LOG4J
VULNERABILITY

REVEALD

INTRODUCTION

LOG4J IS A JAVA FRAMEWORK USED AS A LOGGING ENGINE, TO PERFORM CONSOLE OUTPUTS OR ERROR TRACKING.

This technology is very often used and is found in most Internet services. It is practical, easy to use, and understand. It is open source and developed in Java by the Apache Software Foundation, allowing software developers to choose output and verbose messages or "logs" at run time, rather than at compile time. In December, the cybersecurity community realized that log4j could be used to require a program to log a line of malicious code, causing that code to run in the process, thereby allowing cybercriminals to take control of servers in a simple way.

Log4j has been part of Java programming and frequently used since the mid-1990s. Cloud storage companies like Google, Amazon, and Microsoft, which are the digital hotline for millions of other applications, have been hit hard by log4j exploits. The same goes for other IT giants like IBM, Oracle, and Salesforce, as well as thousands of Internet-connected devices like televisions and security cameras.
This easily accessible vulnerability has enabled hackers to steal information and deliver malicious payloads. It creates a new opportunity to infiltrate a huge range of system environments, enabling many types of malware attacks through remote control of the exploited server. This does not mean that everyone will suffer an attack, but it is certainly a widespread vulnerability that makes exploits much easier.

DESCRIPTION

Log4j is used mostly in commercial and consumer applications, websites and services, and operational technology products, for the purpose of recording security and performance information. It is part of the Apache Software Foundation projects and is commonly used in Apache webserver and JAVA application implementations.

An unauthenticated remote cyber-attack could exploit this vulnerability to take control of a system that has the log4j vulnerability present.
In the events that began in December 2021, the log4j attacks have been produced by executing code using the Java Naming and Directory Interface (JNDI) to generate communications between the developers and the library. JNDI is a programming interface (API) that generates inputs to naming and directory processes in the form of objects and data that may be called from an internal or external service. It supports a multitude of protocols such as LDAP, RMI, CORBA, etc.

It is highly recommended to update the vulnerable versions of log4j in the services and products that use it, to Log4j 2.17.0 (for Java 8), 2.12.3 (for Java 7), and 2.3.1 (for Java 6), and to continue to monitor the latest updates and procedures to mitigate the risk.

The vulnerability that affects the Apache Log4j library is identified as CVE-2021-44228 RCE in versions 2.0-beta9 to 2.14.1. It exists in the action performed by the Java Naming and Directory Interface (JNDI) to resolve the variables. The affected versions have similarities such as use of JNDI and message search override.

A potential attacker can exploit CVE-2021-44228 on a vulnerable system causing that system to execute arbitrary code. When the attacker exploits the vulnerability, he begins to take full control of the victim's system. With the result of stealing information, uploading ransomware or other malware, or performing other malicious activities.

In just 3 days it had more than 60 attack variants on log4j, in which many malware samples were detected to exploit vulnerabilities, such as miners, Trojans, and ransomware, including the new Khonsari ransomware variant.

VULNERABILITIES ATTACKED

- CVE-2021-44228
- CVE 2021-4104
- CVE 2021-45046
- CVE-2021-45105

NEWS

A potential attacker can exploit CVE-2021-44228 on a vulnerable system causing that system to execute arbitrary code. When the attacker exploits the vulnerability, he begins to take full control of the victim's system. With the result of stealing information, uploading ransomware or other malware, or performing other malicious activities.

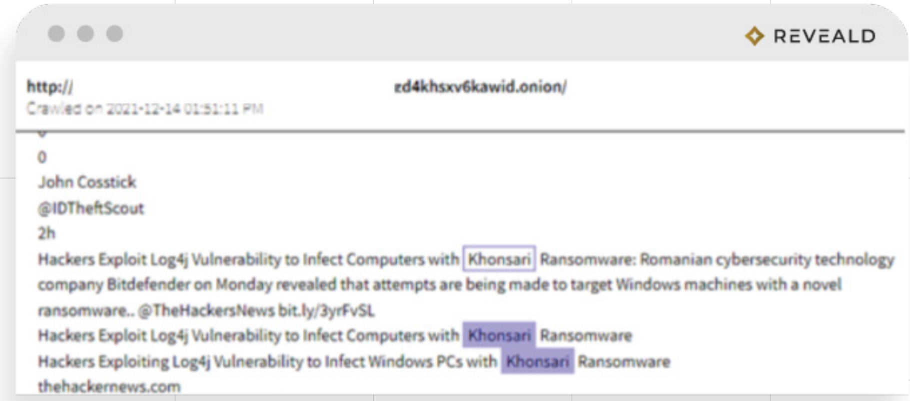
- URL lists
- Fuzzing of more than 60 headers with HTTP
- HTTP POST parameters
- JSON parameters
- DNS callback
- WAF BYPASS Payloads

