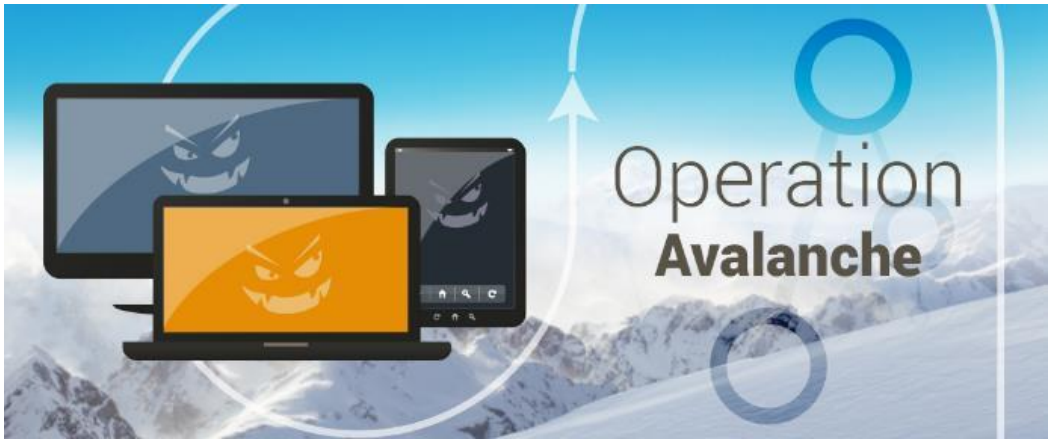
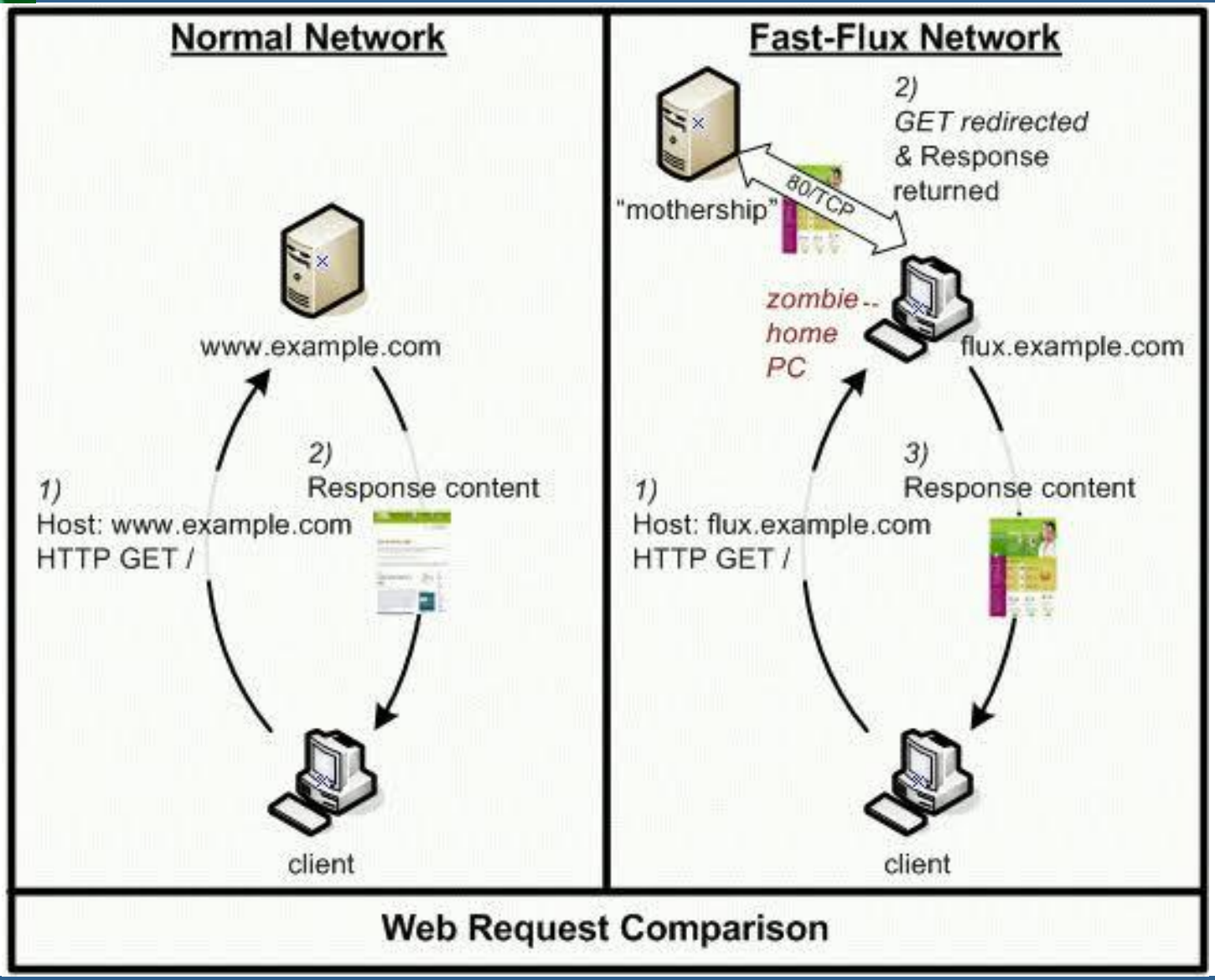
AFRICAN FORUM ON CYBERCRIME

