NASCIO 2016 Recognition Awards Nomination

The State of Missouri

Missouri’s Cybersecurity Threat Intelligence Portal

Project Initiation and Completion Dates: January 2015 to February 2015

Category:

Cybersecurity

Nomination Submitted by
Richard Kliethermes
Acting Chief Information Officer
Office of Administration
Information Technology Services Division
Rich.Kliethermes@oa.mo.gov
(573) 751-1504

Executive Summary

In early 2015, the Office of Cyber Security (OCS) recognized the need to produce threat intelligence that's actionable, timely, and relevant to the State of Missouri that can be shared with internal and external partners. The sharing of actionable threat intelligence has not only been proven to thwart our adversaries attempting to steal our citizen's data and disrupt government, but also raises the organizational cybersecurity awareness to a new level. As OCS' Security Operations Center (SOC) gained visibility throughout the years, their capabilities to generate consumable reports on malware, campaigns, vulnerabilities, and threat actors has increased tremendously.

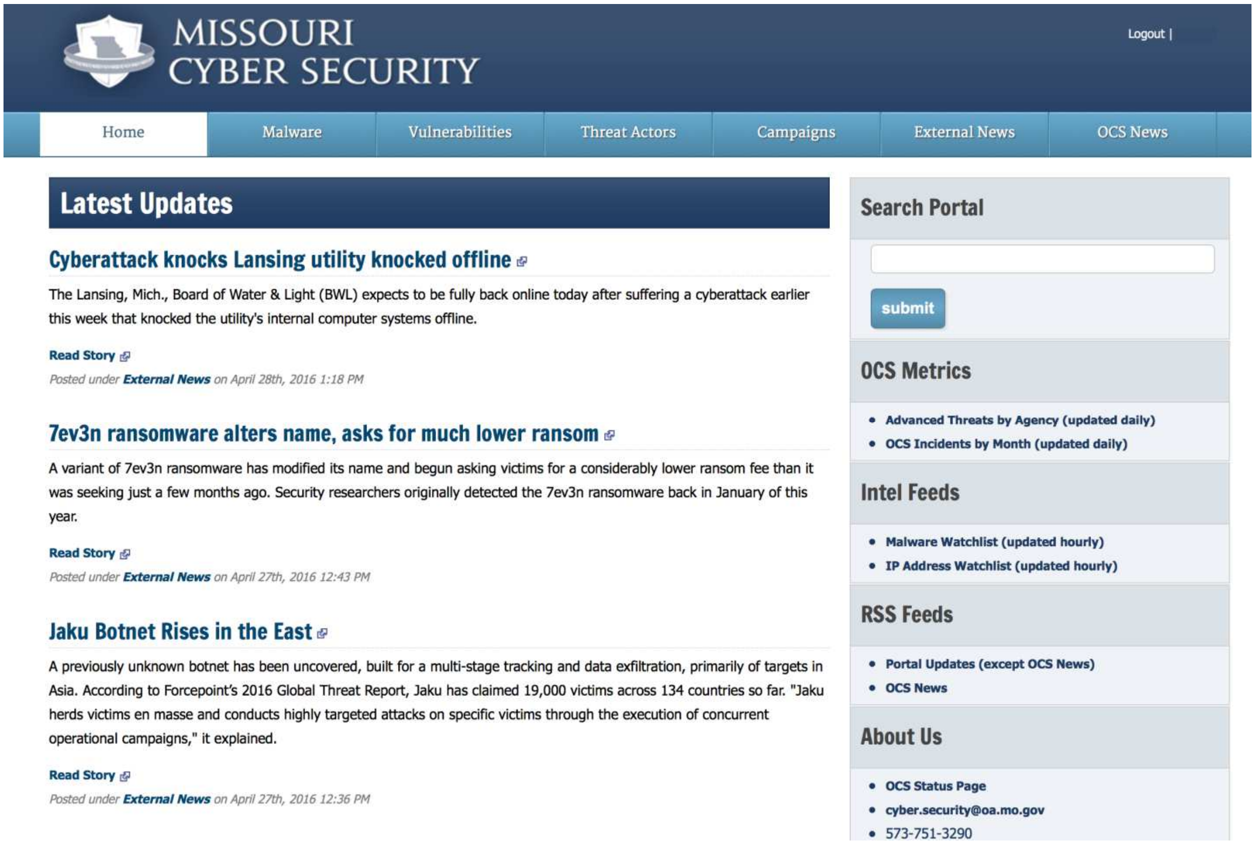
To share the treasure trove of cybersecurity information, OCS built a portal containing threat intelligence that's been collected from inter-agency incidents and other sources. The portal provides a platform to share threat intelligence in a timely manner to trusted entities and enables collaboration between OCS and its partners. The portal is innovative in the state government space, utilizes advanced technologies to feed it, and has the goal of safeguarding citizen's information by sharing threat intelligence as quickly as possible.