TOOLS

KHONSARI.RANSOM

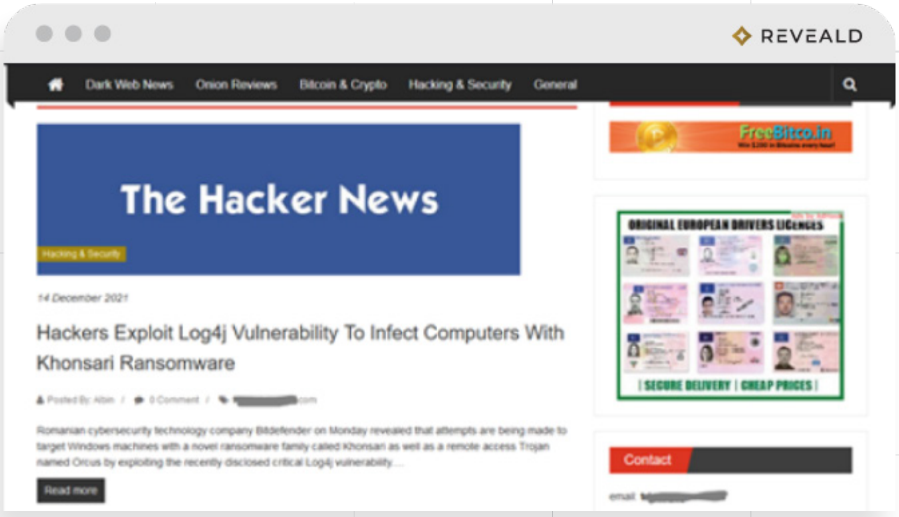
(SEE SEPARATE KHONSARI PACKAGE)

This ransomware is directed to Windows servers, uses the .NET framework while running stops the antivirus, then lists the drives that are connected and finally it starts encrypting the files that are in each one of them. It has been seen in use with Orcus.RAT as a precursor payload.
It creates a ransom note for the victim to communicate with the developers, and first became known in December 2021 as part of exploits for the log4j vulnerability identified in CVE-201-44228, also known as log4shell.
The files attacked by this ransomware are encrypted and assigned a new file extension ending in .Khonsari and the form of payment requested is through cryptocurrencies.



http:// zd4khsxv6kawid.onion/
Crawled on 2021-12-14 01:51:11 PM

0
John Cosstick
@IDTheftScout
2h
Hackers Exploit Log4j Vulnerability to Infect Computers with Khonsari Ransomware: Romanian cybersecurity technology company Bitdefender on Monday revealed that attempts are being made to target Windows machines with a novel ransomware.. @TheHackersNews bit.ly/3yrFvSL
Hackers Exploit Log4j Vulnerability to Infect Computers with Khonsari Ransomware
Hackers Exploiting Log4j Vulnerability to Infect Windows PCs with Khonsari Ransomware
thehackernews.com



14 December 2021

Hackers Exploit Log4j Vulnerability To Infect Computers With Khonsari Ransomware

Posted By: Albin / 0 Comment / [redacted].com

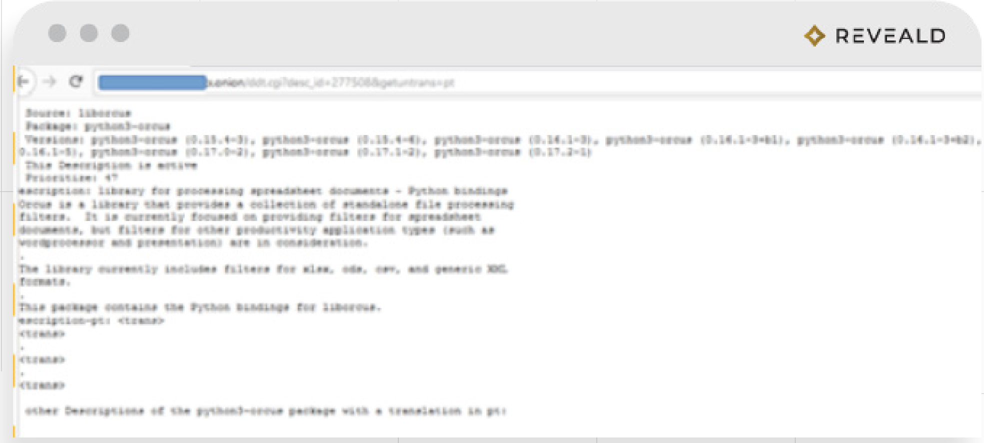
Romanian cybersecurity technology company Bitdefender on Monday revealed that attempts are being made to target Windows machines with a novel ransomware family called Khonsari as well as a remote access Trojan named Orcus by exploiting the recently disclosed critical Log4j vulnerability....