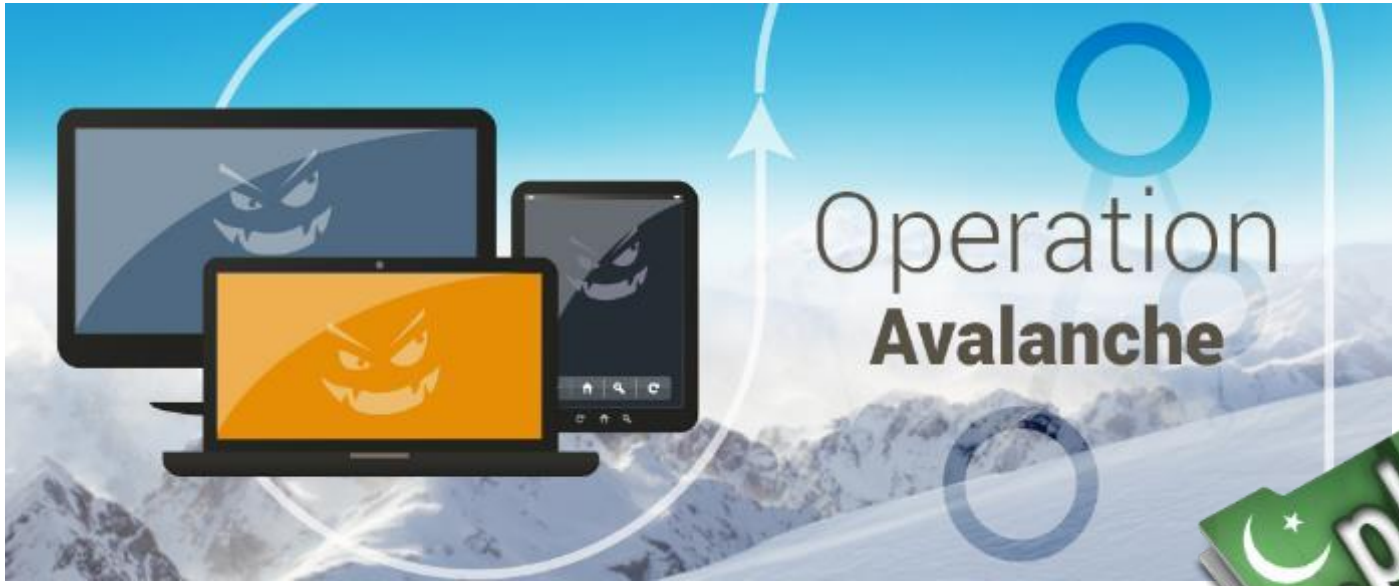
Operation Avalanche



Zahid Jamil
Council of Europe

Addis Ababa – 17 October 2018


Normal Network
www.example.com
1)
Host: www.example.com
HTTP GET /
2)
Response content
client
Fast-Flux Network
"mothership"
2)
GET redirected
& Response
returned
80/TCP
zombie --
home
PC
flux.example.com
1)
Host: flux.example.com
HTTP GET /
3)
Response content
client
Web Request Comparison


Operation
Avalanche

- **30 countries - Prosecutors & Investigators**
- **5 arrested**
- 37 premises searched
- **39 servers seized**
- Over 180 countries Victims of malware identified
- ***221 servers offline***
- (abuse notifications to hosting providers)

- ***Over 800 000 domains seized, sinkholed or blocked***
- Largest-ever use of sinkholing to combat botnet infrastructures
- unprecedented in scale

FIGURES AT A GLANCE

Countries involved: Armenia, Australia, Austria, Azerbaijan, Belgium, Belize, Bulgaria, Canada, Colombia, Finland, France, Germany, Gibraltar, Hungary, India, Italy, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Norway, Poland, Romania, Singapore, Sweden, Taiwan, Ukraine, United Kingdom and United States of America.

Arrests: **5**
Searches conducted: **37**
Servers seized: **39**
Servers taken offline through abuse notifications: **221**

PKNIC

401 domains

399 blocked

2 seized

8 sampled

Lessons Learned

- Some Foreign LEAs cannot contact Cybercrime Unit without going through:
  - Ministry of Foreign Affairs
  - Ministry of Interior
  - DG FIA
- No private sector cooperation
- No relationships or MoUs (legal request vs cooperation)
- Problems could have been avoided if for international cooperation there were:
  - Existing protocols between law enforcement (bypassing bureaucracy)
  - SPOCs
  - Permanent MAG

- Jurisdiction
- Fear of Local LEA future abuse
- Confidentiality
- Future basis for cooperation – Trust created

- Interagency/Interdisciplinary/Public-Private/Transborder

- Operation Avalanche impossible through formal means of cooperation

- Court order required seizure of data that did not even exist at the time of the order

- No mechanisms for accepting such a request under Pakistan law – possible only due to cross-border cooperation with private sector

- Cross-border interagency cooperation poses challenges with respect to proving authenticity of information received, particularly with respect to ensuring chain of custody

