Homeland Security | Enterprise Security Operations Center

DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

Component SOC:	Present	Status
CBP	No	NSTR
DC1	Yes	NSTR
DC2	Yes	NSTR
FEMA	Yes	NSTR
FLETC	Yes	NSTR
FPS	Yes	NSTR
HQ	Yes	NSTR
ICE	Yes	NSTR
NPPD	Yes	NSTR
OIG	No	NSTR
S&T	Yes	NSTR
TSA	Yes	NSTR
USCG	Yes	NSTR
USCIS	Yes	NSTR
USSS	No	NSTR
DHS EWO/NOC	Yes	NSTR
DHS ESOC	Yes	NSTR
DHS Privacy	No	NSTR

Meeting Purpose: To discuss and provide situational awareness of DHS information security operations.		
Facilitator: (b)(6) (b)(6)		
Date: 12/19/2016	Time: 0900-0930	Location: St. Elizabeth/DHS ESOC
Bridge Number: 202-475-4(b)(6)	Confirmation Number: 393 425 88 #	

Homeland Security | Enterprise Security Operations Center

DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

Meeting Summary:
Please see below for the "Meeting Minutes" associated with today's "DHS ESOC Daily Stand-Up" call.

OneNet SOC (DHS ESOC):

Situational Awareness Notes:

- The Department of Homeland Security has been accused by the Georgia Secretary of State, through a formal letter to Secretary Johnson, of conducting an unauthorized penetration test/scan of the "Georgia Secretary of State Firewall" on November 15th, 2016 at 08:43 A.M. The IP address that was logged to this event was the DC2 Proxy 1 IP address (Public: 216.81.81.80; Internal: 10.236.225.141). The IP address of the "Georgia Secretary of State Firewall" was not specified in the letter.
    - Update: The DHS ESOC has begun communicating with the CIO of State of Georgia. The "scanning" event was the result of a FLETC user's Microsoft Office Discovery Protocol sending a packet with the OPTIONS flag to the Secretary of State of Georgia site.
        - Note: Most web servers deny or ignore OPTIONS flag HTTP requests, as it is a depreciated HTTP 1.1 flag. The OPTIONS flag can be used by an attacker to gain information on a web server on what types of request methods it allows. However, in the context of the Georgia case no other suspicious or malicious traffic was found before or after this request.
    - Update 2: The DHS ESOC has received requests from NCCIC and MS-ISAC to investigate other states that have seen "suspicious" activity. If your component receives any State, Local or Tribal (SLT) requests to investigate "suspicious" web traffic from your component or DHS please direct those requests to the NCCIC team and CC the DHS ESOC.
    - Update 3: The DHS ESOC received notice that the Georgia Secretary of State has accused DHS of more "Scanning" activity. We have attached a timeline detailing the date and time of these alleged "scanning" events. The DHS ESOC was able to find logs pertaining to all events after September 12th. However, we are unable to reach back into our logs to find the events that took place on February 2nd, February 28th and May 23rd. The DHS ESOC has found that all "scanning" events happen to coincide with an HTTP "OPTIONS" request to the Georgia site. The Microsoft support team is currently investigating the "OPTIONS" request.
    - Update 4: Microsoft and the ESOC with the assistance of FLETC, were able to confirm that the user non-maliciously copied and pasted elements of the website to an excel document, which triggered the HTTP "OPTIONS" request.

MICROSOFT E-MAIL STATEMENT (Unofficial Statement to ESOC):

“DHS contacted Microsoft regarding a concern raised from the State of Georgia (ga.gov) over a DHS workstation triggering a Nexus alert for use of an Options verb request to web site http://verify.sos.ga.gov/verification/. Nexus web traffic data provided to Microsoft support shows the DHS user making normal, expected requests to the website including search requests for "*Search.aspx?facility=Y&SubmitComplaint=Y*", but it is followed by an Options verb request for http://verify.sos.ga.gov/verification/. No further web requests until ~8 hours later which are again the normal requests. These requests are not followed by any Options verb requests.