email [redacted]

Orcus.RAT

Orcus has been introduced as a Remote Administration Tool (RAT) since early 2016. It contains all the features expected of RAT and more. The thorough list of commands is documented on their website. In log4j attacks, it has been associated with the recent emergence of the Khonsari ransomware. What sets Orcus apart is its ability to load custom user-developed plugins, as well as plugins available from the Orcus repository. In addition, users can also run C# and VB.net code on the remote machine in real-time.

When Orcus RAT finds a server, it performs a process called PK Holdings.exe from the task manager. Then an attacker can configure registry entries, enable advanced system plug-ins, and other suspicious activities. The goal is for the criminal to have full control of the system remotely. When this happens, cyber criminals start collecting the victim's banking details, recording keystrokes, recording webcam video, and stealing Bitcoin wallets.



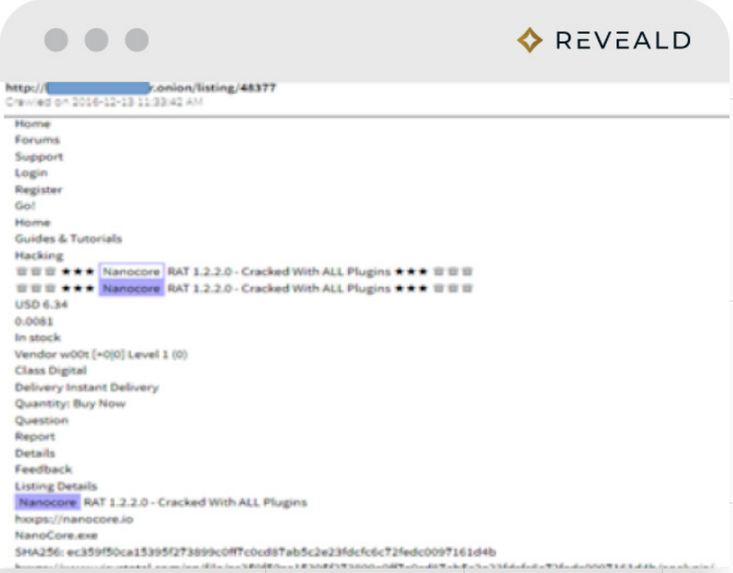
```
[redacted].onion/ddt.cgi?desc_id=277508&getuntrans=pt

 Source: liborcus
 Package: python3-orcus
 Versions: python3-orcus (0.15.4-3), python3-orcus (0.15.4-6), python3-orcus (0.16.1-3), python3-orcus (0.16.1-3+b1), python3-orcus (0.16.1-3+b2),
0.16.1-5), python3-orcus (0.17.0-2), python3-orcus (0.17.1-2), python3-orcus (0.17.2-1)
 This Description is active
 Prioritize: 47
escription: library for processing spreadsheet documents - Python bindings
Orcus is a library that provides a collection of standalone file processing
filters.  It is currently focused on providing filters for spreadsheet
documents, but filters for other productivity application types (such as
wordprocessor and presentation) are in consideration.
.
The library currently includes filters for xlsx, ods, csv, and generic XML
formats.
.
This package contains the Python bindings for liborcus.
escription-pt: <trans>
<trans>
.
<trans>
.
<trans>

 other Descriptions of the python3-orcus package with a translation in pt:
```

INanoCore.RAT

A Remote Access Trojan (RAT) is a type of malicious program that helps a criminal to monitor and control a computer or network. RATs are a type of malware similar to legitimate remote access programs.

