Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement

advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement

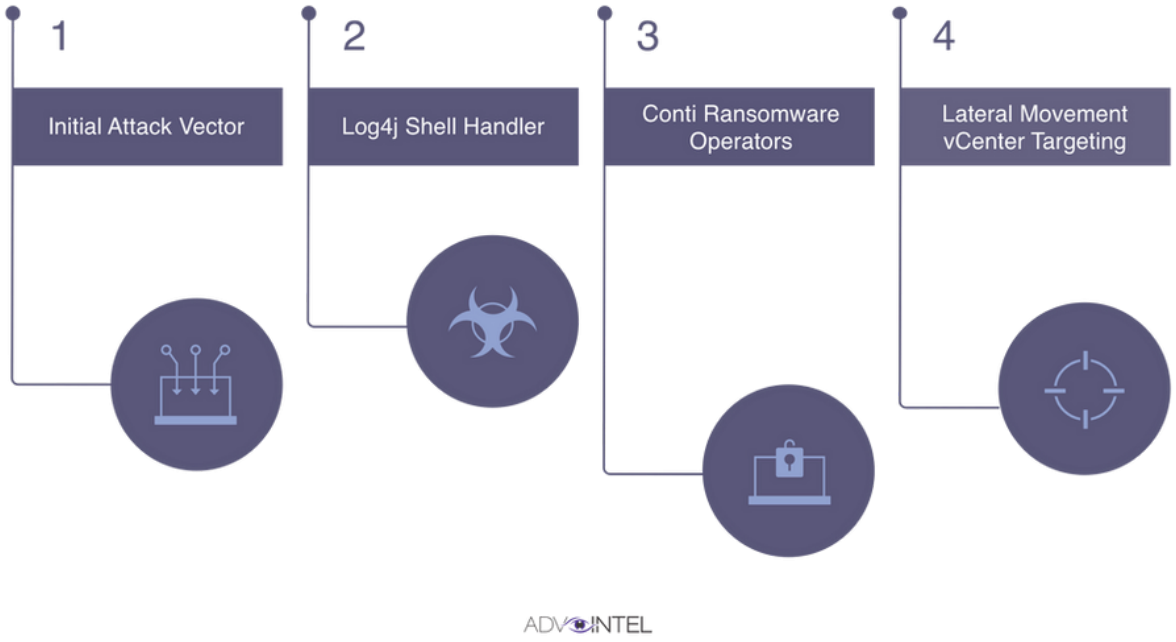
AdvIntel December 17, 2021

- Dec 17, 2021
-
- 5 min read

By Vitali Kremez & Yelisey Boguslavskiy

This redacted report is based on our actual proactive victim breach intelligence and subsequent incident response (not a simulated or sandbox environment) identified via unique high-value Conti ransomware collections at AdvIntel via our product "Andariel."

This is a redacted TLP:WHITE version of the larger AdvIntel findings.



Conti Ransomware Log4Shell Operation

Background: Log4Shell Vulnerability

On December 11, 2021, the US Cybersecurity and Infrastructure Security Agency (CISA) released an urgent announcement on possibly the most important vulnerability of recent years:

“To be clear, this (Log4j2) vulnerability poses a severe risk. We urge all organizations to join us in this essential effort and take action. By bringing together key government and private sector partners via the JCDC, including our partners at the FBI and NSA, we will ensure that our country’s strongest capabilities are brought to bear in an integrated manner against this risk.”

CISA's concerning tone is understandable: the new vulnerability is not another hidden path for a malicious attack. Embedded deeply in the stack level it offers the attackers an entire new dimension of offensive patterns. The depth is transferred to scale as this vulnerability affects core library components supporting thousands of networks, companies, and machines across the world.

Recorded in the vulnerability database on **Friday, November 26, 2021,** the Apache Log4j2 Java-based logging library vulnerability CVE-2021-44228 has the highest possible severity score of Base Score: **10.0 CRITICAL** allowing direct remote code execution on the vulnerable machines. Due to its core component impact, this vulnerability in some way can be compared to the Apache Struts vulnerability **CVE-2019-0230: Apache Struts OGNL Remote Code Execution** that led to the breach of **Equifax**.

Multiple technologies and products run Log4j2 library including popular vCenter, Kafka, Elastic, and Minecraft presenting an attack surface for the attackers.

The current activity surrounding the vulnerability resulted in massive world scanning with the payloads running from miners, unix DDoS malware, and framework stagers pushed to the compromised hosts.

Conti: A Quest For Ultimate Ransomware Exploitation

Naturally, this new attack domain became the focal point of hackers' interests. Hacker teams suspected to work for foreign governments and US adversaries were quickly spotted to investigate Log4j2. And as the new adversarial pattern seen with ProxyLogon in March 2021 suggests, if one day a major CVE is spotted by APTs, the next week it is weaponized by ransomware.

And indeed, a week after the Log4j2 vulnerability became public, AdvIntel discovered the most concerning trend - the exploitation of the new CVE by one of the most prolific organized ransomware groups - Conti.