Completed in February 2015, the cybersecurity threat intelligence portal currently has over 2,000 reports and news stories published. The SOC continuously updates the portal with the latest information on the malware, campaigns, threat actors, and vulnerabilities that are impacting the State of Missouri. In addition, the SOC adds external news stories about relevant cybersecurity events happening across the globe. Besides analyst driven content, the portal contains malware and IP address blacklist feeds sourced by OCS' best of breed security stack. These blacklists are meant to be consumed by our partners to provide proactive protection and to also allow for post event analysis.

In addition to threat intelligence, the portal has several interactive charts that are driven by the integration with the SOC's incident tracking system. Using this integration, easy to understand performance metrics including the number of incidents investigated per month showing year over year differences and advanced threat counts by agency are displayed. These charts not only provide a barometer of the state's current threat landscape but also help gamify cybersecurity by comparing state agencies against each other.

The State of Missouri is submitting its cybersecurity threat intelligence portal because of its effectiveness in raising awareness throughout state government and its partners. In addition, the portal's approach to information sharing is innovative as we're not aware of another state entity sharing threat intelligence in this manner. Thank you for your consideration.

Project Narrative



Latest Updates

Cyberattack knocks Lansing utility knocked offline

The Lansing, Mich., Board of Water & Light (BWL) expects to be fully back online today after suffering a cyberattack earlier this week that knocked the utility's internal computer systems offline.

Read Story

Posted under ***External News*** *on April 28th, 2016 1:18 PM*

7ev3n ransomware alters name, asks for much lower ransom

A variant of 7ev3n ransomware has modified its name and begun asking victims for a considerably lower ransom fee than it was seeking just a few months ago. Security researchers originally detected the 7ev3n ransomware back in January of this year.

Read Story

Posted under ***External News*** *on April 27th, 2016 12:43 PM*

Jaku Botnet Rises in the East

A previously unknown botnet has been uncovered, built for a multi-stage tracking and data exfiltration, primarily of targets in Asia. According to Forcepoint's 2016 Global Threat Report, Jaku has claimed 19,000 victims across 134 countries so far. "Jaku herds victims en masse and conducts highly targeted attacks on specific victims through the execution of concurrent operational campaigns," it explained.

Read Story

Posted under ***External News*** *on April 27th, 2016 12:36 PM*

Search Portal

OCS Metrics

- Advanced Threats by Agency (updated daily)
- OCS Incidents by Month (updated daily)

Intel Feeds

- Malware Watchlist (updated hourly)
- IP Address Watchlist (updated hourly)

RSS Feeds

- Portal Updates (except OCS News)
- OCS News

About Us

- OCS Status Page
- cyber.security@oa.mo.gov
- 573-751-3290

Missouri cybersecurity threat intelligence portal homepage.

