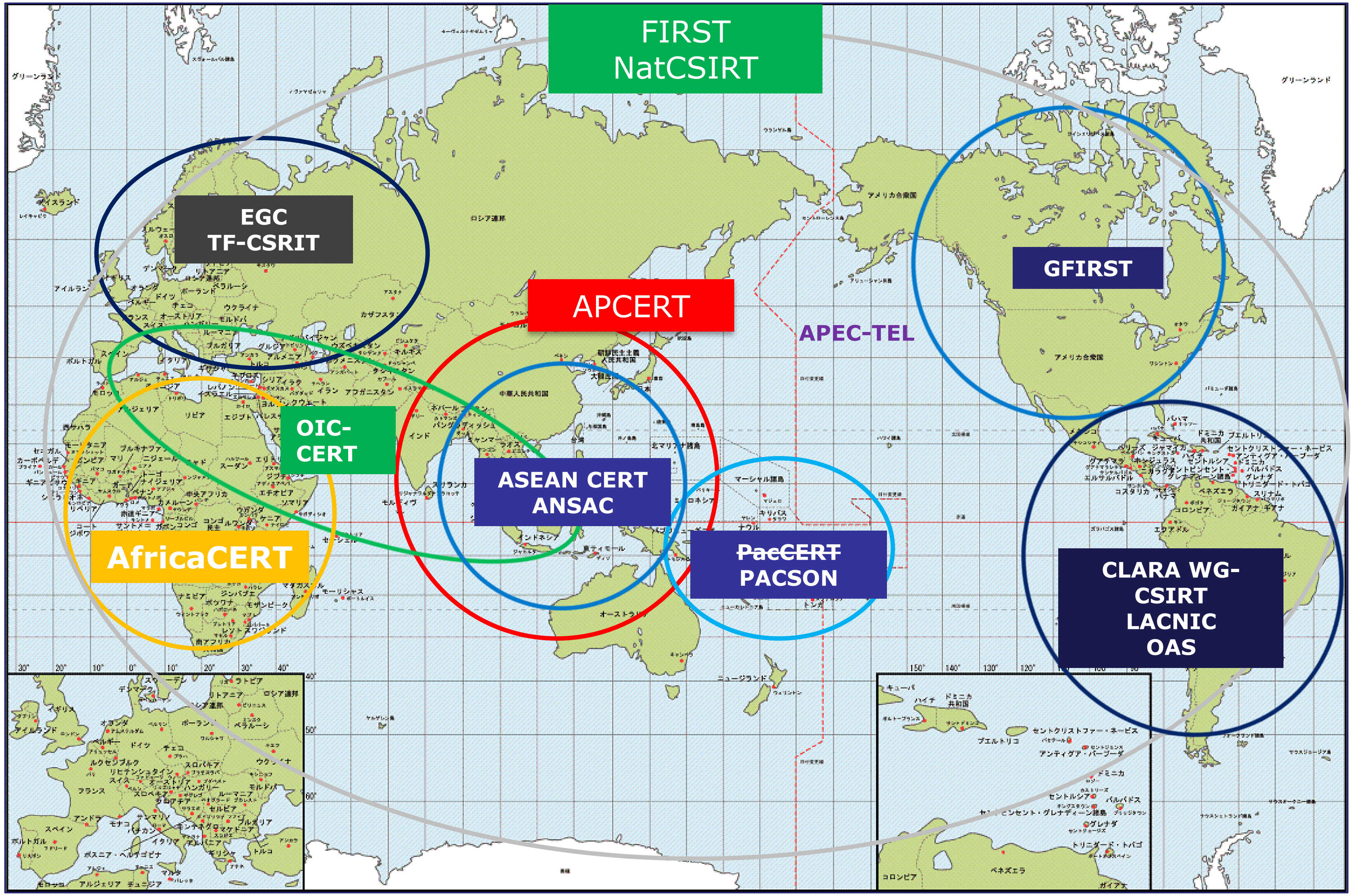
Category	Ratio
Scan	52.3%
Web Defacement	6.7%
Phishing	18.8%
Malware	1.6%
DoS / DDoS	0.1%
APT/Targeted Attack	0.2%
Control system	0.4%
Misc	19.8%

