



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Early Warning and Indicator Notice (EWIN)-11-035-01B **UPDATE**

February 9, 2011

US-CERT Early Warning and Indicator Notice

Information in this US-CERT Early Warning and Indicator Notice represents initial reporting of suspected malicious activity on critical infrastructure / key resources (CIKR) networks. This information should only be distributed to organization personnel who implement network security measures or make cybersecurity decisions.

Technical Details

US-CERT received information containing indicators regarding malicious activity within the CI/KR community and used them to develop signatures listed below. Organizations may find the snort signatures helpful in detecting malicious activity on their systems. US-CERT encourages organizations to review the signatures and determine if they will be useful and appropriate for overall detection strategy. While these signatures have been effective for US-CERT's detection efforts, it is the responsibility of each organization to determine if it is an effective approach given their specific environments. US-CERT also encourages each organization to test these signatures before deploying them on their production network whenever possible.

UPDATE B (1 of 3): After receiving additional information, US-CERT revised signature #2 (pg. 3) and #10 (pg. 4) to include different IP addresses. Please use the updated versions instead of the previous signature #2 and #10.

US-CERT requests:

- Notification of EWIN receipt e-mailed to soc@us-cert.gov with the e-mail subject "Receipt: EWIN-11-035-01B".
- Notification of actions taken (e.g., deployment, customization, issues) to soc@us-cert.gov with the e-mail subject "Actions: EWIN-11-035-01B".
- **Notification if signatures alert via e-mail (soc@us-cert.gov) with the e-mail subject "ALERT: EWIN-11-035-01B" or phone (1-888-282-0870) for additional assistance and instructions.**

Operational Security Recommendations and Handling Instructions

Due to the nature of the threat, the approach to mitigation and response efforts must assume that the Windows Active Directory (AD) infrastructure is fully compromised. Any indication of suspicious activity related to these signatures should follow the steps below:

- Logs (e.g., firewall, proxy, Domain Name Service [DNS], network flow, application, and security event) should be analyzed offline. They must be centrally collected and searched using systems that are outside the organization's normal enterprise control and authentication mechanisms to preclude the ability of malicious actors to see the list of search terms and indicators.
- If the organization's intrusion detection system (IDS) or security information and event management (SIEM) tools use Windows AD, the systems must first be converted to standalone, local authentication with a limited user access list.
- Initial population or upload of signatures into IDS or SIEM tools should be done from workstations not part of a Windows AD.

US-CERT advises organizations to take defensive steps as appropriate to mitigate and minimize the cyber threat to its core and critical business functions.

If malicious actors are present within the organization's network, they may have been present for a period of time. Thus, the organization's approach should balance immediate blocks to protect from immediate harm against the ability to detect and monitor the organization's resources for malicious activity in order to ensure full remediation. For example, immediate blocks could prevent further surreptitious monitoring of the malicious actors' activities that could be used to detect other communication channels or infected internal systems.

Guidance for Investigating Signature Alerts

Signatures 1-13 are based on IP addresses, network administrators should investigate the nature of the activity associated with the alerts to eliminate any false positives. These signatures are designed to detect the initial connection between the organization and the IP address. This design may make it difficult to assess what data was passed, if any, between organization systems and the IP address without the ability to analyze associated historical packet capture data. IP addresses can host multiple domains so activity should be connected to both the IP address and domain listed in the signature message.

If activity is detected to the IP address but not the domain, check for beaconing, infiltration, exfiltration, or other suspicious activity to/from the IP.

Signatures 14-16 are designed to alert on specific domains with ties to suspicious and/or malicious activity. As such, these signatures are a stronger indication of anomalous activity. If these signatures alert, network administrations must identify the system or systems attempting to resolve these domains by reviewing DNS logs. After identifying these systems, network administrators should disconnect the system from the network and obtain a system and memory images for analysis. Please contact US-CERT for additional instructions for submitting forensic images or malware for analysis.

IP ADDRESS-BASED SIGNATURES

1. alert tcp any any <> 188.72.242.42 any (msg:"188.72.242.42 Connection Attempt Associated with livejettsupport net"; flags:S; sid:nnn; rev:1; gid:1; classtype:bad-unknown;)
2. **UPDATE B (2 of 3):** alert tcp any any <> 193.202.17.16 any (msg:"193.202.17.16 Connection Attempt"; flags:S; sid:nnn; rev:1; gid:1; classtype:bad-unknown;)
3. alert tcp any any <> 205.234.236.130 any (msg:"205.234.236.130 Connection Attempt Associated with boston quinthosting com"; flags:S; sid:nnn; rev:1; gid:1; classtype:bad-unknown;)
4. alert tcp any any <> 205.234.236.131 any (msg:"205.234.236.131 Connection Attempt Associated with boston quinthosting com"; flags:S; sid:nnn; rev:1; gid:1; classtype:bad-unknown;)
5. alert tcp any any <> 205.234.236.132 any (msg:"205.234.236.132 Connection Attempt Associated with boston quinthosting com"; flags:S; sid:nnn; rev:1; gid:1; classtype: bad-unknown;)
6. alert tcp any any <> 205.234.236.133 any (msg:"205.234.236.133 Connection Attempt Associated with boston quinthosting com"; flags:S; sid:nnn; rev:1; gid:1; classtype:bad-unknown;)
7. alert tcp any any <> 205.234.236.20 any (msg:"205.234.236.20 Connection Attempt Associated with boston quinthosting com"; flags:S; sid:nnn; rev:1; gid:1; classtype:bad-unknown;)

Reference

- EWIN-10-363-01 Malware Analysis

Contact Information

(UNCLASS) Phone: 1-888-282-0870

(UNCLASS) E-mail: soc@us-cert.gov

Document FAQ

What is an EWIN? An Early Warning and Indicator Notice is intended to provide indicators derived from new cyber incidents and/or malicious code that can pose a threat to federal and state government, critical infrastructure, private industry, or a country CERT that US-CERT collaborates with.

I see that this document is labeled as UNCLASSIFIED. Can I distribute this to other people? With the case of a EWIN, this is defined as a person or group that has a direct role in securing federal and state networks. If necessary, please contact US-CERT for clarification or specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed, or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.