To raise awareness throughout state government and to share threat intelligence swiftly and effectively, the Missouri Office of Cyber Security (OCS) has built a publicly available (registration required) portal. OCS has embraced information sharing as one of the key strategies to thwart adversaries that want to harm state government and its partners. Driven by threat intelligence collected from the Security Operations Center's (SOC) investigations, the end-goal of the portal is to alert portal members of the current campaigns, malware, vulnerabilities, threat actors, and relevant news while also providing key indicators about the state's current cybersecurity posture using various metrics. The portal is open to all forms of government with a heavy emphasis on state partners. The portal is innovative in the state government space, utilizes advanced technology to feed it, and has the overall goal of safeguarding citizen information.

The portal contains the following content:

Malware

For the purpose of the portal, only advanced malware that's not detected by traditional controls is reported. This section contains what OCS understands about the malware including the source, malware family (if known), and the indicators of compromise

(MD5s, host names, OS changes). OCS also shares the malware with vetted individuals who can assist in furthering the analysis.

Vulnerabilities
OCS shares information on publicly known vulnerabilities with an emphasis being placed on technologies that are widely used within governments. The anticipated outcome is to alert state entities and other trusted partners before the adversary has an opportunity to exploit any unpatched systems on their networks.

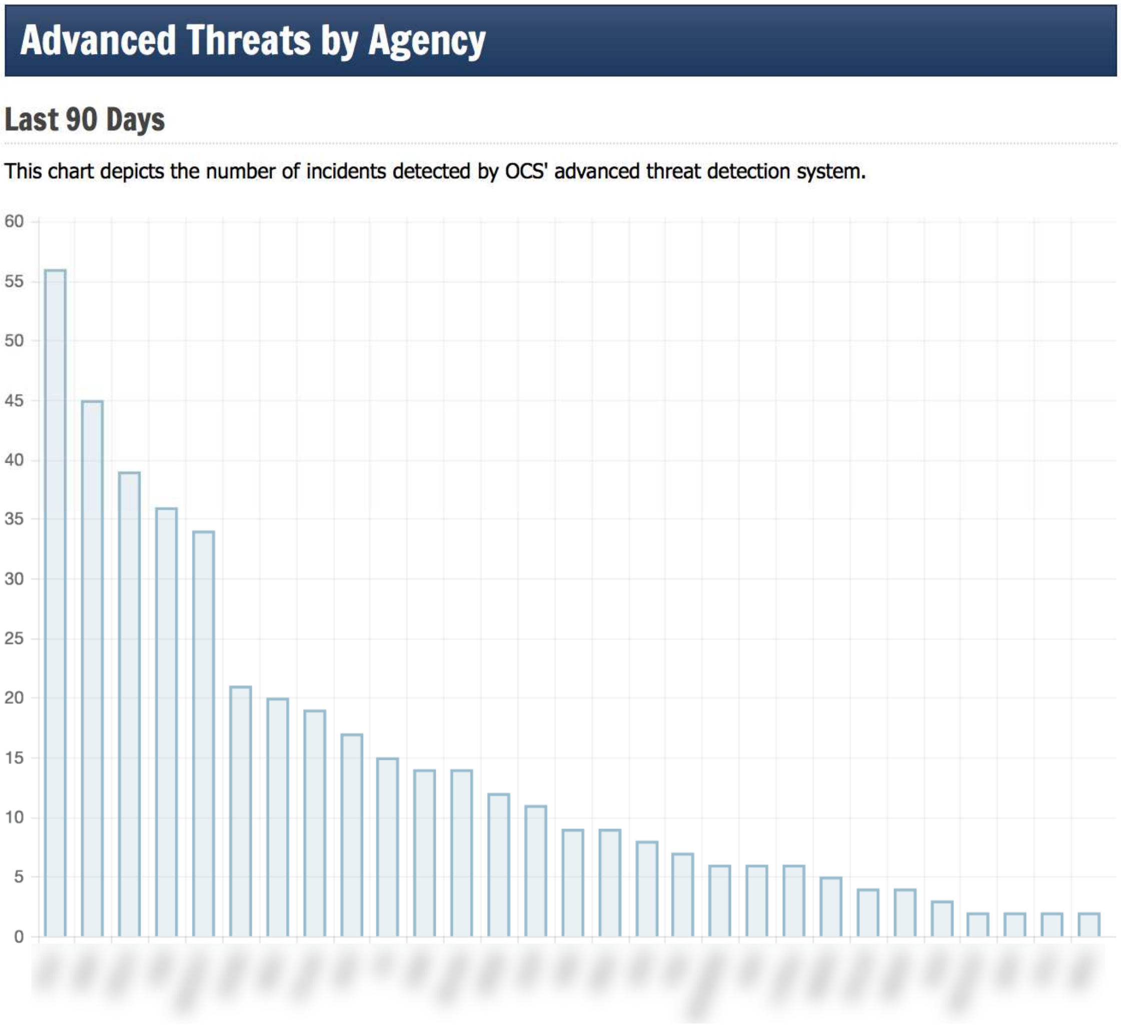
Threat Actors
The threat actors section of the portal includes information about entities that have been targeting state and local governments within Missouri. Tracking and sharing information on actors is beneficial in understanding their tactics, techniques, and procedures and to give an early warning to other state and local governments as these actors tend to go after governments in other regions.

