In 2017, 66% of malware was installed via malicious email attachments.\(^1\) 1.1 billion personal identities were exposed in data breaches in 2017.\(^2\) 49% of all companies suffered at least one cyber ransom incident in 2016.\(^3\) In 2017, the mean time to identify a breach was 190 days and the mean time to contain a breach was 66 days.\(^4\) 50% of small and medium sized businesses suffer at least one cyber attack in a 12 month period.\(^5\) 100% of states reported cyber crime to the FBI’s IC3 in 2017. Business email compromise resulted in $675 million in adjusted losses alone.\(^6\)

**WHAT’S AT STAKE?**

The vast majority of cyber attacks occur via only a few attack vectors. Even though we know how these attacks occur, most groups are not prepared to defend against them. According to Hiscox Insurance CEO Steve Langan, cyber crime cost the global economy “over $450 billion” in 2016.\(^7\)

**TOOLS OF THE TRADE**

Most mature organizations use perimeter protections to prevent and detect intrusions on their enterprise networks. Approved service providers, in partnership with DHS, operate Enhanced Cybersecurity Services (ECS) in order to help private and state/local groups strengthen their perimeter defense capabilities. ECS protects against many of the most common threats facing businesses today including socially engineered malware, password phishing, and advanced persistent threats.\(^8\)

Security teams choose ECS because it is the only commercially available capability that uses sensitive and classified government intelligence to actively detect and block threats. ECS is the fastest way to protect your networks using government information. When millions of connections are traversing a network at any given moment, speed is of the essence.

See the reverse side for service provider contact information.

---

**FISCAL YEAR 2018 Q4 ECS BLOCK REPORT**

In September, ECS recorded Advanced Persistent Threat activity against domains associated with a spear phishing campaign targeting organizations involved with the Pyeongchang Olympics. NCCIC continues to track this indicator, as well as other threats with tactics, techniques, and procedures similar to the identified threat actor.

Each ECS indicator is associated with a Threat Actor (TA) identified by the Intelligence Community. Over the last quarter, 16 of these TAs were detected on ECS systems.

---

**YEAR END NOTES**

Fiscal Year 2018 was a busy one for the ECS program. Perhaps the biggest milestone—ECS began covering the State sector in its participant line-up. Additional participating sectors include the Communications, Defense, Energy, and Financial sectors. The program also worked to improve the data it shares with Service Providers, including adding additional context about threats, tactics, and actors. Behind the scenes, the program accredited a new implementer who now uses ECS to protect their own networks. And as in every year, the program moved to strengthen our partnerships with existing providers and to help facilitate new provider’s entry into the program.
ECS PROGRAM REVIEW

About
ECS is an intrusion detection and prevention capability that helps U.S.-based companies and state and local government groups protect their computer systems against unauthorized access, exploitation, and data exfiltration.

Operations
ECS works by deriving timely, actionable cyber threat indicators from sensitive and classified government information. As a hub for cyber threat intelligence, NCCIC sources and distributes ECS indicators of compromise to ECS CSPs. Those CSPs in turn use the indicators to help protect participant companies’ networks. ECS customers subscribe to receive services from CSPs via a traditional consumer agreement.

Services
ECS currently offers two approved cyber threat services: Domain Name System (DNS) Sinkholing and E-mail (SMTP) Filtering.

Eligibility
All U.S.-based organizations are eligible to enroll in ECS, including state and local government organizations. All sectors can participate. State and local groups, such as city bus systems, state and local government jurisdictions, law enforcement agencies, etc., may be eligible to use FEMA HSGP funds for ECS.

Privacy
The ECS program is designed specifically with privacy protections in mind. DHS does not collect, or receive customer traffic or communications.

Benefits
The biggest advantage of ECS is the speed of protections. ECS protects your organization immediately—and it protects using classified information. ECS is the only system available to non-federal entities that actively blocks threats associated with classified information. As soon as a threat is known to DHS, it is deployed through ECS—and quickly blocks that threat from further propagation. ECS CSPs each offer their services in a unique way. Interested organizations should reach out to them to learn more about their offerings. With millions of connections and interactions traversing a single network every minute, human analysts can easily become overwhelmed trying to separate the good traffic from the bad. ECS makes those distinctions easily, freeing up valuable analyst time. ECS falls neatly into the NIST Cybersecurity Framework via the Protect, Detect, and Respond function areas.

References
1. 2017 Verizon Data Breach Investigation Report
2. 2017 Symantec Internet Security Threat Report
3. Cisco 2017 Midyear Cybersecurity Report
4. 2017 Cost of Data Breach Study: Poneman Institute
5. The 2016 State of SMB Cybersecurity; Keeper Security and Ponemon Institute
6. 2017 Internet Crime Report, FBI IC3
8. CSO Online: https://www.csoonline.com/article/2615315/data-protection/security-the-5-cyber-attacks-you’re-most-likely-to-face.html

ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSP</td>
<td>Commercial Service Provider</td>
</tr>
<tr>
<td>C3VP</td>
<td>Critical infrastructure Cyber Community Voluntary Program</td>
</tr>
<tr>
<td>ECS</td>
<td>Enhanced Cybersecurity Services</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Administration</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>HSGP</td>
<td>Homeland Security Grant Program</td>
</tr>
<tr>
<td>IC3</td>
<td>Internet Crime Complaint Center</td>
</tr>
<tr>
<td>NCCIC</td>
<td>National Cybersecurity &amp; Communications Integration Center</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NPPD</td>
<td>National Protection and Programs Directorate</td>
</tr>
<tr>
<td>TA</td>
<td>Threat Actor</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
</tbody>
</table>

ABOUT DHS CYBER

DHS NPPD is responsible for safeguarding our Nation’s critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

ECS Resources:
State and local governments may be eligible to use the FEMA Homeland Security Grant (HSGP) program to purchase services. The ECS CSPs are familiar with the FEMA grants and can assist state and local groups with the application process.

ECS Information:
AT&T ECS-PMO@list.att.com
CenturyLink ECS@centurylink.com
Verizon Vz-ecs@Verizon.com
ECS Program Office ECS_Program@hq.dhs.gov
ECS Webpage www.dhs.gov/ecs
FEMA HSGP www.fema.gov/homeland-security-grant-program