May 02 2024

NETMANAGEIT

Intelligence Report

Linux Trojan - Xorddos with Filename eyshcjdmzg

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This analysis examines a recurring Linux trojan called Xorddos, which is a distributed denial-of-service (DDoS) malware. It provides details on various file hashes associated with the malware, as well as indicators of compromise (IOCs) such as IP addresses, domains, and email addresses. The analysis includes information from sandbox environments and compares findings with other online sandboxes. It aims to provide insights into the tactics, techniques, and procedures employed by this malware campaign.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

lib.xlsxpi.enoan2107.com

Pattern Type

stix

Pattern

[hostname:value = 'lib.xlsxpi.enoan2107.com']

Name

keld@dkuug.dk

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** True - **Deliverability:** low - **Frequent Complainer:** True - **Spam Trap Score:** medium - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** True - **Sanitized Email:** keld@dkuug.dk - **Domain Age:** {'human': '37 years ago', 'timestamp': 562502957, 'iso': '1987-10-29T05:49:17-05:00'} - **First Seen:** {'human': '7 years ago', 'timestamp': 1483250461, 'iso': '2017-01-01T01:01:01-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'keld@dkuug.dk']

Name

http://lib.xlsxpi.enoan2107.com:112

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 427472 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Malicious Websites - **Domain Age:** {'human': '3 years ago', 'timestamp': 1627348058, 'iso': '2021-07-26T21:07:38-04:00'} - **IPQS: Domain:** lib.xlsxpi.enoan2107.com - **IPQS: IP Address:** 23.235.171.197

Pattern Type

stix

Pattern

[url:value = 'http://lib.xlsxpi.enoan2107.com:112']

Name

f0e4649181ee9917f38233a1d7b6cbb98c9f7b484326f80c1bebc1fa3aef0645

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0e4649181ee9917f38233a1d7b6cbb98c9f7b484326f80c1bebc1fa3aef0645']

Name

ecc33502fa7b65dd56cb3e1b6d3bb2c0f615557c24b032e99b8acd40488fad7c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ecc33502fa7b65dd56cb3e1b6d3bb2c0f615557c24b032e99b8acd40488fad7c']

Name

ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73']

Name

cd9bc23360e5ca8136b2d9e6ef5ed503d2a49dd2195a3988ed93b119a04ed3a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd9bc23360e5ca8136b2d9e6ef5ed503d2a49dd2195a3988ed93b119a04ed3a9']

Name

b39633ff1928c7f548c6a27ef4265cfd2c380230896b85f432ff15c7c819032c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b39633ff1928c7f548c6a27ef4265cfd2c380230896b85f432ff15c7c819032c']

Name

b4a86fdf08279318c93a9dd6c61ceafc9ca6e9ca19de76c69772d1c3c89f72a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b4a86fdf08279318c93a9dd6c61ceafc9ca6e9ca19de76c69772d1c3c89f72a8']

Name

218.92.0.60

Description

ISP: CHINANET-BACKBONE **OS:** - ---------- Services: **53:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '218.92.0.60']

Name

98e53e2d11d0aee17be3fe4fa3a0159adef6ea109f01754b345f7567c92ebebb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '98e53e2d11d0aee17be3fe4fa3a0159adef6ea109f01754b345f7567c92ebebb']

Attack-Pattern

Name
T1081
ID
T1081
Name
T1008
ID
T1008
Description
Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.
Name
T1052
ID

T1052

Description

Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

Name

T1189

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver

Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

T1213

ID

T1213

Description

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization. The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository: * Policies, procedures, and standards * Physical / logical network diagrams * System architecture diagrams * Technical system documentation * Testing / development credentials * Work / project schedules * Source code snippets * Links to network shares and other internal resources Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include web-based platforms such as [Sharepoint](https://attack.mitre.org/

techniques/T1213/002) and [Confluence](https://attack.mitre.org/techniques/T1213/001), specific services such as Code Repositories, IaaS databases, enterprise databases, and other storage infrastructure such as SQL Server.

Name

T1614

ID

T1614

Description

Adversaries may gather information in an attempt to calculate the geographical location of a victim host. Adversaries may use the information from [System Location Discovery](https://attack.mitre.org/techniques/T1614) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to infer the location of a system using various system checks, such as time zone, keyboard layout, and/or language settings. (Citation: FBI Ragnar Locker 2020)(Citation: Sophos Geolocation 2016)(Citation: Bleepingcomputer RAT malware 2020) Windows API functions such as `GetLocaleInfoW` can also be used to determine the locale of the host.(Citation: FBI Ragnar Locker 2020) In cloud environments, an instance's availability zone may also be discovered by accessing the instance metadata service from the instance.(Citation: AWS Instance Identity Documents) (Citation: Microsoft Azure Instance Metadata 2021) Adversaries may also attempt to infer the location of a victim host using IP addressing, such as via online geolocation IP-lookup services.(Citation: Securelist Trasparent Tribe 2020)(Citation: Sophos Geolocation 2016)

Name

T1078

ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

T1098

ID

T1098

Description

Adversaries may manipulate accounts to maintain and/or elevate access to victim systems. Account manipulation may consist of any action that preserves or modifies adversary access to a compromised account, such as modifying credentials or permission groups. (Citation: FireEye SMOKEDHAM June 2021) These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://attack.mitre.org/techniques/T1078).

Name

T1593

ID

T1593

Description

Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.(Citation: Cyware Social Media)(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking) Adversaries may search in different online sites depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Phishing](https://attack.mitre.org/techniques/T1566)).

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the

adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A) Some files and directories may require elevated or specific user permissions to access.

Name

T1071

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.(Citation: Mandiant APT29 Eye Spy Email Nov 22)

Name

T1583

ID

T1583

Description

Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Some infrastructure providers offer free trial periods, enabling infrastructure acquisition at limited to no cost.(Citation: Free Trial PurpleUrchin) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy] (https://attack.mitre.org/techniques/T1090), including from residential proxy services. (Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing)(Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Malware

Name
Xorddos

Name
linux

Hostname

Value
lib.xlsxpi.enoan2107.com

Email-Addr

Value
keld@dkuug.dk

Url

Value
http://lib.xlsxpi.enoan2107.com:112

IPv4-Addr

Value
218.92.0.60

StixFile

Value
f0e4649181ee9917f38233a1d7b6cbb98c9f7b484326f80c1bebc1fa3aef0645
ecc33502fa7b65dd56cb3e1b6d3bb2c0f615557c24b032e99b8acd40488fad7c
ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
cd9bc23360e5ca8136b2d9e6ef5ed503d2a49dd2195a3988ed93b119a04ed3a9
b4a86fdf08279318c93a9dd6c61ceafc9ca6e9ca19de76c69772d1c3c89f72a8
b39633ff1928c7f548c6a27ef4265cfd2c380230896b85f432ff15c7c819032c
98e53e2d11d0aee17be3fe4fa3a0159adef6ea109f01754b345f7567c92ebebb

External References

- https://isc.sans.edu/diary/rss/30880
- https://otx.alienvault.com/pulse/66329e2d6c3c1f2ec577888d