After looking at the data I do not see requests that look malicious in nature or appear to be attempting to exploit a vulnerability. Additionally the user is known to use copy/'paste special' for data from the webpage to Excel which invokes the Options verb. We have also been able to reproduce the Options verb request by using "right-click Export to Excel" and "right-click Send to OneNote" on the web page, but the user has not reported performing this action.”

Timeline of DHS Scanning Activity.pd

***PLEASE DIRECT ALL MEDIA REQUESTS TO THE DHS OFFICE OF PUBLIC AFFAIRS.**

- SEN 2016-11-260 – Wells Fargo performed a third party security assessment against the DHS Enterprise. The assessment found DHS email addresses out in the public and security vulnerabilities on public facing servers. The DHS ESOC recommends notifying the users that their email addresses are out in the public and potentially susceptible to spam and phishing e-mails. The DHS ESOC has attached a security vulnerabilities list to the SEN log on EOC. Please verify these vulnerabilities and develop a plan to remediate them as soon as possible.
    - **The Wells Fargo Team conducted their assessment based off a proprietary tool that uses Open Source methods to collect data on an organization. The DHS ESOC and NCCIC will receive a list of their tools and have a follow-up meeting to discuss their methodology more in-depth at a later date.**
    - **In the coming week, the FISMA Compliance team will provide a way ahead for DHS to remedy the vulnerabilities found during this assessment.**

- Please see below for Cyber Hygiene Results Weekly Rollup; view the following site for weekly cyber hygiene reports: http://mgmt-ocio-sp.dhs.gov/ciso/fisma%20reporting/SitePages/FNR%20Cyber%20Hygiene%20Scans.aspx

New ISVM Releases:

There was one (1) ISVM released Friday (12/16/2016):

2016-305-0-B-Apple Multi-Products Vulnerabilities - Apple has released security advisories to address vulnerabilities within Apple Sarfari, Apple macOS, as well as Apple iTunes products, in which successful local/remote exploitation may result in arbitrary code execution, cross-site scripting (XSS), sensitive information disclosure, elevated privileges and/or denial of service.

Research for today:

Nagios vulnerabilities that may result in elevated privileges and/or arbitrary code execution.

ISVM Acknowledgement(s):

- NSTR

ISVM Compliance(s):

- NSTR

Vulnerability Assessment Scans:

- NSTR

US-CERT C-CAR Data Call

- **Binding Operational Directive (BOD-16-02) for all Federal civilian executive branch departments and agencies on Threats to Network Infrastructure Devices has been approved and signed by the DHS Secretary.**

- **Perform all actions in the "Solution" sections of the "Technical Annexes" to the NCCIC Analysis Report AR-16-20173 no later than 45 days after issuance of this Directive.**
- **Report to DHS ESOC, either full mitigation or provide a detailed plan of action and milestones explaining the constraints preventing mitigation and the associated compensating controls established no later than 45 days after issuance of this Directive. (11/11/2016)**
- **Provide additional reports or plans of action and milestones every 30 days thereafter until full mitigation is achieved.**
- We are now issuing a high-priority "DHS Enterprise Data Call," in order to obtain a departmental security posture/status related to recently-discovered "Critical" vulnerabilities (affecting Cisco Routers, Cisco Adaptive Security Appliances (ASA) and other vendor firewall devices).
- The following provides general background information and/or context on the three (3) groups of vulnerabilities being addressed via this data call.
    - **Hacking tools targeting firewalls:** A group calling themselves "The Shadow Brokers" claims to have obtained a large-set of hacking tools from the "Equation Group." Said large-set of cyber-weapons (exploits, implants and hacking tools) have targeted firewall devices from vendors such as Cisco, Fortinet, Juniper, WatchGuard, TOPSEC and Huawei.
    - **Cisco ROMMON Integrity:** Based on technical data obtained from focused, in-depth malware analysis, US-CERT was able to identify detection methods/strategies to defend against the involved "Threat Actor."
    - **Cisco Adaptive Security Appliance:** US-CERT received several reports of compromised Cisco Adaptive Security Appliance (ASA) devices. The ASA devices were modified in an unauthorized manner, which resulted in the occurrence of malicious "redirects" (for social engineering/credential-harvesting purposes).
- References:
    - ISVM: 2016-010-0-A-Cisco Adaptive Security Appliance Vulnerabilities
    - ISVM: 2016-010-1-A-Cisco Adaptive Security Appliance Vulnerabilities
    - ISVM: 2016-011-0-A-Fortigate Vulnerability
    - ISVM: 2016-013-0-A-Cisco ASA Clientless SSL VPN Vulnerability
    - ISVM: 2016-016-0-TA-Juniper NetScreen ScreenOS Vulnerability
    - US-CERT Documents:
        - AR-16-20150-Network_Analysis_Report_on_Compromised_Cisco_ASA_Devices.pdf
        - AR-16-20173_The_Increasing_Threat_to_Network_Infrastructure_Devices.pdf
        - CISCO Malware-detection strategy-2.0.pdf

