

City of Los Angeles

LA Cyber Lab

The Cyber Threat Landscape

Get Involved



LA CYBER LAB

Eric Garcetti
@MayorOfLA

Deputy Mayor Jeff Gorell
Mayor's Office of Public Safety

 **\$600 Billion** 
Lost Globally Each Year







 **\$600 Billion** 
Lost Globally Each Year



Dallas Texas



- Hackers turn on citywide sirens
- Mass panic
- Residents flood 9-1-1
- EMS slow to respond to real emergencies

Atlanta Georgia



- Iran-based hackers lock citywide networks
- \$20 million lost
- DWP networks down
- Police dash-cams wiped
- Loss of 10 years of city attorney documents
- City budget delayed

Los Angeles California



- 4 Million unauthorized access attempts on city servers each day
- 2,200 intrusions each week

City of Los Angeles

LA Cyber Lab

The Cyber Threat Landscape

Get Involved



LA CYBER LAB

Eric Garcetti
@MayorOfLA

Deputy Mayor Jeff Gorell
Mayor's Office of Public Safety

The City of Los Angeles

1,000,000,000
security events analyzed daily

4,000,000
blocked attempts daily

2,200
weekly successful intrusions

L.A. ISOC Helps Capture Hacking Group



Integrated Security Operations Center (ISOC)



Managing threats strategically
LAWA JTA DWP PCLA



Eric
Garcetti
#Iamayor

MEDIA

TALK TO US GET HELP BLOG PERFORMANCE ABOUT

Press Releases

Home — Media — Press Releases —

Mayor Garcetti Issues Executive Directive on Cyber Security

Mayor Eric Garcetti today signed an Executive Directive creating a City of Los Angeles Cyber Intrusion Command Center to lead cybersecurity preparation and response across city departments. The Center will be led by the Office of the Mayor and will include assistance from the FBI and Secret Service.

"I'm creating this Cyber Intrusion Command Center so that we have a single, focused team responsible for implementing enhanced security standards across city departments and serving as a rapid reaction force to cyber-attacks," Mayor Garcetti said. "Today, our traffic lights, our routing system for trash pick-up, and so much more are electronic. Cybersecurity means protecting the basic services at the core of city government, and it means protecting our critical infrastructure like our port and airport, which we know are top targets."



Mandated citywide departmental coordination of cybersecurity



Cybersecurity is a critical function of government

Integrated Security Operations Center (ISOC)



Managing threats strategically
LAWA ITA DWP POLA

1,000,000,000
security events analyzed daily

4,000,000
blocked attempts daily

2,200
weekly successful intrusions

L.A. ISOC Helps Capture Hacking Group




- ISOC detects suspicious activity
- Alerts FBI and LAPD
- 3 hackers in Indonesia arrested
- Connected to 600 cyber attacks

Intelligence
Sony's Very, Very Expensive Hack
 By Anne Loomer



Photo: Ed Arapaci/CTMG


Hollywood hospital pays \$17,000 in bitcoin to hackers; FBI investigating
 By RICHARD WINTON
 FEB 18, 2016 10:44 AM



Hollywood Medical Center in 2014. The hospital was recently the target of a ransomware attack in which hackers seized control of its computer systems and then demanded \$17,000 in bitcoin to regain access. (Richard Winton/Los Angeles Times)

The Threat to LA Businesses

Maersk's L.A. port terminal remains closed after global cyberattack
 By JILL LEDDY and ALEXA D'ANGELO
 JUN 29, 2017 3:33 PM



Maersk containers at a terminal in Germany in 2013. (Patrick Stillerz / AFP/Getty Images)

Snapchat Employee Data Leaks Out Following Phishing Attack
 Jon Russell @jorrussell / Feb 20, 2016