Wide range of cooperation (per CCTLD)

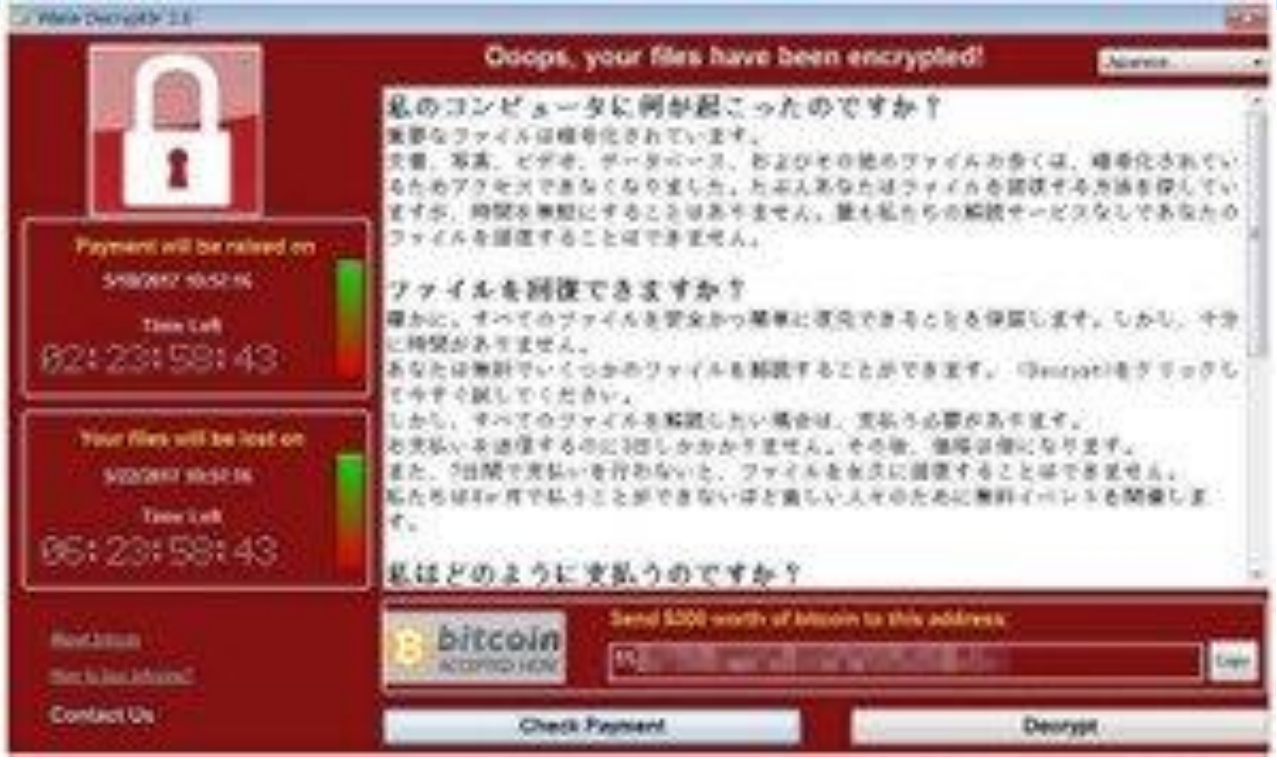
- Coordinated with 130 countries during last 7 years
- Composition?
  1. US
  2. China
  3. Hongkong
  4. Germany
  5. Taiwan
  6. Brazil
  7. Singapore
  8. France



International and Regional Collaborative Activities



Challenge 1: Role of Tech community for Attribution



Ooops, your files have been encrypted!