        - ShadowBroker-EquationGroupHackv1.5.pdf
    - **UPDATE: Ensure to include Estimated Completion Date**
    - **Due weekly, Wednesday 1200 EST**

- **Apple iOS Vulnerability Data Call**
    - **Due Weekly Friday NLT 1600 EST.**
    - Please provide the total number of GFE Apple Mobile Devices, per DHS Component, that have been upgraded to the most current Apple iOS Version.
    - Please provide the total number of GFE Apple Mobile Devices, per DHS Component, that have NOT been successfully upgraded to the most current Apple iOS Version.
    - For those devices that have NOT been properly updated, please provide an explanation as to why this upgrade has not occurred.
    - For those devices that have NOT been properly updated, please provide an Estimated Time to Completion.
    - Reference: 2016-012-0-A-Apple iOS Vulnerabilities

- **Secure Socket Layer (SSL) Version 2 and 3 Vulnerability Data Call:**
    - We have received new guidance from DHS CISO senior leadership for this high-priority "DHS Enterprise Data Call," in order to obtain a departmental security posture status - surrounding a recently-discovered "Critical" vulnerability in devices that utilize "Secure Socket Layer (SSL) versions 2 and 3." If exploited, this vulnerability can result in a successful "cross-protocol attack" being carried-out, potentially resulting in undesirable/unauthorized information disclosures. To meet reporting requirements, the DHS ESOC requires all DHS Component SOC responses weekly on **Friday NLT 1600 EST**.
    - Changes have been updated to the data call and the following information will now be collected:
        - Total Number of Devices Affected
        - Total Number of Devices with available patches/fix (based on vendor(s) releases)
        - Total Number of Devices Remediated
    - Reference: ISVM 2016-053-0-B-OpenSSL DROWN Vulnerabilities

- **Bash Vuln Reporting requirements:**
    - For any remaining unpatched systems, each component will need to determine which systems are internal and external.
    - Numbers will be reported to OMB daily. Please focus on patching external facing systems.
    - Reference: ISVM 2014-009-0-A-GNU Bash Code Injection Vulnerability