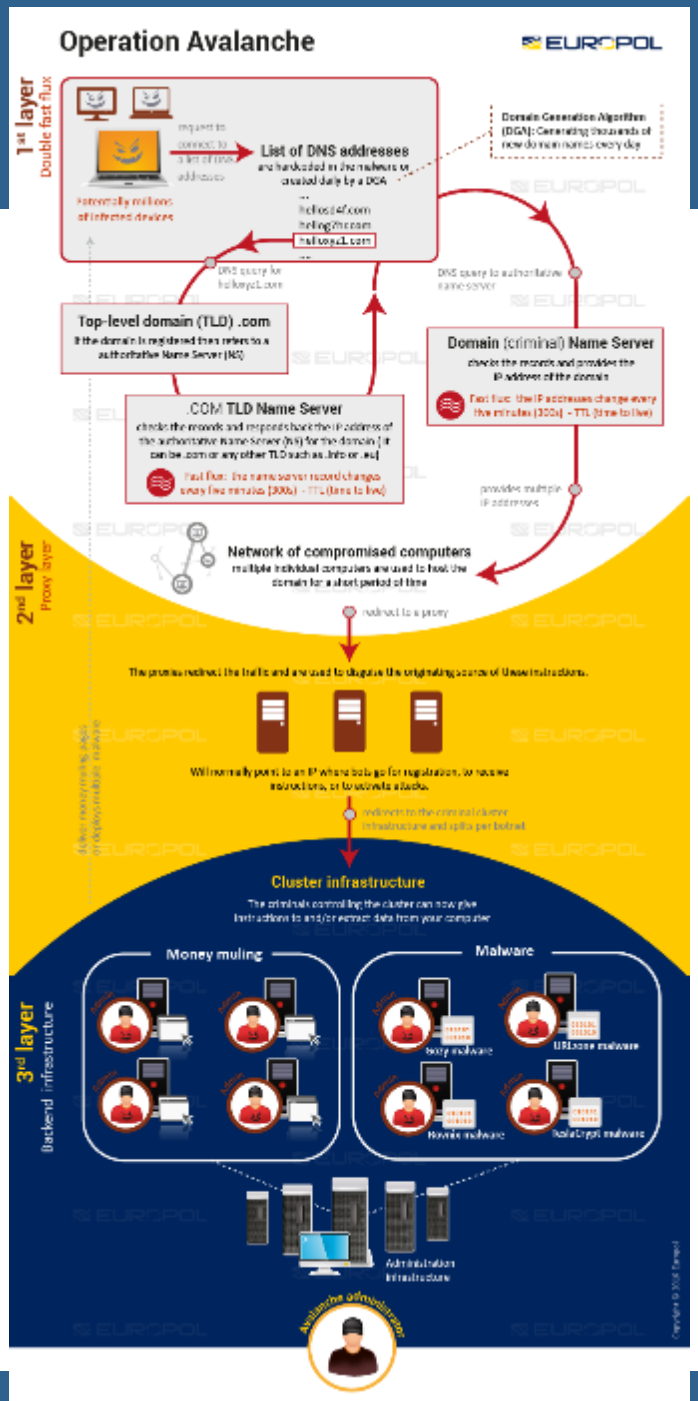
- Many MLATs are not designed for cooperation with respect to cybercrime (requests of which are usually urgent)

- **Julian King, European Commissioner for the Security Union:**

"Avalanche shows that we can only be successful in combating cybercrime when we ***work closely together, across sectors and across borders***. ***Cybersecurity and law enforcement authorities*** need to work hand in hand with the ***private sector*** to tackle continuously evolving criminal methods. The EU helps by ensuring that the right legal frameworks are in place to enable such cooperation on a daily basis".

- **Rob Wainwright, Europol Director:**

"Avalanche has been a highly significant operation involving ***international law enforcement, prosecutors and industry resources*** to tackle the global nature of cybercrime. The complex trans-national nature of cyber investigations requires international ***cooperation between public and private organisations*** at an unprecedented level to successfully impact on top-level cybercriminals. Avalanche has shown that through this cooperation we can collectively make the internet a safer place for our businesses and citizens".


Operation Avalanche
EUROPOL
1st layer
Double fast flux
List of DNS addresses
Domain Generation Algorithm (DGA): Generating thousands of new domain names every day
Top-level domain (TLD) .com
Domain (criminal) Name Server
.COM TLD Name Server
2nd layer
Proxy layer
Network of compromised computers
Cluster infrastructure
3rd layer
Backend infrastructure
Money muling
Malware
Administration infrastructure
Avalanche administrator

Operation Avalanche

EUROPOL

1st layer
Double fast flux

Potentially millions of infected devices connected to the internet request to connect to a list of addresses

Computers connected to the Internet use name servers to resolve human readable domain names into the IP addresses used to route the IP network traffic (e.g. www.europol.europa.eu has the following IP: 158.169.131.22). **Usually one domain is delegated to one IP address for a long period of time.**

A Domain Generation Algorithm (DGA) generates thousands of new domain names every day

hellosd4f.com, hellog7hr.com, helloxyz1.com, ...

request to connect

The Avalanche platform uses a complex system of **Double Fast Flux** networks and layers of proxy servers to rapidly change the apparent location of IP address records from a domain and the name servers that resolve it, with the aim of making it more difficult for Law Enforcement to trace and take down hosted criminal infrastructures.