私のコンピュータに何が起こったのですか？

重要なファイルは暗号化されています。

文書、写真、ビデオ、データベース、およびその他のファイルの多くは、暗号化されているためアクセスできなくなりました。たぶんあなたはファイルを回復する方法を探していますが、時間を無駄にすることはありません。誰も私たちの解読サービスなしであなたのファイルを回復することはできません。

ファイルを回復できますか？

確かに。すべてのファイルを安全かつ簡単に復元できることを保証します。しかし、十分に時間がありません。

あなたは無料でいくつかのファイルを解読することができます。<Decrypt>をクリックして今すぐ試してください。

しかし、すべてのファイルを解読したい場合は、支払う必要があります。

お支払いを送信するのに3日しかかかりません。その後、価格は倍になります。

また、7日間で支払いを行わないと、ファイルを永久に回復することはできません。

私たちは6ヶ月で払うことができないほど貧しい人々のために無料イベントを開催します。

私はどのように支払うのですか？

Payment will be raised on

5/18/2017 10:52:16

Time Left

02:23:58:43

Your files will be lost on

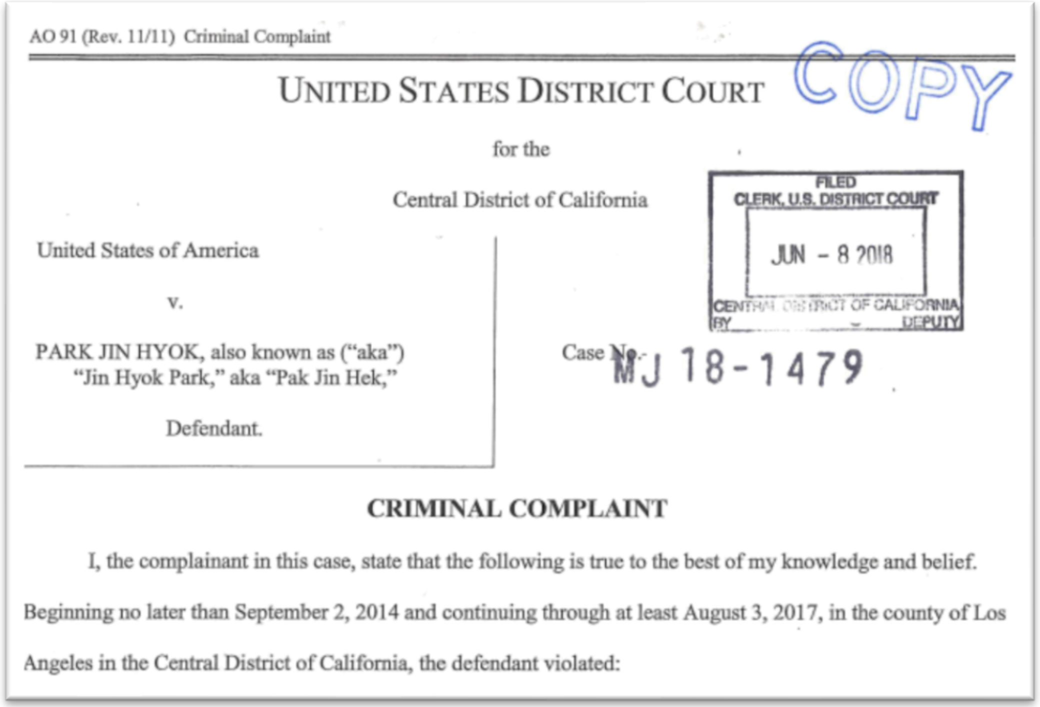
5/22/2017 10:52:16

Time Left

06:23:58:43

Send $300 worth of bitcoin to this address:

bitcoin
ACCEPTED HERE
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt



AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Central District of California

COPY

FILED
CLERK, U.S. DISTRICT COURT
JUN - 8 2018
CENTRAL DISTRICT OF CALIFORNIA
BY ________ DEPUTY

United States of America

v.

PARK JIN HYOK, also known as ("aka")
"Jin Hyok Park," aka "Pak Jin Hek,"

Defendant.