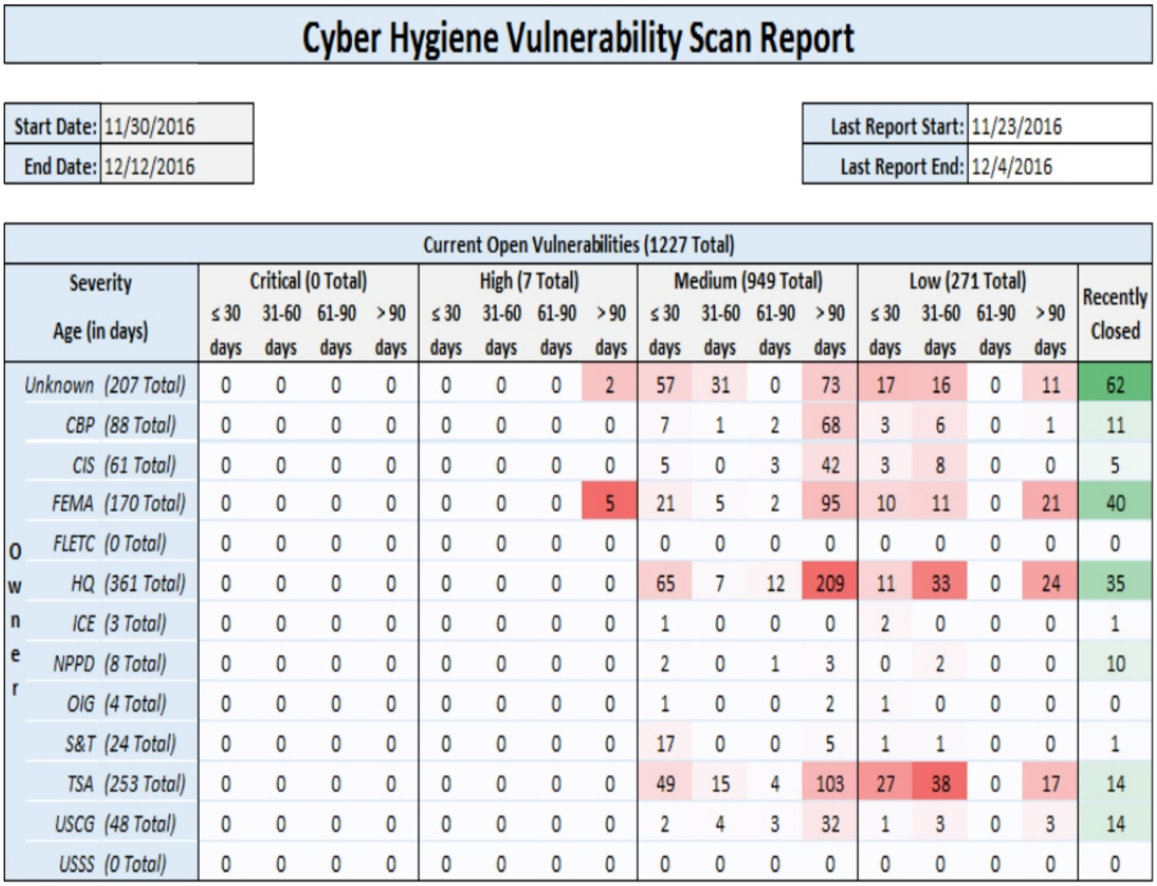
- **Cyber Hygiene Vulnerability Scan Report**

DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

Below you will see the Dashboard for this week's Cyber Hygiene Report. To view more detailed information regarding the vulnerabilities, please see the Scan Results posted on SharePoint.

Make sure to take a look at the Weekly IP Updates tab, specifically at IP's owned by your Component and those marked as having an unknown owner. It would be very much appreciated if you would reply back to me verifying ownership of these IPs. Also, please let me know if you have any updates to contribute to this list, any questions regarding these changes or the current data, or any difficulty accessing the SharePoint link.

If you have any immediate technical questions please reach out to (b)(6)



Cyber Hygiene Vulnerability Scan Report

Start Date:	11/30/2016
End Date:	12/12/2016

Last Report Start:	11/23/2016
Last Report End:	12/4/2016

Current Open Vulnerabilities (1227 Total)																		
	Severity	Critical (0 Total)				High (7 Total)				Medium (949 Total)				Low (271 Total)				Recently Closed
	Age (in days)	≤ 30 days	31-60 days	61-90 days	> 90 days	≤ 30 days	31-60 days	61-90 days	> 90 days	≤ 30 days	31-60 days	61-90 days	> 90 days	≤ 30 days	31-60 days	61-90 days	> 90 days	
Owner	Unknown (207 Total)	0	0	0	0	0	0	0	2	57	31	0	73	17	16	0	11	62
	CBP (88 Total)	0	0	0	0	0	0	0	0	7	1	2	68	3	6	0	1	11
	CIS (61 Total)	0	0	0	0	0	0	0	0	5	0	3	42	3	8	0	0	5
	FEMA (170 Total)	0	0	0	0	0	0	0	5	21	5	2	95	10	11	0	21	40
	FLETC (0 Total)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	HQ (361 Total)	0	0	0	0	0	0	0	0	65	7	12	209	11	33	0	24	35
	ICE (3 Total)	0	0	0	0	0	0	0	0	1	0	0	0	2	0	0	0	1
	NPPD (8 Total)	0	0	0	0	0	0	0	0	2	0	1	3	0	2	0	0	10
	OIG (4 Total)	0	0	0	0	0	0	0	0	1	0	0	2	1	0	0	0	0
	S&T (24 Total)	0	0	0	0	0	0	0	0	17	0	0	5	1	1	0	0	1
	TSA (253 Total)	0	0	0	0	0	0	0	0	49	15	4	103	27	38	0	17	14
	USCG (48 Total)	0	0	0	0	0	0	0	0	2	4	3	32	1	3	0	3	14
	USSS (0 Total)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