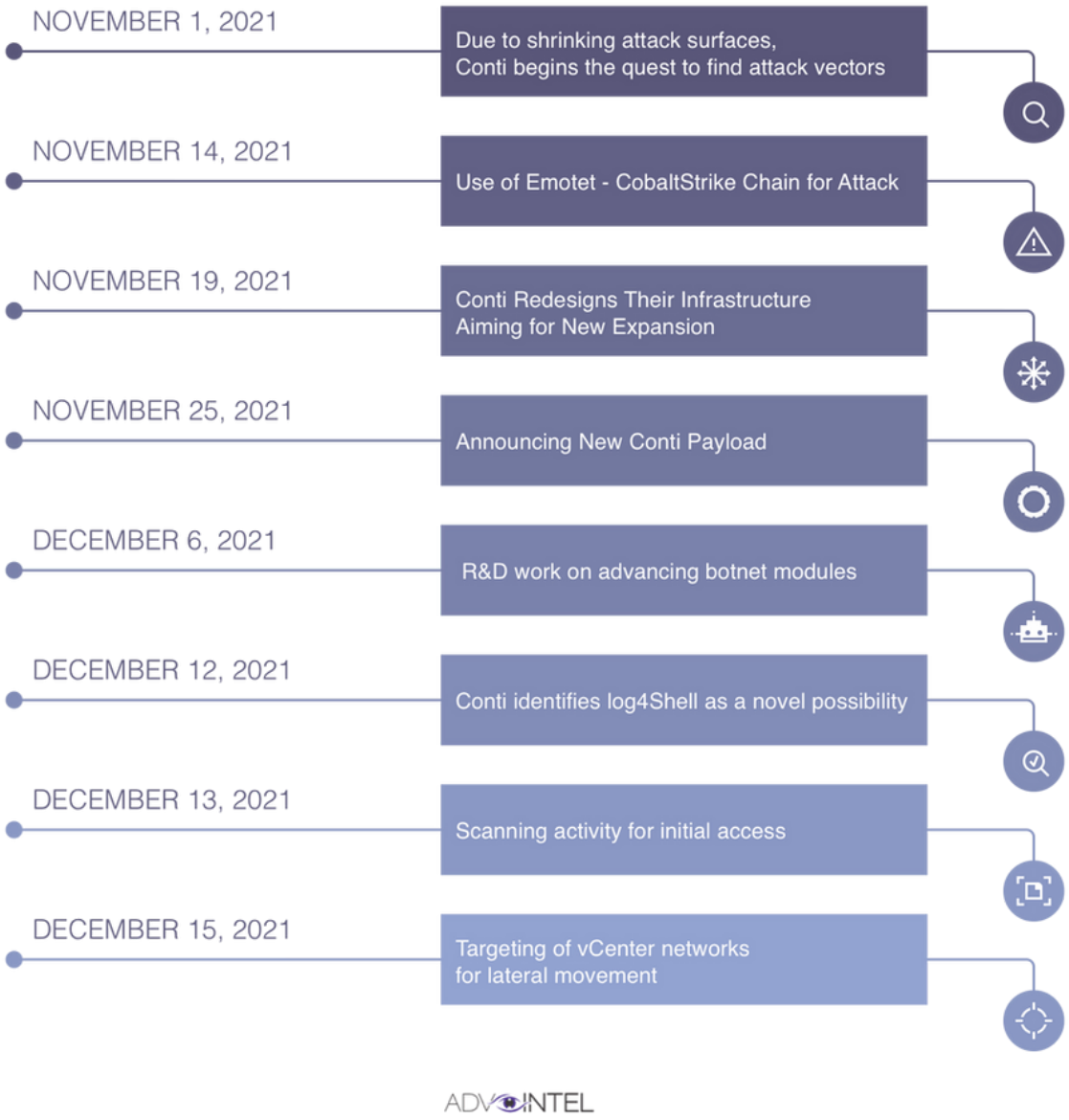
Conti plays a special role in today's threat landscape, primarily due to its scale. Divided on several teams and involving tenths of full-time members, the Russian-speaking Conti made over $150 million USD in the last six months, according to AdvIntel research into the ransomware logs. And they continue to expand. It is this expansion that has set Conti on a long quest of searching for new attack surfaces and methods. Since August, they have employed many new means: hidden RMM backdoors, new backup removal solutions, and, most recently, even an entire operation to revive Emotet.

Moreover, Conti already had a history of leveraging exploits as an initial attack vector and for lateral movement. For instance, the group leverages **Fortinet VPN vulnerability** CVE-2018-13379 to target unpatched devices for the initial attack vector. Conti favors PrintNightmare privilege elevation CVE-2021-34527/CVE-2021-1675, Zerologon (CVE-2020-1472), and ms17-010 for local privilege elevation and lateral movement on the compromised hosts.

As such, Log4j2 vulnerability appears at a time for Conti: at the moment when the syndicate has both the strategic intention and the capability to weaponize it for its ransomware goals.