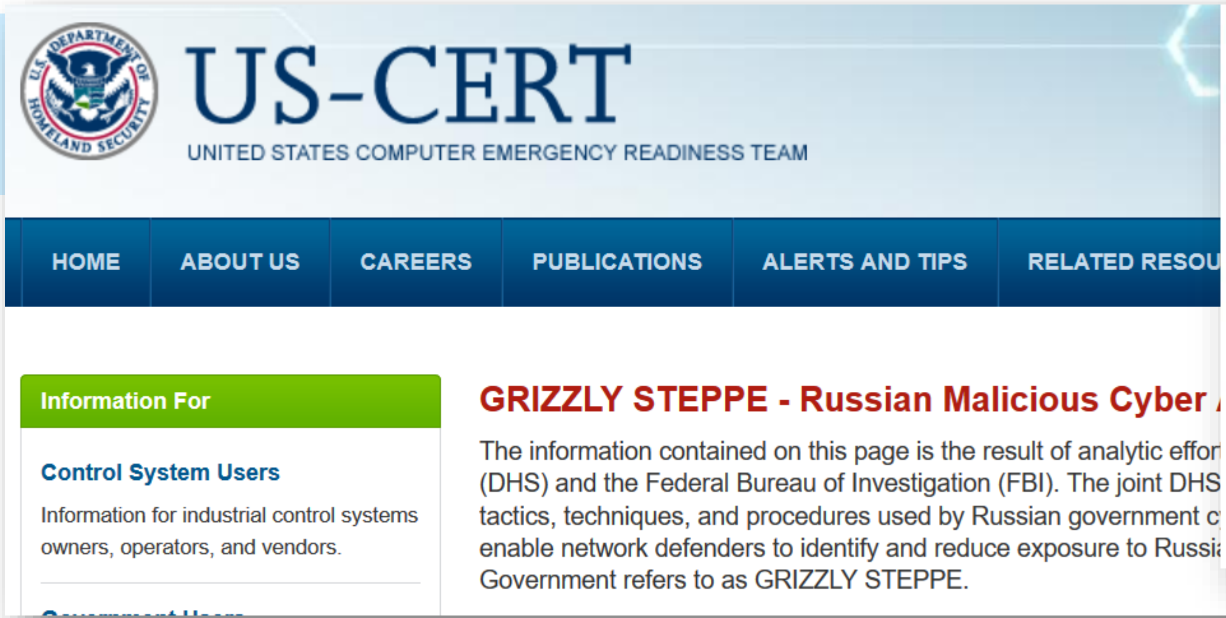
Case No. MJ 18-1479

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los Angeles in the Central District of California, the defendant violated:

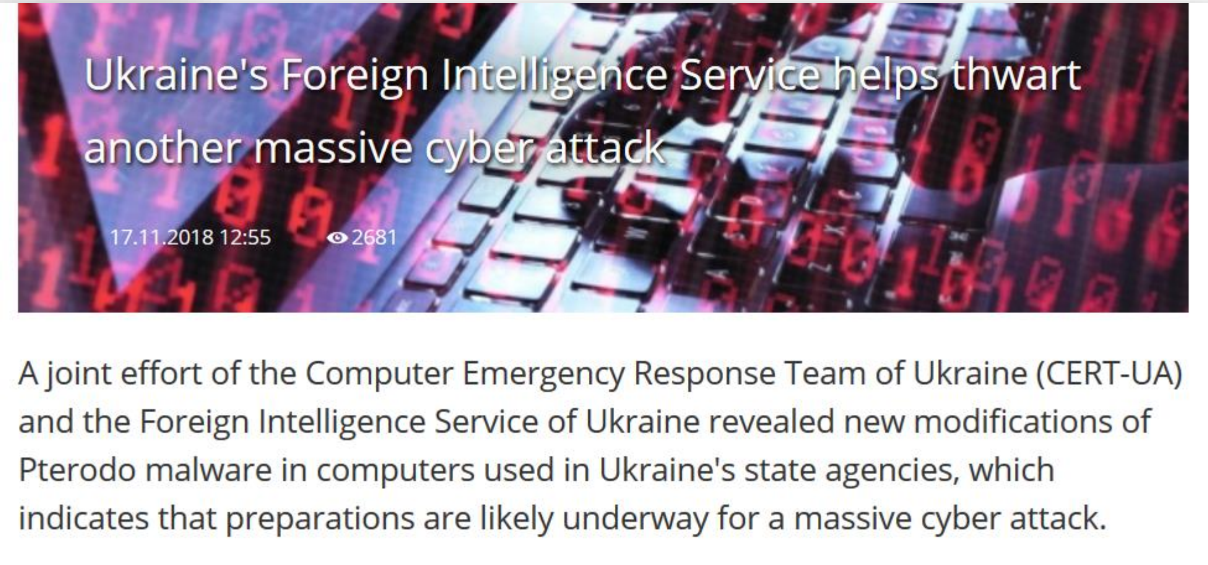
DOJ criminal complaint against an alleged spy for the North Korean goverment



