April 16, 2015

Senator Dianne Feinstein
331 Hart Senate Office Building
Washington, D.C. 20510

Senator Richard Burr
217 Russell Senate Office Building
Washington, DC 20510

Congressman Adam Schiff
2411 Rayburn HOB
Washington D.C. 20515

Congressman Devin Nunez
Longworth House Office Building
Suite 1013
Washington, DC 20515

Congressman Michael McCaul
131 Cannon House Office Building
Washington, DC 20515

RE: Cyber Threat Information Sharing Bills

Dear Senator Burr, Senator Feinstein, and Representatives Nunez, Schiff, and McCaul:

We are writing you today as technologists, academics, and computer and network security professionals who research, report on, and defend against Internet security threats. Among us are antivirus and threat signature developers, security researchers and analysts, and system administrators charged with securing networks. We have devoted our careers to building security technologies, and to protecting networks, computers, and critical infrastructure against a wide variety of even highly sophisticated attacks.

We do not need new legal authorities to share information that helps us protect our systems from future attacks. When a system is attacked, the compromise will leave a trail, and investigators can collect these bread crumbs. Some of that data empowers other system operators to check and see if they, too, have been attacked, and also to guard against being similarly attacked in the future. Generally speaking, security practitioners can and do share this information with each other and with the federal government while still complying with our obligations under federal privacy law.

Significantly, threat data that security professionals use to protect networks from future attacks is a far more narrow category of information than those included in the bills being considered by Congress, and will only rarely contain private information. In those rare cases, we generally scrub the data without losing the effectiveness of the threat signature.

These are some common categories of data that we share to figure out if systems have been compromised (indicators of compromise, or IoCs) and to mitigate future threats:

- Malware file names, code, and hashes
- Objects (code) that communicate with malware
- Compile times: data about the conversion of source code to binary code
- File size
- File path location: where on the computer system malware files are stored
- Registry keys: configuration settings for low-level operating system and applications
- Memory process or running service information

Attached to this letter is an actual example of a threat signature containing data that helps system administrators secure their networks. You'll see that the information does not contain users' private information.

Waiving privacy rights will not make security sharing better. The more narrowly security practitioners can define these IoCs and the less personal information that is in them, the better. Private information about individual users is often a detriment in developing threat signatures because we need to be able to identify an attack no matter where it comes from and no matter who the target is. Any bill that allows for and results in significant sharing of personal information could decrease the signal-to-noise ratio and make IoCs less actionable.

Further, sharing users' private information creates new security risks. Here are just three examples: First, any IoC that contains personal information exacerbates the danger of false-positives, that innocent behavior will erroneously be classified as a threat. Second, distribution of private data like passwords could expose our users to unauthorized access, since, unfortunately, many people use the same password across multiple sites. Third, private data contained in personal emails or other messages can be abused by criminals developing targeted phishing attacks in which they masquerade as known and trusted correspondents.

For these reasons, we do not support any of the three information sharing bills currently under consideration--the Cybersecurity Information Sharing Act (CISA), the Protecting Cyber Networks Act (PCNA), or the National Cybersecurity Protection Advancement Act of 2015. These bills permit overbroad sharing far beyond the IoCs described above that are necessary to respond to an attack, including all "harms" of an attack. This excess sharing will not aid cybersecurity, but would significantly harm privacy and could actually undermine our ability to effectively respond to threats.

As a general rule, when we do need to share addressing information, we are sharing the addresses of servers which are used to host malware, or to which a compromised computer will connect for the exfiltration of data. In these cases, this addressing information helps potential victims block malicious incoming connections. These addresses do not belong to subscribers or customers of the victims of a security breach or of our clients whose systems we are helping to secure. Sharing this kind of addressing is a common current practice. We do not see the need for new authorities to enable this sharing.

Before any information sharing bill moves further, it should be improved to contain at least the following three features:

1. Narrowly define the categories of information to be shared as only those needed for securing systems against future attacks;
2. Require firms to effectively scrub all personally identifying information and other private data not necessary to identify or respond to a threat; and
3. Not allow the shared information to be used for anything other than securing systems.

We appreciate your interest in making our networks more secure, but the legislation proposed does not materially further that goal, and at the same time it puts our users' privacy at risk. These bills weaken privacy law without promoting security. We urge you to reject them.