Name Server
is used to resolve the domain name

Fast Flux: the name server record changes every five minutes (300s) - TTL (time to live)

The technique known as Fast Flux involves automatically and frequently changing the IP address records associated with a domain name. Single Fast Flux changes the IP address used to host address records associated with a domain (such as a website name). **Double Fast Flux changes both the IP address records and the name server that is used to resolve the domain** too.

IP Address Record
provides the IP address of the domain

Fast Flux: the IP addresses change every five minutes (300s) - TTL (time to live)

2nd layer
Proxy layer

Network of compromised computers
multiple individual computers are used to host the domain for a short period of time

redirect to a proxy

domain and the name servers that resolve it, with the aim of making it more difficult for Law Enforcement to trace and take down hosted criminal infrastructures.

Name Server

is used to resolve the domain name

Fast Flux: the name server record changes every five minutes (300s) - TTL (time to live)

The technique known as Fast Flux involves automatically and frequently changing the IP address records associated with a domain name. Single Fast Flux changes the IP address used to host address records associated with a domain (such as a website name). **Double Fast Flux changes both the IP address records and the name server that is used to resolve the domain** too.

IP Address Record

provides the IP address of the domain

Fast Flux: the IP addresses change every five minutes (300s) - TTL (time to live)

2nd layer
Proxy layer

Network of compromised computers

multiple individual computers are used to host the domain for a short period of time

redirect to a proxy

The proxies redirect the traffic and are used to disguise the originating source of these instructions.

Will normally point to an IP where bots go for registration, to receive instructions, or to activate attacks.

redirects to the criminal cluster infrastructure and splits per botnet

deliver money muling pages
or deploys multiple malware

Cluster infrastructure

The criminals controlling the cluster can now give

deliver money
or deploys m

redirects to the criminal cluster
infrastructure and splits per botnet

Cluster infrastructure

The criminals controlling the cluster can now give
instructions to and/or extract data from your computer

