Oct 05 2023

NETMANAGEIT

Intelligence Report

Analyzing LuoBot: A Node.js Malware with Vast Capabilities

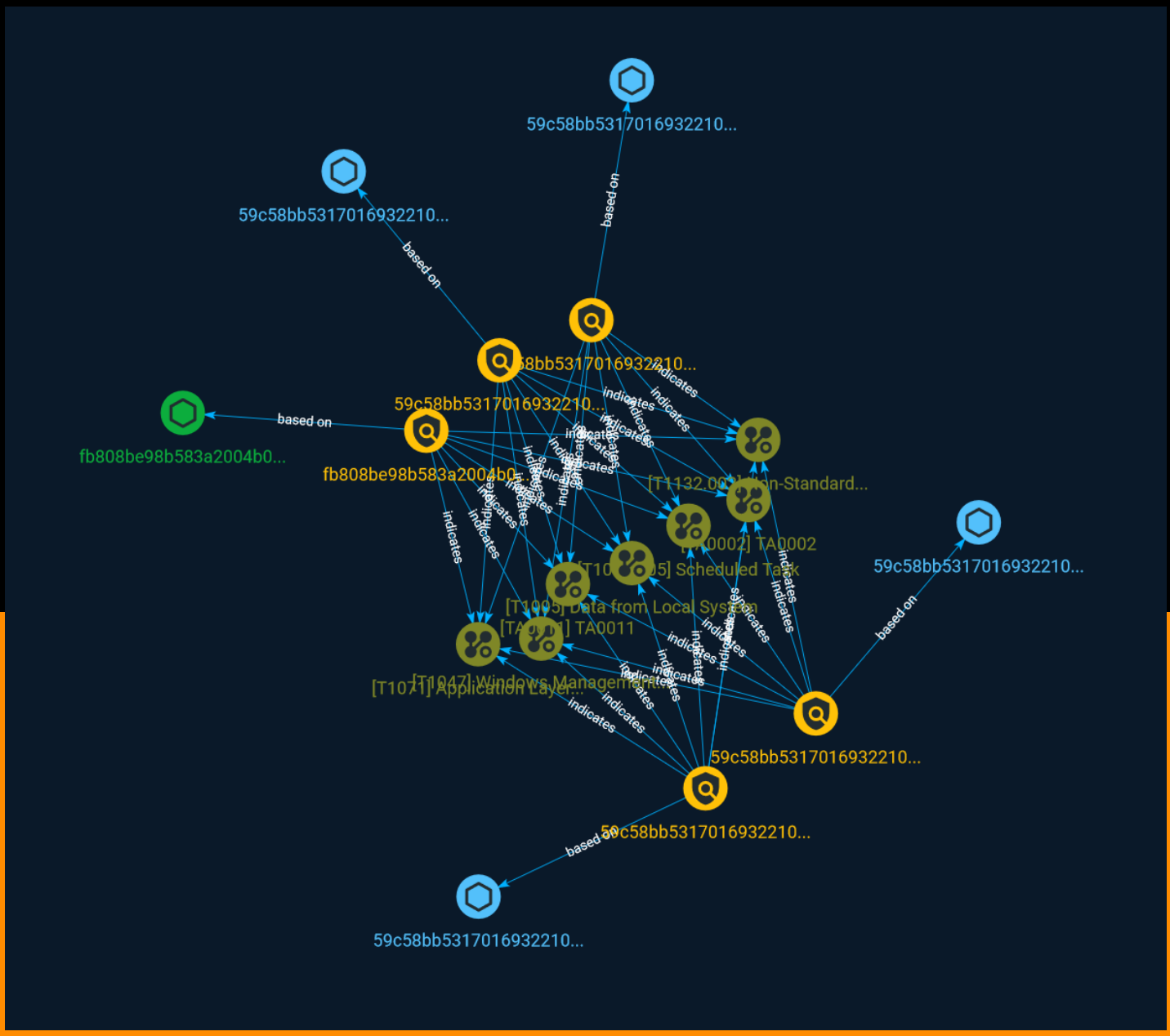

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Discover a comprehensive technical analysis of Lu0Bot, a Node.js malware with near-unlimited capabilities, and collect IOCs.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
TA0002
ID
TA0002
Name
Windows Management Instrumentation
ID
T1047
Description
Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015) An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote

Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)

Name

Scheduled Task

ID

T1053.005

Description

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task. The deprecated [at](https://attack.mitre.org/software/S0110) utility could also be abused by adversaries (ex: [At](https://attack.mitre.org/techniques/T1053/002)), though `at.exe` can not access tasks created with `schtasks` or the Control Panel. An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent) Adversaries may also create "hidden" scheduled tasks (i.e. [Hide Artifacts](https://attack.mitre.org/techniques/T1564)) that may not be visible to defender tools and manual queries used to enumerate tasks. Specifically, an adversary may hide a task from `schtasks /query` and the Task Scheduler by deleting the associated Security Descriptor (SD) registry value (where deletion of this value must be completed using SYSTEM permissions).(Citation: SigmaHQ)(Citation: Tarrask scheduled task) Adversaries may also employ alternate methods to hide tasks, such as altering the metadata (e.g., `Index` value) within associated registry keys.(Citation: Defending Against Scheduled Task Attacks in Windows Environments)

Name

Data from Local System

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

TA0011

ID

TA0011

Name

Non-Standard Encoding

ID

T1132.002

Description

Adversaries may encode data with a non-standard data encoding system to make the content of command and control traffic more difficult to detect. Command and control (C2)

information can be encoded using a non-standard data encoding system that diverges from existing protocol specifications. Non-standard data encoding schemes may be based on or related to standard data encoding schemes, such as a modified Base64 encoding for the message body of an HTTP request.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Indicator

Name

59c58bb5317016932210991180008a04a642894b5363501835669022123 2f.hsh.juz09.cfd

Pattern Type

stix

Pattern

[hostname:value = '59c58bb5317016932210991180008a04a642894b5363501835669022123 2f.hsh.juz09.cfd']

Name

fb808be98b583a2004b0af7b6f4bf5e3419d8b6a385c5ce4e8fab4ddc0b48428

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fb808be98b583a2004b0af7b6f4bf5e3419d8b6a385c5ce4e8fab4ddc0b48428']

Name

59c58bb5317016932210991180108a04a642894b536350183566902212 32f.hsh.juz09.cfd

Pattern Type

stix

Pattern

[hostname:value = '59c58bb5317016932210991180108a04a642894b536350183566902212 32f.hsh.juz09.cfd']

Name

59c58bb5317016932210991180208a04a642894b536350183566902212 32f.hsh.juz09.cfd

Pattern Type

stix

Pattern

[hostname:value = '59c58bb5317016932210991180208a04a642894b536350183566902212 32f.hsh.juz09.cfd']

Name

59c58bb5317016932210991180209a04a642894b536350183566902212 32f.hsh.juz09.cfd

Pattern Type

stix

Pattern

[hostname:value =
'59c58bb5317016932210991180209a04a642894b5363501835669022l232f.hsh.juz09.cfd']

StixFile

Value
fb808be98b583a2004b0af7b6f4bf5e3419d8b6a385c5ce4e8fab4ddc0b48428

Hostname

Value
59c58bb5317016932210991180108a04a642894b5363501835669022l232f.hsh.juz09.cfd
59c58bb5317016932210991180209a04a642894b5363501835669022l232f.hsh.juz09.cfd
59c58bb5317016932210991180208a04a642894b5363501835669022l232f.hsh.juz09.cfd
59c58bb5317016932210991180008a04a642894b5363501835669022l232f.hsh.juz09.cfd

External References

- https://otx.alienvault.com/pulse/651ebf808c85ed605dbc0b57
- https://any.run/cybersecurity-blog/lu0bot-analysis/?utm_source=hacker_news&utm_medium=article&utm_campaign=lu0bot0928&utm_content=linktoblog