Sincerely[*],

Ben Adida

Jacob Appelbaum, Security and privacy researcher, The Tor Project

Sergey Bratus, Research Associate Professor, Computer Science Department, Dartmouth College

Eric Brunner-Williams, CTO, Wampumpeag

Dominique Brezinski, Principal Security Engineer, Amazon.com

Jon Callas

Katherine Carpenter, Independent Consultant

Antonios A. Chariton, Security Researcher, Institute of Computer Science, Foundation of Research and Technology — Hellas

Stephen Checkoway, Assistant Research Professor, Johns Hopkins University

Gordon Cook, Technologist, writer, editor and publisher of "COOK report on Internet Protocol" since 1992.

Shaun Cooley, Distinguished Engineer, Cisco

John Covici, Systems Administrator, Covici Computer Systems

Tom Cross, CTO, Drawbridge Networks

David L. Dill, Professor of Computer Science, Stanford University

A. Riley Eller, Chief Technology Officer, CoCo Communications Corp.

Rik Farrow, USENIX

Robert G. Ferrell, Special Agent (retired), U.S. Dept. of Defense

Kevin Finisterre, Owner, DigitalMunition

Bryan Ford, Associate Professor of Computer Science, Yale University

Dr. Richard Forno, Affiliate, Stanford Center for Internet and Society

Paul Ferguson, Vice President, Threat Intelligence

Jim Fruchterman, Benetech

Kevin Gennuso, Information Security Professional

Dan Gillmor. Teacher and technology writer

Sharon Goldberg, assistant professor, Computer Science Department, Boston University

Joe Grand, Principal Engineer, Grand Idea Studio, Inc.

Thaddeus T Grugq, independent security researcher

J. Alex Halderman, Morris Wellman Faculty Development Assistant Professor of Computer Science and Engineering, University of Michigan
Director, University of Michigan Center for Computer Security and Society

Professor Carl Hewitt, Emeritus EECS MIT

Gary Knott, PhD (Stanford CS, 1975), CEO, Civilized Software

Rich Kulawiec, Senior Internet Security Architect, Fire on the Mountain, LLC

Ryan Lackey; Product, CloudFlare, Inc

Ronald L. Larsen, Dean and Professor, School of Information Sciences, University of Pittsburgh

Christopher Liljenstolpe, Chief architect for AS3561 (at the time about 30% of the Internet backbone by traffic) and AS1221 (Australia's main Internet infrastructure).

Ralph Logan, Partner, Logan Haile, LP

Robert J. Lupo, Senior Security Engineer "sales team", IBM inc.

Marc Maiffret, Former CTO BeyondTrust

Steve Manzuik, Director of Security Research, Duo Security

Ryan Maple. Information security professional.

Brian Martin, President, Open Security Foundation (OSF)

Morgan Marquis-Boire

Aaron Massey, Postdoctoral Fellow, School of Interactive Computing, Georgia Institute of Technology

Andrew McConachie. Network engineer with experience working on Internet infrastructure.

Daniel L. McDonald, RTI Advocate and Security Point-of-Contact, illumos Project

Alexander McMillen, Mission critical datacenter and cloud services expert

Charlie Miller, Security Engineer at Twitter

HD Moore, Chief Research Officer, Rapid7

Joseph “Jay” Moran, Vice President of Cimpress Technology Operations

Peter G. Neumann, Senior Principal Scientist, SRI International
Moderator of the ACM Risks Forum (risks.org)

Jesus Oquendo, Information Security Researcher, E-Fensive Security Strategies

Ken Pfeil, CISO, Pioneer investments

Benjamin C. Pierce, Professor of Computer and Information Science, University of Pennsylvania

Ryan Rawdon, Network and Security Engineer

Bruce Schneier, security researcher and cryptographer, published seminal works on applied cryptography

Sid Stamm, Ph.D., Principal Engineer, Security and Privacy, Mozilla; Visiting Assistant Professor of Computer Science, Rose-Hulman Institute of Technology

Armando Stettner, Technology Consultant

Matt Suiche, Staff Engineer, VMware

C. Thomas (Space Rogue), Security Strategist, Tenable Network Security

Arrigo Triulzi, independent security consultant

Doug Turner, Sr. Director - Privacy, Security, Networking, Mozilla Corporation

Daniel Paul Veditz, Principal Security Engineer, Mozilla, Co-chair Web Application Security Working Group, W3C

David Wagner, Professor of Computer Science, University of California, Berkeley

Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker Institute for Public Policy, Rice University

Jonathan Weinberg, Professor of Law, Wayne State University

Stephen Wilson, Managing Director and Founder, Lockstep Technologies

Chris Wysopal, CTO and co-founder Veracode, Inc.