3rd layer
Backend infrastructure

Money muling

Malware

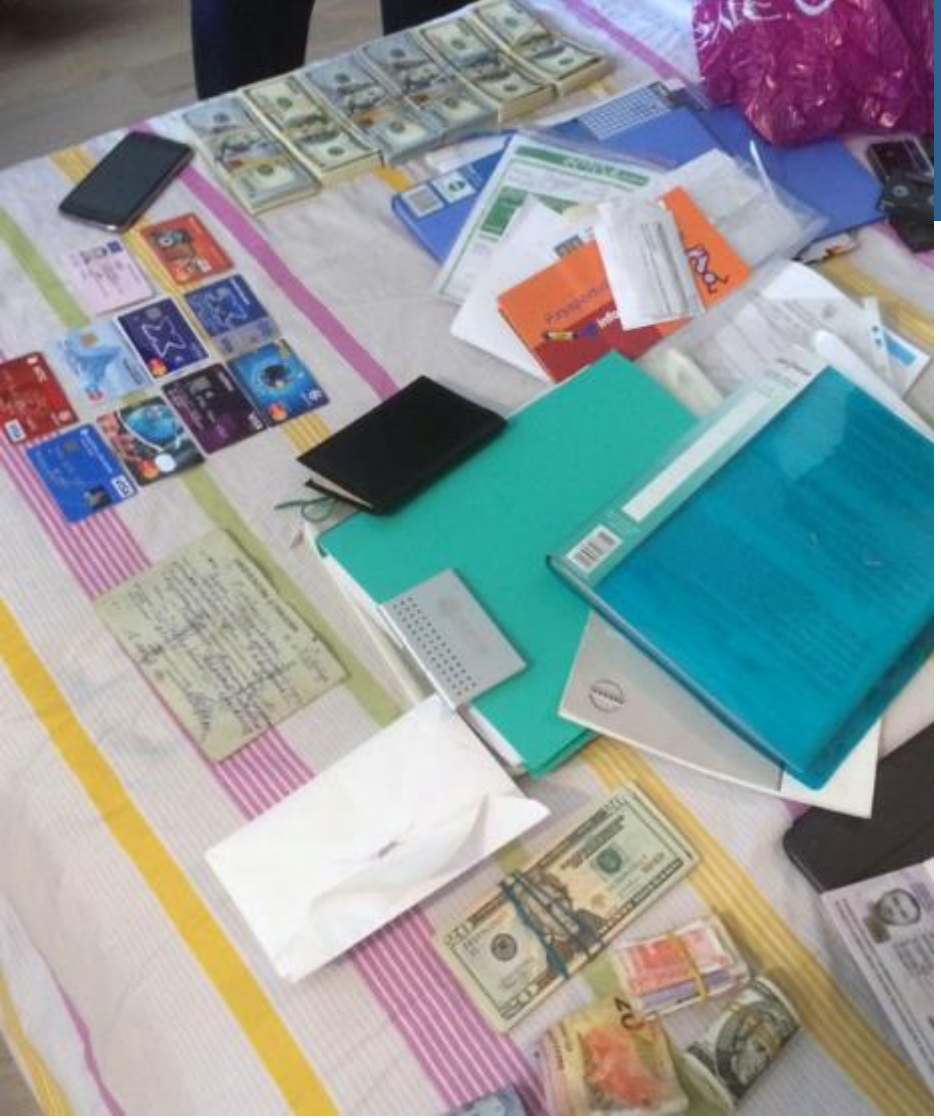
Administration
infrastructure

Sinkholing

is an action whereby ***traffic*** between infected computers and a criminal infrastructure is ***redirected to servers controlled by law enforcement*** authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses.

When employed at a ***100% scale, infected computers can no longer reach the criminal command and control computer systems*** and so criminals can ***no longer control the infected computers***.

The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and Network Owners.



Bulgarian extradited to Pittsburgh as part of malware investigation

December 12, 2016 5:03 PM

By Torsten Ove / Pittsburgh Post-Gazette

A Bulgarian national appeared in federal court this afternoon for an initial hearing on charges related to using malware that was part of the Avalanche network dismantled recently by the FBI and its international counterparts.

Krasimir Nikolov, 44, of Varna, Bulgaria, is the first person to be named in the Pittsburgh district in that investigation, announced last week by the U.S. attorney's office and the Pittsburgh FBI.

Mr. Nikolov, who appeared before a federal magistrate with a translator, is charged with conspiracy, unauthorized use of a computer to obtain financial data and three counts of bank fraud.

U.S. marshals extradited him to Pittsburgh from Bulgaria on Saturday night, and he remains in the county jail pending a detention hearing Dec. 19.