There continues to be an incomplete reflection of component scanning activity as indicated by the representation of opened/closed/pending VAT records within EOCOnline. The DHS ESOC VAT continues to request for VAT record creation within the EOCOnline Portal reflecting component's scanning activities. DHS ESOC analysts routinely receive requests from components for assistance with reporting/investigating unexpected network activity, which could be perceived as potentially malicious traffic. A simple query into the VAT records would afford our team with the ability to quickly diffuse any unnecessary alarm(s), or quickly respond appropriately to bad-actors attempting to compromise the network.

2.3.4.1 Component Vulnerability Assessments

> *"Components shall prepare schedules including complete coverage of all systems and shall conduct monthly credentialed vulnerability assessments. The schedules must be provided to the DHS VMB through the Government provided system of record and may be updated as often as necessary. Schedules, updates, and assessment and remediation results will be provided to DHS VMB no less than quarterly and upon request in periodic data calls. Each scan shall be posted in the Government-provided system of record as an in-process scan for each Component. Scan results shall be uploaded into Enterprise Vulnerability Management System (EVMS). Components shall declare any inability to perform vulnerability assessments, analysis, penetration testing or reporting to the DHS VMB and arrange for an alternate solution."*
>
> Source: 4300A, Attachment O, Section 2.3.4.1

For further inquiries regarding ISVM notifications or vulnerabilities assessments, please contact DHS_SOC_VAT (b)(6)

DHS ESOC Threat Intelligence

NSTR

DHS ESOC IDS:

NSTR

DHS ESOC Engineering:

NSTR

DHS ESOC E-mail Team:

2016-12-160 Users: 1 (USCIS 1)

Subject: "incoming report"

Sender: (b)(6)

Date: 12/16

Type: Credential Harvesting

Attachment: NA

Callbacks: hxxp://rdastudio[d]net/rage/ayo1/ayo1/index[d]html

2016-12-161 Users: search underway…

Subject: [WARNING: MESSAGE ENCRYPTED][SPAM]*xxxx

Sender: search underway…

Date: 12/18

Type: Malicious Logic

Attachment: *****.zip

Callbacks: hl3gj7zkxjvo6cra.onion[.]to

DHS ESOC Incident Response (IR):

SENS: 10

2016-12-161	ML-Phishing-Campaign
2016-12-135	MU-CBP-DHS
2016-12-160	credential Phishing

2016-12-157	S&T_STCS_Domain_Admin
2016-12-152	Investigation Un
2016-12-158	Investigation Un
2016-12-159	MU-CBP-DHS
2016-12-154	IU-CBP-DHS
2016-12-153	USCG Recruiting Command
2016-12-155	IM48253

Incidents: 8

2016-12-075	MU-CBP-DHS
2016-12-074	Misuse
2016-12-073	Misuse
2016-12-072	Misuse
2016-12-071	USCG Recruiting Command
2016-12-070	PII Non-Technical Spill
2016-12-069	PII Non-Technical Spill
2016-12-068	MU-CBP-DHS

Blocks: 5

rdastudio[.]net

The DHS ESOC received Fire Eye alerts for phishing email from sender "sawerning17@benton.k12.ia.us" using subject line "incoming report" was delivered to a DHS user.The email solicits the user to click a link to see the attached document. OOB analysis shows the link "hxxp://rdastudio[d]net/rage/ayo1/ayo1/index[d]html" opens a page asking for email username and password Recommending blocking the domains to enhance DHS security.

118[.]193[.]243[.]149

171[.]83[.]99[.]175

184[.]28[.]218[.]190

23[.]76[.]205[.]110

US-CERT reported to DHS ESOC on December 16th, 2016 of known MalSpam delivering Locky ransomware. DHS ESOC recommends blocking associated IPs, in order to strengthen our security posture.