UBISTOR

SECURITY BULLETIN

Cybersecurity Advisory on Newly Identified Truebot Malware Variants and MOVEit Vulnerability

Release Date: July 17, 2023

CISA and Partners Release Joint Cybersecurity Advisory on Newly Identified Truebot Malware Variants and MOVEit Vulnerability

Introduction

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known CL0P ransomware IOCs and TTPs identified through FBI investigations as recently as June 2023.

According to open source information, beginning on May 27, 2023, CL0P Ransomware Gang, also known as TA505, began exploiting a previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution known as MOVEit Transfer. Internet-facing MOVEit Transfer web applications were infected with a web shell named LEMURLOOT, which was then used to steal data from underlying MOVEit Transfer databases. In similar spates of activity, TA505 conducted zero-day-exploit-driven campaigns against Accellion File Transfer Appliance (FTA) devices in 2020 and 2021 and Fortra/Linoma GoAnywhere MFT servers in early 2023.

FBI and CISA encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of CL0P ransomware and other ransomware incidents.to protect your technology stack is to educate yourself and your team on potential firewall vulnerabilities and ensure that your system has all the latest updates and additional security features to protect your company from these evolving threats.

To learn more about this vulnerability click on the following link: https://www.cisa.gov/sites/default/files/2023-06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf

Truebot Malware

Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigations (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Canadian Centre for Cyber Security (CCCS) released a joint Cybersecurity Advisory (CSA), Increased Truebot Activity Infects U.S. and Canada Based Networks, to help organizations detect and protect against newly identified Truebot malware variants. Based on confirmation from open-source reporting and analytical findings of Truebot variants, the four organizations assess cyber threat actors leveraged the malware through phishing campaigns containing malicious redirect hyperlinks.

Additionally, newer versions of Truebot malware allow malicious actors to gain initial access by exploiting a known vulnerability with Netwrix Auditor application (CVE-2022-31199). As recently as May 2023, cyber threat actors used this common vulnerability and exposure to deliver new Truebot malware variants and to collect and exfiltrate information against organizations in the U.S. and Canada.

- CISA, FBI, MS-ISAC, and the CCCS encourage all organizations to review this joint advisory and implement the recommended mitigations contained therein—including applying patches to CVE-2022-31199, to reduce the likelihood and impact of Truebot activity, as well as other ransomware related incidents. To report incidents and anomalous activity, please contact one of the following organizations:
- CISA, either through the agency's online tool (cisa.gov/report) or the 24/7 Operations Center at report@cisa.gov or (888) 282-0870.
- FBI via a local field office.
- State, local, tribal, and territorial (SLTT) government entities can report to the MS-ISAC (SOC@cisecurity.org or 866-787-4522).
- Organizations are also encouraged to visit StopRansomware.gov—which provides a range of free U.S. government resources and services that can help bolster cyber hygiene, cybersecurity posture and reduce risk to ransomware, and contains an updated Joint #StopRansomware Guide.

To learn more about this vulnerability click here: https://www.cisa.gov/news-events/alerts/2023/07/06/cisa-and-partners-release-joint-cybersecurity-advisory-newly-identified-truebot-malware-variants

SafeStor Edge Protection Protects Your Business

Defending against the most potential threats requires up-to-date cyber intelligence pulled from multiple reputable sources. To help protect your business, UbiStor synthesizes data from more than 30 threat intelligence providers and uses this knowledge to prepare you for any threat it could potentially face.

UbiStor improves your security posture by blocking inbound and outbound threats to enable an ideal protected network to improve firewall efficiency and enhance your existing security stack. Mitigating false positives quickly and intuitively using automation saves you time and resources on otherwise consuming manual tasks.

Working with your IT team we implement and manage our edge protection services and close gaps that put your security at risk. It's easy to use and can connect to anything in your technology stack.

UbiStor's SafeStor Edge Protection service has monitored and blocked the IPs associated with MOVEit since June 7, 2023.

Our vast intelligence repository leverages the latest information to protect against cyber criminals.

- SafeStor Edge Protection autonomously blocks malicious inbound and outbound connections confirmed by leading cyber intelligence agencies.
- CL0p group targets file transfer programs, accessing data within and outside the company's network, holding it for ransom.
- UbiStor offers a free Threat Assessment that will show you what and how many malicious connections, inbound and outbound, your firewall is making, the connections our service will block, and what threat actors are currently inside your network.

  Click here to request a free assessment: https://www.ubistor.com/threat-assessment/

About UbiStor

For today's modern business, efficiency is key and utilizing a top-tier Managed Service Provider like UbiStor can streamline workflows, mitigate risk, and offer improved flexibility. In the current technology landscape, your company must respond quickly to cyber threats, disasters, employee error and hardware failure. Outsourcing the management of your data protection and disaster recovery strategy can save your IT team countless hours, allowing them to focus on more business-critical initiatives and ensure you are protected when disaster strikes.

Since 2001, UbiStor has been developing bulletproof data protection and disaster recovery strategies for their customers. With a consultative approach, UbiStor can cultivate strong relationships and perfectly constructed solutions for their customers, ensuring they are set up for success.

Learn more at https://www.ubistor.com/products/safestor-edge-protection/