The underlying case remained under seal this afternoon, but the U.S. attorney's office said Mr. Nikolov used a malware package called GozNym that is designed to steal banking information from infected computers. Among GozNym's victims were a bolt-manufacturing company in Carnegie and a New Castle paving business.

GozNym was among several types of malware hosted on the Avalanche network, a platform for the distribution of malware to criminals who bought it so they could infect computers and try to steal money from business bank accounts.

Federal prosecutors said last week that the Avalanche group operated since 2010 and infected at least a half-million computers around the world.

At least week's press conference, Soo Song, the acting U.S. attorney, said five people had been arrested as a result of the investigation and were being held in the countries of their origin.

SUBSCRIBE | ABOUT | RSS

cyberscoop

BRO

GOVERNMENT | TRANSPORTATION | HEALTHCARE | TECHNOLOGY | FINANCIAL | WATCH | LISTEN

Bulgarian hacker charged in million-dollar malware scheme

Prosecutor's Office Paid Bitcoin Ransom in Cyberattack

By JOE MANDAK, ASSOCIATED PRESS ·
PITTSBURGH — Dec 5, 2016, 6:56 PM ET

A state prosecutor's office in Pennsylvania was among hundreds of thousands of victims of a now-shuttered international cybercrime operation, paying nearly $1,400 in a bitcoin ransom to free up its infected computer network, authorities disclosed Monday.