Stefano Zanero, Board of Governors member, IEEE Computer Society

[*] In all cases, titles and affiliations are listed for information purposes only. Signatories do not necessarily speak on behalf of their affiliated organizations.

```
<?xml version='1.0' encoding='UTF-8'?>
<!--
    TITLE:          113e561e-60d2-48db-979d-02f207550125.ioc
    VERSION:        1.0
    DESCRIPTION:    OpenIOC file
    LICENSE:        Copyright 2014 FireEye Corporation.  Licensed under the Apache 2.0 license.

    FireEye licenses this file to you under the Apache License, Version
    2.0 (the "License"); you may not use this file except in compliance with the
    License.  You may obtain a copy of the License at:

            http://www.apache.org/licenses/LICENSE-2.0

    Unless required by applicable law or agreed to in writing, software
    distributed under the License is distributed on an "AS IS" BASIS,
    WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
    implied.  See the License for the specific language governing
    permissions and limitations under the License.
-->
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas
  <short_description>RAZOR BLADES IN THE CANDY JAR (BLOG)</short_description>
  <description>This IOC contains indicators detailed in the blog post "Razor Blades in the Candy Jar" that can be read here:
  <keywords/>
  <authored_by>FireEye</authored_by>
  <authored_date>2014-11-07T13:45:38Z</authored_date>
  <links>
    <link rel="category">Exploit</link>
    <link rel="license">Apache 2.0</link>
  </links>
  <definition>
    <Indicator id="958fa712-7e84-4a0d-a4e3-2918b9aeda9a" operator="OR">
      <IndicatorItem id="1d233eb6-52d7-4843-a013-6de4d6877515" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">img.lakeforestparkhome.info</Content>
      </IndicatorItem>
      <IndicatorItem id="dbd5b695-fb67-4987-9ee1-4c680eaefc6c" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">micagirl.net</Content>
      </IndicatorItem>
      <IndicatorItem id="258695cd-c21a-48b1-9f57-7768dfb699c2" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">h.micagirl.net</Content>
      </IndicatorItem>
      <IndicatorItem id="ce4bfd0f-bc4e-4250-b784-110af8a77436" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">a.micagirl.net</Content>
      </IndicatorItem>
      <IndicatorItem id="b105fbd3-c53e-416f-ac80-9c16448598f3" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">img.kirklandhouse.info</Content>
      </IndicatorItem>

      <IndicatorItem id="27f23053-6941-4e6f-ad6d-cc6442f6798d" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">cdn.jameswoodwardmusic.com</Content>
      </IndicatorItem>
      <IndicatorItem id="c0082ee6-fc2f-4b5a-8bf5-a3aac8f8da76" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">cdn.movetoclarksville.com</Content>
      </IndicatorItem>
      <IndicatorItem id="ed986932-8ba0-4195-bad0-2313cb3b887a" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">img.greenwoodhouse.info</Content>
      </IndicatorItem>
      <IndicatorItem id="362c6b4f-f3aa-4f77-864b-083c143d976d" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">src.sandcastlesmagazine.com</Content>
      </IndicatorItem>
      <IndicatorItem id="4bb8378d-7df5-4b8a-b136-48588c1c37b9" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">src.sheffieldwoods.org</Content>
      </IndicatorItem>
      <IndicatorItem id="aea5076e-8c2d-49b8-b968-31cbd79601f1" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">yimg.1stdayofwinter.com</Content>
      </IndicatorItem>
      <IndicatorItem id="68c52dfc-9d6a-4ffb-8d55-40c3f78493dc" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">yimg.1208nw199thpl.info</Content>
      </IndicatorItem>
      <IndicatorItem id="38e7cd32-0f5e-4224-a932-0c4dfde4881e" condition="contains">
```

```
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">img.broadviewhome.info</Content>
      </IndicatorItem>
      <IndicatorItem id="d56689cd-975d-4cb7-bbcc-60682c5ea162" condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">cdn2.movetoclarksville.com</Content>
      </IndicatorItem>
      <IndicatorItem id="3dd71368-5044-43ac-a8d5-d69ed026ad85" condition="is">
        <Context document="PortItem" search="PortItem/remoteIP" type="mir"/>
        <Content type="IP">185.22.233.136</Content>
      </IndicatorItem>
      <IndicatorItem id="bed525e5-8fb7-4ed5-9b88-5fe84e38b26a" condition="is">
        <Context document="PortItem" search="PortItem/remoteIP" type="mir"/>
        <Content type="IP">192.185.16.158</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```