City of Los Angeles

LA Cyber Lab

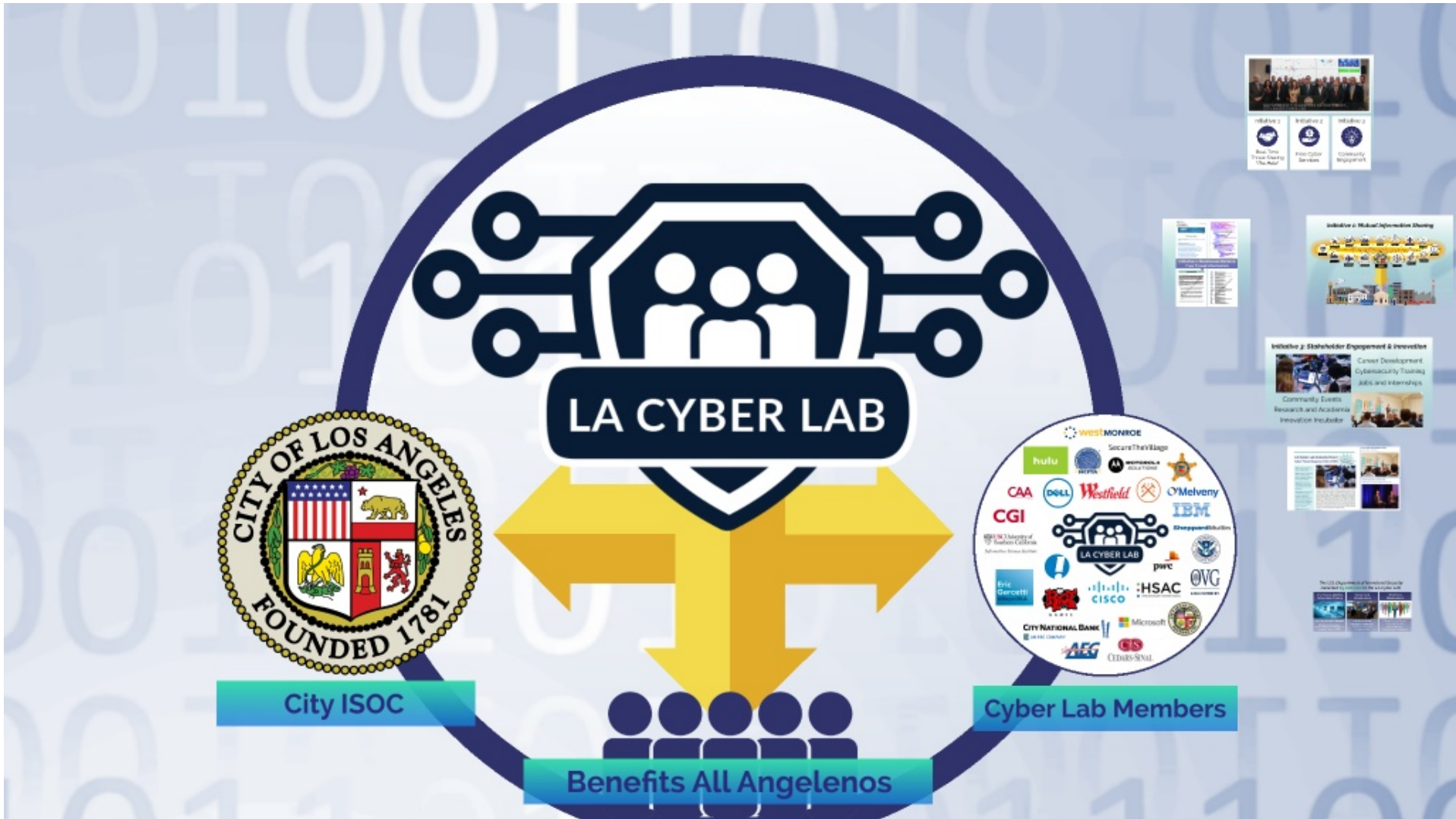
The Cyber Threat Landscape

Get Involved

LA CYBER LAB

Eric Garcetti
@MayorOfLA

Deputy Mayor Jeff Gorell
Mayor's Office of Public Safety







MAYOR GARCETTI LAUNCHES NATION'S FIRST CITY-BASED CYBER LAB

Initiative 1



Real-Time
Threat Sharing
"The Halo"

Initiative 2



Free Cyber
Services

Initiative 3



Community
Engagement

Initiative 1: Mutual Information Sharing



Daily Threat Report
1 message
LA Cyber Lab - threatintel@dailyrpt.org
Reply To: threatintel@dailyrpt.org
The LA Cyber Lab - threatintel@dailyrpt.org
Re: threatintel@dailyrpt.org@dailyrpt.org

Nov 3, 2017 at 10:24 AM



November 3, 2017

Daily Threat Report

Los Angeles - Physical Security
Los Angeles, CA: No Trump Day LA - World's Largest Solidarity Rally Held on November 4th at 4:00 PM (RPT)