Campaigns
The campaigns section includes information about organized attacks. The majority of the campaigns posted cover phishing attacks with distributed denial of service attacks coming in second. By using analytics and other mechanism, SOC analysts keep track of and monitor campaigns for changes in techniques used by the adversary.

External News
OCS shares information security related news that's happening in Missouri, around the country, and across the globe. The journal of news has proven to be invaluable in raising awareness throughout all levels of government; many cabinet level members read this section to understand the current threat landscape and how its changing.

OCS News
The internal users of the portal have access to a privileged section of the portal called OCS News. This section contains announcements meant for internal users only. The bulk of the items within this section touch on acute threats and what detailed changes OCS is making to its various network and endpoint controls to mitigate the risk.

OCS Metrics
To provide organizational awareness about the current threat landscape and to spur a little competition between agencies, users have access to various charts that are automatically updated daily. The first chart, advanced threat by agency, depicts the number of advanced threats investigated over a 90-day period broken out by agency. This chart provides agency administration a quick glance of their current status and how they compare to others. Because agencies don't want to be trailing, this chart assists in "motivating" agencies to help OCS raise awareness with its end-users.



Advanced Threats by Agency

Last 90 Days

This chart depicts the number of incidents detected by OCS' advanced threat detection system.

Advanced threats by agency chart

The second chart, OCS incidents by month, provides a monthly and year over year comparison on the number of incidents that the SOC investigates. This chart provides some insight into the growing awareness and visibility within the state's networks and endpoints.

Intelligence Feeds
Generated automatically every hour from the state's security stack, OCS's malware and IP address blacklists are available through the portal. All state and external partners have access to these lists to secure their networks but to also collaborate in what's being detected. These feeds are CSV formatted, so they're both human and machine readable.

RSS Feeds
For portal members that prefer continuous alerts on content updates, they can subscribe to the various RSS feeds.

Daily Newsletter

A newsletter covering the latest portal news and updates is sent to all portal members on a daily basis. The newsletter has been a key component of the portal as it pushes content to the users and provides them a quick and easy way to see what's happening from the comfort of their mailbox.

Concept History

Over the last 3 years, OCS has increased its visibility of endpoint and network security events by leveraging cyber analytics and advanced malware platforms. SOC analysts have been able to correlate sophisticated attacks and apply a level of attribution to many of them. As time went on, the SOC amassed a treasure trove of threat intelligence but did not have a good mechanism to share this information with other state members. In early 2015, OCS decided to build a publicly accessible portal so that any trusted partner, including other states, can benefit from the threat intelligence gleaned from the SOC investigations.

