CIS Center for Internet Security®

MS-ISAC Multi-State Information Sharing & Analysis Center

Cyber Threat Information Sharing

Ben Spear

Senior Intelligence Analyst

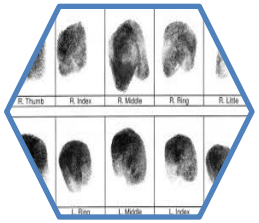
Multi-State Information Sharing and Analysis Center

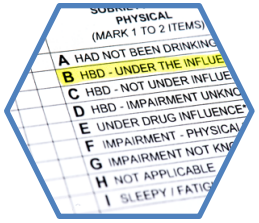
The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's SLTT governments.

Why SLTT Governments?

Criminals look for data...

and governments have a lot of it!





MS-ISAC Cyber Alerts

To: Thomas Duffy
Cc:
Subject: MS-ISAC Cyber Alert - DHS Issues Binding Operational Directive on Kaspersky Products - TLP: WHITE

TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members and Intel Partners

DATE ISSUED: September 13, 2017

SUBJECT: DHS Issues Binding Operational Directive on Kaspersky Products

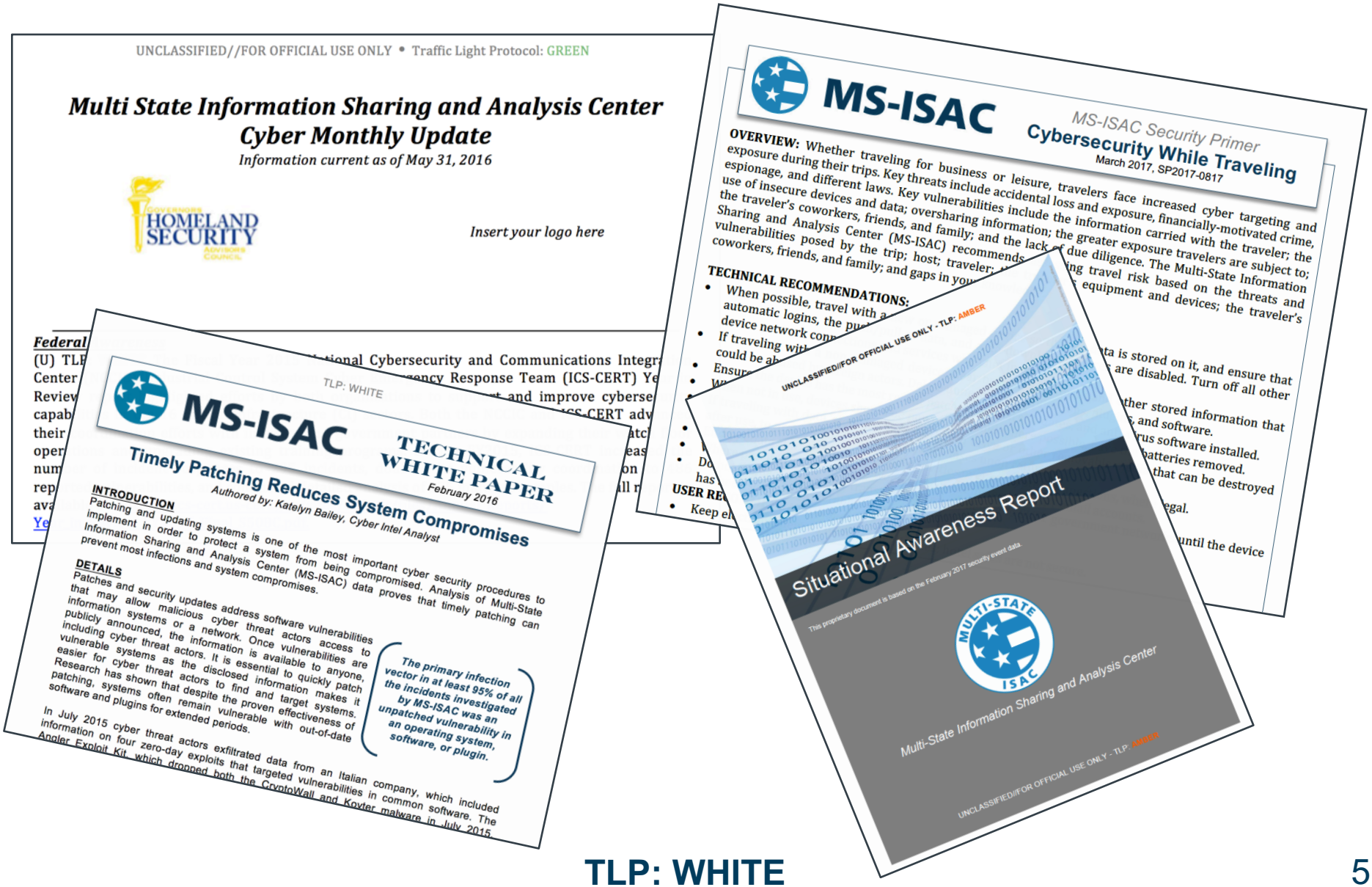
On September 13, 2017, the U.S. Department of Homeland Security (DHS) released Binding Operational Directive (BOD) 17-01 directing federal agencies to remove/discontinue use of products, solutions, and services provided by AO Kaspersky Lab or related entities. The BOD mandates that federal agencies identify Kaspersky Lab products on federal information systems within the next 30 days, develop detailed plans to remove and discontinue use of the products within 60 days, and implement those removal/discontinuation plans within 90 days. This follows the July 11, 2017, General Services Administration (GSA) decision to remove Kaspersky Lab from its list of approved vendors due to alleged ties between the company and Russian intelligence services.