The NanoCore RAT was first discovered in 2013 when it was up for sale on secret forums. It has many functions, including keyloggers and password stealers that can transmit data remotely to malware operators. It is also capable of spoofing, displaying webcam images, locking the screen, downloading and stealing files, and more. The RAT collects the following data and sends it to its server:

- Username and password for the browser
- FTPP (File Transfer Protocol) client or account information stored by file management software
- Email DS of popular email clients



```
http://[redacted].onion/listing/48377
Crawled on 2016-12-13 11:33:42 AM
Home
Forums
Support
Login
Register
Go!
Home
Guides & Tutorials
Hacking
▥ ▥ ▥ ★★★ Nanocore RAT 1.2.2.0 - Cracked With ALL Plugins ★★★ ▥ ▥ ▥
▥ ▥ ▥ ★★★ Nanocore RAT 1.2.2.0 - Cracked With ALL Plugins ★★★ ▥ ▥ ▥
USD 6.34
0.0081
In stock
Vendor w00t [+0|0] Level 1 (0)
Class Digital
Delivery Instant Delivery
Quantity: Buy Now
Question
Report
Details
Feedback
Listing Details
Nanocore RAT 1.2.2.0 - Cracked With ALL Plugins
hxxps://nanocore.io
NanoCore.exe
SHA256: ec359f50ca15395f273899c0ff7c0cd87ab5c2e23fdcfc6c72fedc0097161d4b
```

Bitcoinminer.Miner

This malware infects a computer by going low profile to to make use of the target's processing resources, to generate cryptocurrencies, such as Bitcoin. Cryptomining has been a common type of attack exploiting the log4j vulnerability. Increasingly, criminals want to use processing resources of their attack targets to generate quick income through cryptomining, due to the quick return on investment while evading discovery.

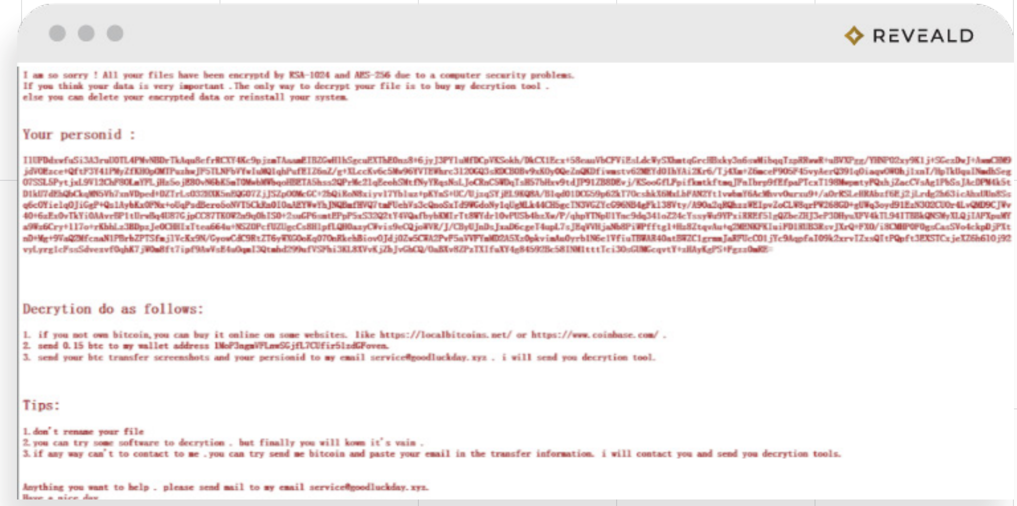
Disguisedxmrigminer.Trojan

This malware is another cryptomining trojan, Once downloaded and executed it copies itself in multiple paths. It creates a process and modifies the system registry to be able to run at every startup.

TellYouThePass.Ransom

(SEE SEPARATE TELLYOUTHEPASS PACKAGE)

TellYouThePass ransomware is malware compiled in Golang, making it more versatile for use with multiple operating systems, including Windows and Unix. Although it was first seen in March 2019, regained notoriety in December 2021 due to its use together with the Log4shell exploit on vulnerable computers.



```
I am so sorry ! All your files have been encryptd by RSA-1024 and AES-256 due to a computer security problems.
If you think your data is very important .The only way to decrypt your file is to buy my decrytion tool .
else you can delete your encrypted data or reinstall your system.


Your personid :

[illegible]



Decrytion do as follows:

1. if you not own bitcoin,you can buy it online on some websites. like https://localbitcoins.net/ or https://www.coinbase.com/ .
2. send 0.15 btc to my wallet address 1MoP3ngmVFLmwSGjfL7CUfir51zdGFoven.
3. send your btc transfer screenshots and your persionid to my email service@goodluckday.xyz . i will send you decrytion tool.


Tips:

1.don't rename your file
2.you can try some software to decrytion . but finally you will kown it's vain .
3.if any way can't to contact to me .you can try send me bitcoin and paste your email in the transfer information. i will contact you and send you decrytion tools.


Anything you want to help . please send mail to my email service@goodluckday.xyz.
Have a nice day
```