Global Findings - Information Security
No Facebook 'Hacker' Accounts Compromised After Data Breach
Dental X-rays Big Money Risk Assured in Employment Scan
Homesite's Cyber Week Local Remembrance - Types, Features, Sites & Social - Report
Man Jailed for Cheating After Buying PayPal and Credit Card Account Details on Dark Web
Russian Hunting Word For Beyond US Borders, Digital Hitlist Reveals
Trump Organization Staff Discovers Shadow Subdomains with Russian IP for Four Years
Another Microsoft Azure 50 Server Leaks Data of 50,000 Australian Employees
Hacker Feels Clinging to Breach FiveEye Arrested, CSO Says
Shutterstock Credit Involving High Compliance Status - Report
No Facebook Employees Aren't Reading Your Private Google Docs Files
Analysis of 1,200 Phishing Kits Shows Light on Malware Tools and Techniques
Prime TV Services are Taking a Bite Out of Cable Company Revenue
Wealthy Muslim Art Dealer Hit by Cyber Attack Costing Them Up to \$10m

```

1 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
2 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
3 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
4 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
5 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
6 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
7 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
8 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
9 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
10 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
11 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
12 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
13 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
14 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
15 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
16 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
17 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
18 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
19 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
20 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
21 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
22 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
23 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
24 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
25 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
26 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
27 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
28 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
29 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
30 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
31 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
32 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
33 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
34 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
35 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
36 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
37 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
38 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
39 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
40 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
41 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
42 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
43 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
44 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
45 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
46 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
47 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
48 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
49 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
50 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
51 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
52 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
53 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
54 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
55 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
56 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
57 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
58 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
59 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
60 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
61 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
62 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
63 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
64 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
65 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
66 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
67 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
68 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
69 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
70 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
71 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
72 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
73 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
74 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
75 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
76 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
77 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
78 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
79 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
80 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
81 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
82 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
83 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
84 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
85 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
86 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
87 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
88 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
89 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
90 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
91 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
92 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
93 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
94 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
95 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
96 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
97 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
98 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
99 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]
100 2017-11-03 10:24:00 [INFO] [Daily Threat Report] [Daily Threat Report] [Daily Threat Report]

```

Initiative 2: Businesses Receive Free Threat Information

Executive Summary

On May 12, the Russian government began spreading across the globe, including countries in at least 120 countries. At least one hundred of organizations obtained 20,000 addresses of active malware, which was initially delivered via an unknown initial infection vector. The malware included security agency (S&A) capabilities in program as a service and allowed the government to perform a wide range of activities, including the ability to control and monitor other malware infections globally.

The initial malware payload does not appear to have any specific functionality, but its delivery mechanism and propagation are a work in progress. Threat sources indicate a distribution was made of cyber malware representing diverse capabilities and tools, as well as the Russian government. This includes development, and possibly support and potential communication, however, the exact details of the malware are not known at this time.

Key Points

- On May 12, 2017, the Russian government began spreading malware across the globe, including countries in at least 120 countries with Russia, China, France, and Mexico being the most affected.
- The initial infection vector is currently unknown - there is no evidence to suggest previously reported capabilities. It may have been made available to malware infections.
- The malware includes S&A capabilities to propagate as a work in progress and external malware.
- There have been multiple versions of the malware released already, indicating active development and response to the security community's research and intelligence activities.
- As of the writing, there is no information on the likelihood of any global or regional impact.

*This report is based on open source intelligence. Therefore, the report is open source intelligence and does not contain any sensitive information. Information from the open source cannot necessarily be verified and is provided as intelligence and is additional information to evidence in ongoing current investigations.

Indicator Type	Indicator
IP	192.168.1.1
IP	192.168.1.2
IP	192.168.1.3
IP	192.168.1.4
IP	192.168.1.5
IP	192.168.1.6
IP	192.168.1.7
IP	192.168.1.8
IP	192.168.1.9
IP	192.168.1.10
IP	192.168.1.11
IP	192.168.1.12
IP	192.168.1.13
IP	192.168.1.14
IP	192.168.1.15
IP	192.168.1.16
IP	192.168.1.17
IP	192.168.1.18
IP	192.168.1.19
IP	192.168.1.20
IP	192.168.1.21
IP	192.168.1.22
IP	192.168.1.23
IP	192.168.1.24
IP	192.168.1.25
IP	192.168.1.26
IP	192.168.1.27
IP	192.168.1.28
IP	192.168.1.29
IP	192.168.1.30
IP	192.168.1.31
IP	192.168.1.32
IP	192.168.1.33
IP	192.168.1.34
IP	192.168.1.35
IP	192.168.1.36
IP	192.168.1.37
IP	192.168.1.38
IP	192.168.1.39
IP	192.168.1.40
IP	192.168.1.41
IP	192.168.1.42
IP	192.168.1.43
IP	192.168.1.44
IP	192.168.1.45
IP	192.168.1.46
IP	192.168.1.47
IP	192.168.1.48
IP	192.168.1.49
IP	192.168.1.50
IP	192.168.1.51
IP	192.168.1.52
IP	192.168.1.53
IP	192.168.1.54
IP	192.168.1.55
IP	192.168.1.56
IP	192.168.1.57
IP	192.168.1.58
IP	192.168.1.59
IP	192.168.1.60
IP	192.168.1.61
IP	192.168.1.62
IP	192.168.1.63
IP	192.168.1.64
IP	192.168.1.65
IP	192.168.1.66
IP	192.168.1.67
IP	192.168.1.68
IP	192.168.1.69
IP	192.168.1.70
IP	192.168.1.71
IP	192.168.1.72
IP	192.168.1.73
IP	192.168.1.74
IP	192.168.1.75
IP	192.168.1.76
IP	192.168.1.77
IP	192.168.1.78
IP	192.168.1.79
IP	192.168.1.80
IP	192.168.1.81
IP	192.168.1.82
IP	192.168.1.83
IP	192.168.1.84
IP	192.168.1.85
IP	192.168.1.86
IP	192.168.1.87
IP	192.168.1.88
IP	192.168.1.89
IP	192.168.1.90
IP	192.168.1.91
IP	192.168.1.92
IP	192.168.1.93
IP	192.168.1.94
IP	192.168.1.95
IP	192.168.1.96
IP	192.168.1.97
IP	192.168.1.98
IP	192.168.1.99
IP	192.168.1.100