Information for industrial control systems owners, operators, and vendors.

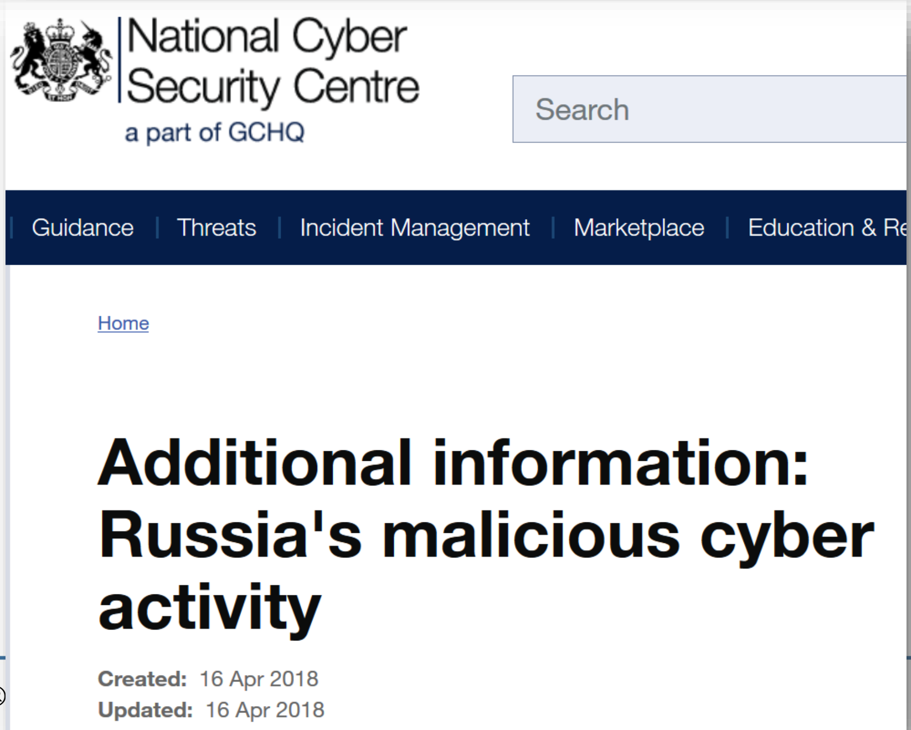
GRIZZLY STEPPE - Russian Malicious Cyber

The information contained on this page is the result of analytic effor (DHS) and the Federal Bureau of Investigation (FBI). The joint DHS tactics, techniques, and procedures used by Russian government c enable network defenders to identify and reduce exposure to Russi Government refers to as GRIZZLY STEPPE.



Ukraine's Foreign Intelligence Service helps thwart another massive cyber attack

A joint effort of the Computer Emergency Response Team of Ukraine (CERT-UA) and the Foreign Intelligence Service of Ukraine revealed new modifications of Pterodo malware in computers used in Ukraine's state agencies, which indicates that preparations are likely underway for a massive cyber attack.