Federal prosecutors said in court documents only that an unidentified state government entity had been victimized by the ring known as the Avalanche network. But the Allegheny County district attorney, Stephen Zappala Jr., confirmed to The Associated Press that it was his office.

The disabling of the Avalanche network by the European Union and U.S. authorities was announced last week in Europe. Federal documents unsealed in Pittsburgh on Monday provided additional details.

The Avalanche group had operated since at least 2010 and infected at least 500,000 computers worldwide, said Soo Song, acting U.S. Attorney in Pittsburgh.

"The takedown of Avalanche was unprecedented in its scope, scale, reach and level of cooperation among 40 countries," Song said.

Avalanche was a platform to distribute malware to people who wanted to buy it and use it to infect the computers of people and businesses.

In general, there were two broad types of malware. One was used to steal online banking information from computers so people known as "money mules" could transfer funds from those victims to overseas banks. The other was ransomware, which locks up a computer network until the victim agrees to pay a ransom.

The prosecutor's office was hit by ransomware in January 2015 when an employee clicked on a link embedded in phishing email, Zappala said. Phishing is a process computer hackers use to try to get people to unwittingly install malware on their

Feds: Business lost $387,500 in world cybercrime operation

December 5, 2016 by Joe Mandak

Credit: George Hodan/Public Domain

A Pennsylvania business lost more than $387,000 in an international cybercrime operation disabled by federal authorities and the European Union last week.

Federal prosecutors and FBI agents in Pittsburgh on Monday plan to offer more details from last week's sweep of the Avalanche network. The group is accused of inflicting hundreds of millions of dollars in losses worldwide before it was dismantled and five key suspects were arrested.

Documents unsealed Monday show a business in Carnegie lost $387,500 when someone drained the money from the company's online account.

Another business in New Castle was twice targeted with unsuccessful efforts to steal more than $120,000.

The U.S. Department of Justice has accused the network of hosting some of the world's most pernicious malware as well as several money laundering campaigns.

Explore further: Police make 5 arrests in 'unprecedented' cybercrime takedown

Department of Justice

U.S. Attorney's Office

Western District of Pennsylvania

SHARE

FOR IMMEDIATE RELEASE

Monday, December 12, 2016

Bulgarian Charged with GozNym Malware Attacks in the U.S.

PITTSBURGH – A Bulgarian man has been indicted by a federal grand jury in Pittsburgh in connection with a sophisticated malware package known as GozNym, designed to steal banking credentials and other confidential personal information from infected computers, Acting United States Attorney Soo C. Song announced today.

The six-count indictment, returned on Oct. 4, 2016, and unsealed today, named Krasimir Nikolov, age 44, of Varna, Bulgaria, as the sole defendant. Count One charges Nikolov with criminal conspiracy; Count Two charges unauthorized access of a computer to obtain financial information; and Counts Three through Six charge bank fraud. The indictment alleges that Nikolov acquired victims' stolen banking credentials through GozNym malware infections of victims' computers to gain unauthorized access to victims' online bank accounts from which electronic funds transfers were issued or attempted to be issued.

According to Acting U.S. Attorney Song, GozNym malware has been used to target private businesses and

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	Criminal No. 16-218
	)	**[UNDER SEAL]**
v.	)	(18 U.S.C. §§ 371, 1030(a)(2)(A),
	)	1030(c)(2)(B)(i), 1344, and 2)
KRASIMIR NIKOLOV	)	

FILED

OCT - 4 2016

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

The grand jury charges:

INTRODUCTION

At all times material to this indictment, unless otherwise alleged:

1) Malicious software ("malware") is a software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, or do other unauthorized action on a computer system. Common examples of malware include viruses, worms, Trojan horses, rootkits, keyloggers, spyware, and others.

2) "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers' computers.

3) Keystroke logging is the action of recording (or logging) the keys struck on a keyboard. This action is usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist's knowledge. Malware

Avalanche 2

2017

Questions