Initiative 3: Stakeholder Engagement & Innovation



Career Development
Cybersecurity Training
Jobs and Internships

Community Events
Research and Academia
Innovation Incubator



LA Cyber Lab Industry Event Cyber Threat Response Clinic (CTRC)



When: Tuesday, August 28, 2018—9:00AM-5:00PM

Where: Emergency Operations Center – 500 East Temple Street, Los Angeles, CA 90012 (Free parking available)

Registration: All attendees must register online and will close out with the first (35) participants.

What to Bring: A laptop* and a current CCO account are required. All registered attendees will need to have a valid CCO account (1) week prior to the event and by 8/21. Cisco can assist in assigning guest CCO accounts.

Audience: This course is



The Cyber Threat Response Clinic (CTRC) is an exciting security education initiative. This lab has been built as a training platform based on security Integrated solutions to address real world threat situations occurring most commonly today. Students will get to experience life-like cyber security attack situations in a virtualized enterprise lab environment, where they will get to play both the role of attacker and defender. Utilizing an environment that models many enterprise networks, students will learn and understand how environments get compromised, how security breaches get detected, and how to respond with maximum effectiveness. The clinic will be held in a classroom setting and the labs will consist of simulations of various cyber threats including phishing attacks, ransomware propagation and DNS breaches.

Agenda:

Route Fifty Tech Roadshow 2018

JUNE 14, 2018 | HONEYPOT LA



Evanta SoCal CISO Summit 2018

JUNE 5, 2018 | HILTON LOS ANGELES/UNIVERSAL CITY



*The U.S. Department of Homeland Security Awarded **\$3,000,000** to the LA Cyber Lab*

Machine-to-Machine Information Sharing



Real-Time Information Exchange
Building a Universal and
Accessible Threat Intelligence
Sharing Platform (TISP)

Personnel & Infrastructure



Full-Time Personnel
Advanced Technology for
Situational Awareness
LA Cyber Lab HQ

Workforce Development



College-to-Career Pipeline
Continuing Education
Networking Events
Research and Development

City of Los Angeles

LA Cyber Lab

The Cyber Threat Landscape

Get Involved



LA CYBER LAB

Eric Garcetti
@MayorOfLA

Deputy Mayor Jeff Gorell
Mayor's Office of Public Safety

www.lacyberlab.org



No-Cost Cyber Tools for LA Businesses

Sign up below to receive free city of Los Angeles cyber alerts and threat intelligence. Using ~1 billion daily records from the city of Los Angeles and the Federal government, your organization can receive information via email PDF, email CSV, or machine-to-machine STIX files loaded directly into your cyber security tools. *CyberLabLA membership is subject to validation by the city of Los Angeles.*

Business Name *

Contact Name *

Contact Email *

Contact Phone Number *

Preferred Method Of Delivery *

- Email PDF
- Email CSV File
- STIX/TAXII Interface

I'm not a robot



SUBMIT

***Questions?
Contact Us!***



Jeff Gorell

Deputy Mayor for Public Safety
jeff.gorell@lacity.org

Jacob Finn

Policy Manager for Cybersecurity
jacob.finn@lacity.org
(213) 310-1276

City of Los Angeles

LA Cyber Lab

The Cyber Threat Landscape

Get Involved



LA CYBER LAB

Eric Garcetti
@MayorOfLA

Deputy Mayor Jeff Gorell
Mayor's Office of Public Safety



**Eric
Garcetti**
@MayorOfLA