Wisconsin Statewide Intelligence Center (WSIC)
608.242.5393 • 888.DCI.WSIC • Fax: 608.240.3592 • wsic@doj.state.wi.us

WSIC Analytic Note

May 28, 2024

(TLP: WHITE) The Wisconsin Statewide Intelligence Center (WSIC) developed this intelligence product based on information from trusted third-party. If you have information or suggestions for future products, please e-mail wsic@doj.state.wi.us

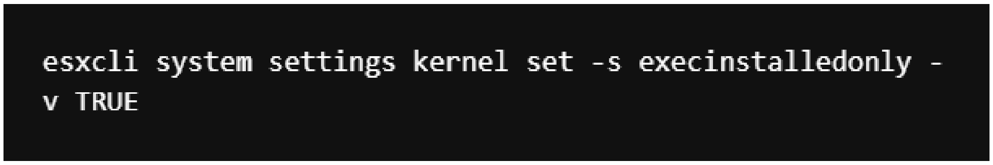
TLP: WHITE Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction. For further information on the traffic light protocol, please see https://www.us-cert.gov/tlp

(TLP: WHITE) Emerging Ransomware Threat Actor in Wisconsin

(TLP: WHITE) WSIC Comment: Please contact the Wisconsin Statewide Intelligence Center, e-mail (wsic@doj.state.wi.us) or phone (608-242-5393), if you need additional information. To report a cybersecurity incident to the WSIC, please visit https://wifusion.widoj.gov and click on the “Report Cyber Incident” button.

(TLP: WHITE) As of 05/01/2024, WSIC has seen an increase in ransomware attacks impacting the state of Wisconsin. During recent incidents, WSIC identified an emerging threat actor known as “Fog”. This threat actor has been targeting ESXi servers and encrypting VMware Virtual Machine Disks (VMDKs) and log files at the hypervisor or host level, after gaining access to the root user credentials, even if complex, protected passwords were in use. Most of these attacks appear to be utilizing past practices of compromising credentials through lack of security protocols, use of exposed or unpatched firewall/VPNs, and most commonly, different types of phishing attacks. Once in the systems, the threat actors encrypt important documents and files that are then held for ransom.

(TLP: WHITE) **ANALYST NOTE:** When securing ESXi servers, WSIC recommends using named administrators and administrator’s rights and roles to limit permission as best practice. Root users who can access the ESXi host should only be logging in using the direct console user interface and only use SSH when performing troubleshooting or supporting tasks. After each use, the SSH should be disabled to limit any kind of unauthorized access. Additionally, investigate different ESXi lockdown modes on the VMware Docs website and determine what best fits your organization. Lastly, ESXi host default configuration settings can also be changed to enable execInstalledOnly, which is an advanced setting where the VMware kernel will only be able to execute signed VIB files. After the ESXi server is rebooted, the execution of custom code should then be prohibited. (see Figure 1).



```
esxcli system settings kernel set -s execinstalledonly -
v TRUE
```

(TLP: WHITE) Figure 1: command to run to enable execInstalledOnly.

(TLP: WHITE) Research by WSIC indicates that FOG is a newer ransomware group that has targeted multiple school districts, churches, and non-profit organizations with at least two reported incidents in the state of Wisconsin. WSIC strongly recommends that users review log settings on servers and firewalls, with the goal of increasing logging time frames and capacities while considering sending the logs to a Security Information and Event management (SIEM) or any other logging servers to preserve and protect logs in the event of a cyber incident. While the user review of log settings won't prevent an attack, preserved logs provide incident responders increased situational awareness during post-intrusion response and assist in enhancing security protocols.

(TLP:WHITE) For More Information on securing VMware Virtual Machine

- (TLP: WHITE) https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-E9B71B85-FBA3-447C-8A60-DEE2AE1A405A.html
- (TLP: WHITE) https://www.truesec.com/hub/blog/secure-your-vmware-esxi-hosts-against-ransomware

(TLP:WHITE) **Sources:**

(TLP:WHITE) Securing the ESXi Hypervisor. (n.d.). https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-E9B71B85-FBA3-447C-8A60-DEE2AE1A405A.html

(TLP:WHITE) Configuring and managing lockdown mode on esxi hosts. Available at: https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html (Accessed: 16 May 2024).

(TLP:WHITE) (n.d.). Secure Your VMware ESXi Hosts Against Ransomware. Truesec. (n.d.). https://www.truesec.com/hub/blog/secure-your-vmware-esxi-hosts-against-ransomware

Reporting Notice: Please contact the Wisconsin Statewide Intelligence Center, e-mail address wsic@doj.state.wi.us or phone 608-242-5393, if you need additional information. To report a cybersecurity incident to the WSIC, please visit https://wifusion.org and click on the "Report Cyber Incident" button.

This document addresses the following Homeland Security Standing Information Needs (HSEC SINS) and the Wisconsin Statewide Intelligence Center Standing Information Needs (WSIC SINS): 1.2.2, 1.2.3, 1.5.2, 1.6.2.20, 1.6.2.22, 1.8.1, 1.9.6, and 1.10.1.

For Administrative Purposes Only:
Produced: W3C20A20
Contributed:
Reviewed: W10C13A20
Updated: