TLP:AMBER

Homeland Security

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

Reference Number: JAR-16-20223 **October 14, 2016**

Threats to Federal, State, and Local Government Systems

Summary

Government systems present rich and attractive targets for computer intrusions. This problem is not unique to the Federal Government or individual states—it is shared across the nation. The keys to good cybersecurity are awareness and constant vigilance.

To address threats to government systems, this Joint Analysis Report (JAR) provides indicators associated with recent compromises and exploit attempts, along with prevention and mitigation recommendations.

This JAR is the result of efforts between the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) to highlight known cyber threats. DHS and the FBI continue to pursue related information of threats to federal, state, and local government systems and as such, further releases of technical information may be forthcoming.

Technical Details

Indicators of Compromise (IOC)

IOCs are provided within the accompanying .csv and .stix files of JAR-16-20223

Yara Signature

```
rule PAS_TOOL_PHP_WEB_KIT
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset"
condition:
(filesize > 20KB and filesize < 22KB) and
#cookie == 2 and
#isset == 3 and
all of them

}
```

Recommended Mitigations

What actions should I take with these indicators?

DHS recommends that network administrators review the IP addresses, file hashes, and YARA signature provided. The review of network perimeter netflow or firewall logs will assist in determining if successful connections have been experienced on your network.

When reviewing network perimeter logs for the IP addresses, organizations may find numerous instances of these IPs attempting to connect to their systems. Upon reviewing the traffic from these IPs, some traffic may resemble vulnerability scanning or browsing of legitimate public facing services, such as HTTP, HTTPS, or FTP. Connections from these IPs may be performing vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. If vulnerable sites were identified during the scanning, attempts to exploit the vulnerabilities may be experienced.

Network administrators are encouraged to check their public-facing websites for the malicious file hashes and implement inspection of the YARA signature if possible.

What are the threats from these indicators?

Malicious actors may use a variety of methods to interfere with websites and databases. Some methods of attack are listed below and provide guidance that is applicable to many other computer networks.

- ***Injection Flaws*** are broad web application attack techniques that attempt to send commands to a browser, database, or other system, allowing a regular user to control behavior. The most common example is SQL injection, which subverts the relationship between a webpage and its supporting database, typically to obtain information contained inside the database. Another form is command injection, where an untrusted user is able to send commands to operating systems supporting a web application or database. See the United States Computer Emergency Readiness Team (US-CERT) Publication on SQL Injection for more information.
- ***Cross-site scripting (XSS) vulnerabilities*** allow threat actors to insert and execute unauthorized code in web applications. Successful XSS attacks on websites can provide the attacker unauthorized access. For prevention and mitigation strategies against XSS, see US-CERT's Alert on Compromised Web Servers and Web Shells.
- ***Server vulnerabilities*** may be exploited to allow unauthorized access to sensitive information. An attack against a poorly configured server may allow an adversary access to critical information including any websites or databases hosted on the server. See US-CERT's Tip on Website Security for additional information.

DHS encourages network administrators to implement the recommendations below, which can prevent as many as 85 percent of targeted cyber attacks. These strategies are common sense to many, but DHS continues to see intrusions because organizations fail to use these basic measures.

- **Patch applications and operating systems –** Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- **Application whitelisting –** Whitelisting is one of the best security strategies as it allows only specified programs to run while blocking all others, including malicious software.
- **Restrict administrative privileges –** This may prevent malicious software from running or limit its capability to spread through the network.
- **Input validation –** Input validation is a method of sanitizing untrusted user input provided by users of a web application, and may prevent many types of web application security flaws, such as SQLi, XSS, and command injection.

- **Understanding firewalls –** When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

A commitment to good cybersecurity and best practices is critical to protecting Internet-facing web services. Here are some questions you may want to ask of your organization to help prevent attacks against websites and databases:

1. **Backups**: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training**: Have we trained staff on cybersecurity best practices?
4. **Vulnerability Scanning & Patching**: Have we implemented regular scans of our network and systems, and appropriate patching of known system vulnerabilities?
5. **Application Whitelisting**: Do we allow only approved programs to run on our networks?
6. **Incident Response**: Do we have an incident response plan, and have we practiced it?
7. **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing**: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

How do I respond to unauthorized access to my network?

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact DHS or law enforcement immediately. We encourage you to contact DHS's National Cybersecurity and Communications Integration Center (NCCIC) (NCCICcustomerservice@hq.dhs.gov or 888-282-0870), or the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

How do I enhance my organization's cybersecurity posture?

DHS offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Other resources include:

- **The Cybersecurity Framework (Framework)**, developed by the National Institute of Standards and Technology (NIST) in collaboration with the public and private sectors, is a tool that can improve the cybersecurity readiness of entities. The Framework enables entities, regardless of size, degree of cyber risk, or cyber sophistication, to apply principles and best practices of risk management to improve the security and resiliency of critical infrastructure. The Framework provides standards, guidelines, and practices that are working effectively today. It consists of three parts—the Framework Core, the Framework Profile, and Framework Implementation Tiers—and emphasizes five functions: Identify, Protect, Detect, Respond, and Recover. Use of the Framework is strictly voluntary. For more information, visit https://www.nist.gov/cyberframework or email cyberframework@nist.gov.

- **The Cyber Security Advisors (CSA)** program bolsters cybersecurity preparedness, risk mitigation, and incident response capabilities of critical infrastructure entities and more closely align them with the Federal Government. CSAs are DHS personnel assigned to districts throughout the country and territories, with at least 1 advisor per the 10 CSA regions that mirror the Federal Emergency Management Agency regions. For more information, email cyberadvisor@hq.dhs.gov.

- **Cyber Resilience Review (CRR)** is a no-cost, voluntary assessment to evaluate and enhance cybersecurity within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators of an entity's operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress and crisis. Visit https://www.cert.org/resilience/rmm.html to learn more about the CERT Resilience Management Model.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. Include the JAR reference number (JAR-16-20223) in the subject line of all email correspondence. For any questions related to this report, please contact NCCIC or the FBI at:

NCCIC:
Phone: +1-888-282-0780
Email: NCCICcustomerservice@hq.dhs.gov

FBI:
Phone: +1-855-292-3937
Email: cywatch@ic.fbi.gov

Feedback

NCCIC continuously strives to improve its products and services. You can help by answering a few short questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.