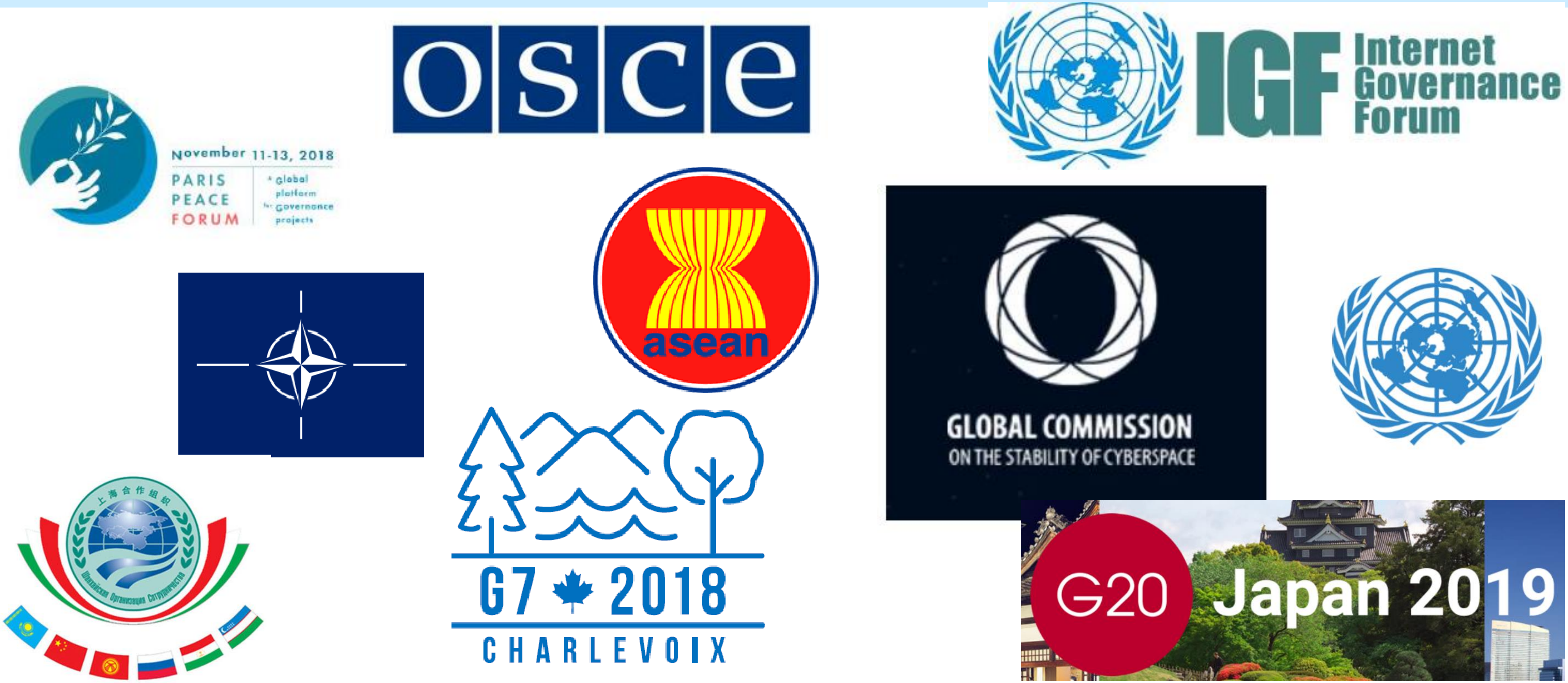


Additional information: Russia's malicious cyber activity

Created: 16 Apr 2018
Updated: 16 Apr 2018

- CSIRTs are accusing others

Challenge 2: Normative approach


osce
IGF Internet Governance Forum
November 11-13, 2018
PARIS PEACE FORUM
a global platform for governance projects
asean
GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE
上海合作组织
Шанхайская Организация Сотрудничества
G7 2018
CHARLEVOIX
G20 Japan 2019

Challenge 2: Normative approach

- 11 recommendation of UNGGE Report (July 2015)
  - (k) States should not conduct or knowingly support activity to harm the information systems CSIRTs of another State.
  - State should not use CSIRTs to engage in malicious international activity.

(Photo by Andrew Burton/Getty

Our Future

- Information sharing among CERTs/CSIRTs will become harder
- Shared value, individual trust is key to overcome