New Multi-Platform Xbash Packs Obfuscation, Ransomware, Coinminer, Worm and Botnet

Archived: 2026-04-05 19:55:04 UTC

Researchers discovered a new malware family, named Xbash, targeting servers of various platforms, with four different versions seen in the wild actively seeking unprotected services, exploiting vulnerabilities, and deleting databases in Linux and Microsoft systems. Xbash evades detection, scans targets from IP addresses and domain names, brute forcing, and combines ransomware, cryptocurrency coinmining, worm, and scanner capabilities. Reverse analysis found an estimated $6,000 worth of Bitcoin wired from approximately 48 victims to the C&C IP address, though evidence of data recovery has yet to be seen.

[Read: The evolution of ransomware]

Xbash specifically targets Linux servers with ransomware and botnet installations, and Windows servers for coinminer installs and propagation. Developed using Python, attackers used legitimate tool PyInstaller to distribute the Linux ELF executables, with Redis services enabling Xbash to determine if the system is running on Windows or not. Once it confirms that it's running on a Windows server, a hijacked Javascript or VBScript payload will download and execute a coinminer. It also has obfuscation capabilities that tries to bypass static analysis to avoid detection.

[Read: Cryptocurrency-mining malware targets Kodi users on Windows, Linuxnews- cybercrime-and-digital-threats]

Unlike recent variants of Mirai and Gafgytnews article that target vulnerable Linux systems via randomly generated IP addresses, Xbash also scans and trawls through domain names. The C&C scans for specific destinations' known vulnerabilities in Hadoop, Redis and ActiveMQ (CVE-2016-3088) for self-propagation. Hadoop's unauthenticated command execution flaw discovered in October 2016, as well as the Redis arbitrary and remote command execution vulnerability disclosed in October 2015, have yet to be assigned CVE numbers. Based on the active C&C traffic, it scans and probes for open TCP or UDP ports such as HTTP, VNC, MySQL/MariaDB, Telnet, FTP, MongoDB, RDP, ElasticSearch, Oracle Database, CouchDB, Rlogin and PostgreSQL. While the malware uses a weak username and password dictionary to brute force itself into the service, it is also able to update its set from the C&C server, delete all the databases, and display the ransom message.

Security researchers note this to be the first malware family to pack ransomware, coinmining, and worm capabilities that target services for both Linux and Windows.open on a new tab Further, the samples of Xbash indicate developing new capabilities of scanning for eventual implementation of intranet infection in enterprises, much like WannaCry and Petya.

[Read: WannaCry/Wcry Ransomware: How to defend against itnews- cybercrime-and-digital-threats]

Threats such as Xbash will continue to evolve as cybercriminals find more ways to profit from legitimate businesses and enterprises. Here are some best practices to protect enterprise systems from these kind of threats:

- Frequently change your passwords and make them complicated, from the gateway to the endpoint. Practice good password hygiene, and avoid reusing credentials on multiple user accounts.
- Regularly install system updates and patches for your systems once released by legitimate vendors.
- Regularly back up your files. Practice the 3-2-1 system to minimize or mitigate data loss.

Malware related to this threat are detected as:

- Ransom.Linux.XBASH.A
- Ransom.Linux.XBASH.AB
- Ransom.Linux.XBASH.AC
- Ransom.Linux.XBASH.AD
- Ransom.Linux.XBASH.AE
- Ransom.Linux.XBASH.AF
- Trojan.JS.POWLOAD.AA
- Trojan.VBS.POWLOAD.AB
- Trojan.Win32.INFOSTEAL.TIDAOCN
- Coinminer.Win32.MALXMR.AX
- Coinminer_TOOLXMR.SMB-WIN64
- Coinminer.Unix.MALXMR.AA

Trend Micro™ Endpoint Securityproducts offers the broadest range of defense against the changing, advanced threat landscape. Trend Micro™ OfficeScanproducts™ infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across any user activity and any endpoint. It constantly learns, adapts, and automatically shares threat intelligence across your environment. All of this modern threat security technology is made simple for your organization with central visibility, management, and reporting.

Trend Micro™ Deep Discoveryproducts™ protects customers from this threat via these Deep Discovery Inspector (DDI) rules:

- 1536 - HTTP Request to a malware Command and Control Site
- 2573 - MINER - TCP (Request)

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-

-
-
-
  - The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
  - Complexity and Visibility Gaps in Power Automatenews article
-
  - Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
  - Azure Control Plane Threat Detection With TrendAI Vision One™news article
-
  - The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
  - Ransomware Spotlight: DragonForcenews article
-
  - Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
  - The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---