Since its inception, over 2,000 reports and news stories have been posted, raising awareness and providing a view into the state's threat landscape. The portal has been well received by its members, and countless examples exist where it helped thwart future attacks against the state and the state's partners. To date, the portal has over 200 members primarily consisting of state entities but the members also include representatives from US DHS, FBI, education (higher and secondary), local government, MS-ISAC, and some trusted private partners.

Technology and Development

The foundation of the portal is a commercial off-the-shelf content management system (CMS) called ExpressionEngine by EllisLab. ExpressionEngine was chosen because it has a strong reputation for being a secure platform (it powered the Obama transition portal, change.gov). In addition, ExpressionEngine allows for complex customization as it makes no assumptions about the data contained within it. These attributes were the primary factors in selecting the CMS technology. For a period of five weeks, the threat intelligence portal underwent development. Using an agile approach, the portal was wireframed and storyboarded to ensure functionality, standard look and feel, and a positive user experience.

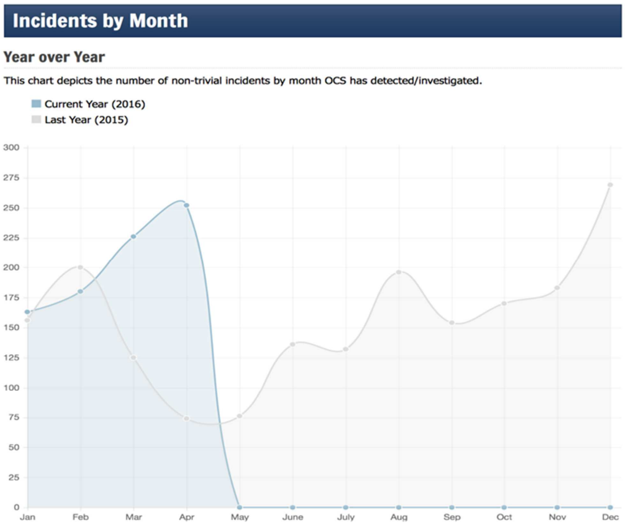
On the backend, several custom modules were built to send out a daily newsletter and status changes to the services provided by OCS. In addition, internal scripts were built to push summarized information to the portal from the SOC's incident management system and blacklists sourced from the state's security stack.

The portal is one of the first state websites hosted on Amazon's AWS service. Knowing that the portal is a pivotal tool in times of attack, by having it outside of the state's datacenter we can ensure availability. Also, by leveraging AWS' platform-as-a-service offerings (PaaS), OS and other infrastructure updates occur seamlessly and automatically ensuring a secure and robust environment. Finally, by having the portal in the cloud, it provides an example to other state agencies that secure computing can exist outside of a traditional on-premise data center.

Significance and Impact

The portal has played a significant role in raising the organizational cybersecurity awareness throughout Missouri state government and its partners by giving OCS the ability to share key aspects of their investigations and by curating news that matters. The portal not only acts as a pulpit; it also acts as a window into the state's overall threat landscape. Because of the information shared on the portal, agencies have changed their business and IT processes, close partners have leveraged the intelligence to thwart off attacks proactively and assist with their own investigations, and new conversations are taking place throughout state government about the latest threats and their potential impacts.

While much of the impact is qualitative in nature, OCS has seen agency movement within the advanced threats by agency chart. One particular agency was trailing all others by a significant margin. The agency was quite aware and decided to do something about it and take action. They implemented various security controls and over a several month period, they were able to pull themselves out of their position and be in alignment with other agencies of similar size and type. From an internal perspective, the impact has been positively measurable. From our partner's perspective, OCS receives feedback about how the threat intelligence prepared a partner for a phishing attack that eventually hit them. From the law enforcement side, numerous pieces of malware and other intelligence have been collected through the portal to assist in on-going federal investigations in tracking down the attackers and bringing them to justice.



Incidents by Month

Year over Year

This chart depicts the number of non-trivial incidents by month OCS has detected/investigated.

Portal Access

The portal is located at https://portal.cybersecurity.mo.gov. If you would like access, please email Michael.Roling@oa.mo.gov for more details.