DHS assesses that Kaspersky products, solutions, and services, supplied directly or indirectly by Kaspersky Lab or related entities, provide broad access to files and elevated privileges. The risks cited by DHS is twofold: that DHS is concerned with ties between Kaspersky Lab officials and that the Russian government and that Russian law could allow Russian intelligence or government agencies to request or compel assistance from Kaspersky Lab. These actions could result in the interception of U.S. communications transiting Russian networks and/or capitalize on the access provided to U.S. federal government networks through Kaspersky products.

RECOMMENDATIONS:
The MS-ISAC recommends members follow the guidance in the federal directive.

REFERENCES:
DHS Statement on BOD 17-01:
https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

MS-ISAC Intel Papers

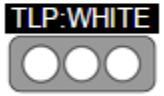


TLP: WHITE

Other Common Intel Products

- DHS Intelligence Note
- DHS Intelligence Assessment
- FBI/DHS Joint Intelligence Bulletin (JIB)
- FBI Private Industry Notification (PIN)
- FBI Liaison Alert System (FLASH)
- FBI/DHS Joint Analysis Report (JAR)
- US-CERT Malware Initial Findings Report (MIFR)

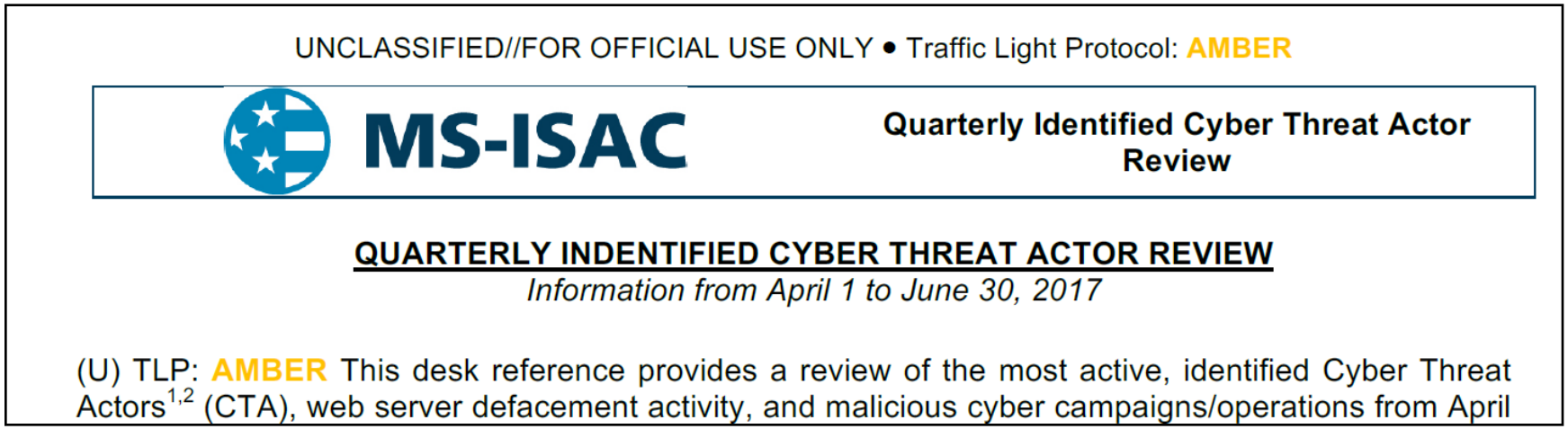
Traffic Light Protocol (TLP)

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

TLP: WHITE

Other Keywords to Look For

- **Unclassified (U)**
- **For Official Use Only (FOUO)**
- **Sensitive but Unclassified (SBU)**



UNCLASSIFIED//FOR OFFICIAL USE ONLY • Traffic Light Protocol: AMBER

MS-ISAC

Quarterly Identified Cyber Threat Actor Review

QUARTERLY INDENTIFIED CYBER THREAT ACTOR REVIEW

Information from April 1 to June 30, 2017

(U) TLP: AMBER This desk reference provides a review of the most active, identified Cyber Threat Actors[1,2] (CTA), web server defacement activity, and malicious cyber campaigns/operations from April

What's in an Intel Product?

- **Executive Summary (BLUF)**
- **Examples of the activity**
- **Description of technical terms, processes, actors**
- **Indicators**
  - IP addresses
  - Domains
  - Hashes
  - Snippets of malicious code
- **Recommendations**

What Should You Do With Products?

SHARE THEM!

- Follow the guidance outlined by markings
- Provide indicators to IT and security teams
- Take any necessary precautions as outlined in the recommendations
- Contact the MS-ISAC, DHS, or FBI if you identify any activity similar to the report

What Can You Do?

Low Hanging Fruit!

1. PATCH!
2. Use defensive software
3. Back-up
4. Train users
5. Enforce strong, complex, unique passwords

Critical Security Controls

1. Identify authorized and unauthorized devices
2. Inventory authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
5. Controlled use of admin privileges

Center for Internet Security®

MS-ISAC
Multi-State Information Sharing & Analysis Center

MS-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@msisac.org

Ben Spear

Senior Intelligence Analyst
518.880.0705
ben.spear@cisecurity.org