Discovery: Conti Becomes The First Sophisticated Crimeware Ransomware Group Weaponizing Log4j2

Ransomware Exploitation Timeline: Conti Search for Newer Attack Vectors



- November 1, 2021 - Due to shrinking attack surfaces, Conti begins the quest to find new attack vectors
- November 14, 2021 - Use of Emotet - CobaltStrike Chain for Attack
- November 19, 2021 - Conti Redesigns Their Infrastructure Aiming for New Expansion
- November 25, 2021 - Announcing New Conti Payload
- December 6, 2021 - R&D work on advancing botnet modules
- December 12, 2021 - Conti identifies Log4Shell as a novel possibility
- December 13, 2021 - Scanning activity for initial access

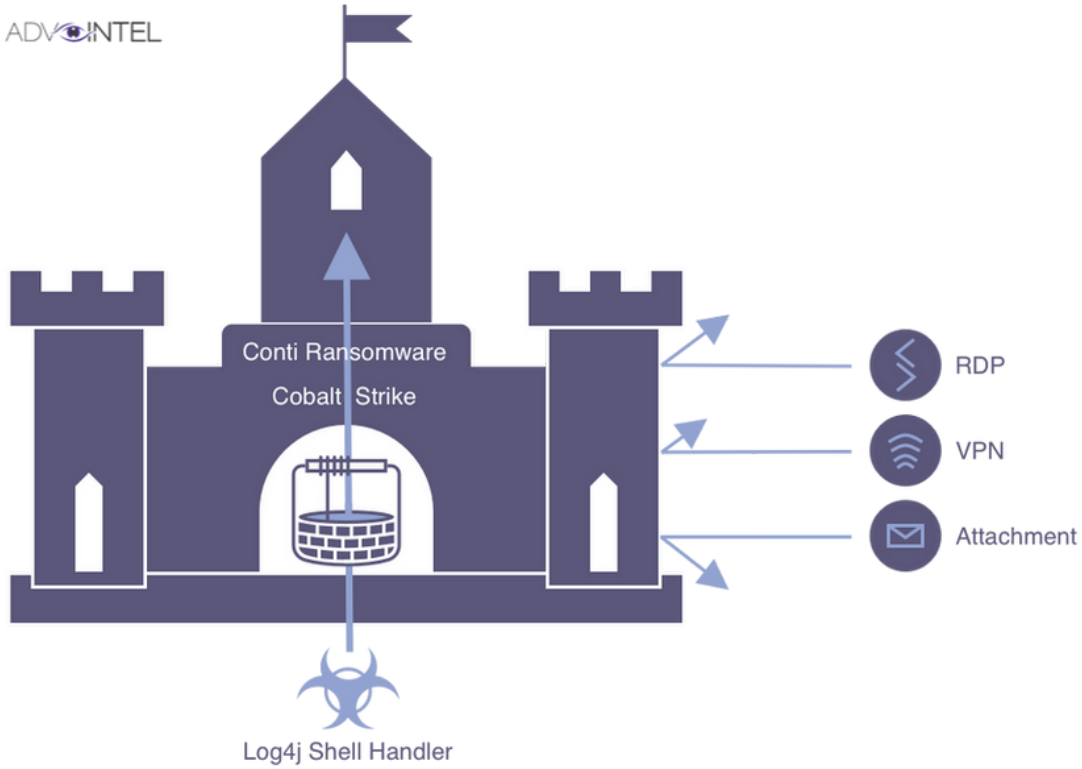
- December 15, 2021 - Targeting of vCenter networks for lateral movement

On December 12, through deep visibility into adversarial collections, AdvIntel discovered that multiple Conti group members expressed interest in the exploitation of the vulnerability for the initial attack vector resulting in the scanning activity leveraging the publicly available Log4J2 exploit. This is the first time this vulnerability entered the radar of a major ransomware group.

The current exploitation led to multiple use cases through which the Conti group tested the possibilities of utilizing the Log4J2 exploit. Most importantly, AdvIntel confirmed that the criminals pursued targeting specific vulnerable Log4J2 VMware vCenter for lateral movement directly from the compromised network resulting in vCenter access affecting US and European victim networks from the pre-existent Cobalt Strike sessions.

Early Warning: Ransomware Exploitation of Core Vulnerability

It is only a matter of time until Conti and possibly other groups will begin exploiting Log4j2 to its full capacity. It is recommended to patch the vulnerable system immediately and view the Log4j2 as a ransomware group exploitation vector.



AdvIntel provides direct customer access to targeting datasets related to CVE-2021-44228 Log4Shell exploitation from the Conti ransomware list. The Log4Shell dataset informs possible targeted devices from vulnerability scanner devices only. Targeted Searches are available using TLD & IP Range in Log4Shell Exposure Collections.

Recommendations & Mitigations

- The Dutch National Cyber Security Center shared a list of the affected software and recommendations linked to each one of them - https://github.com/NCSC-NL/log4shell/tree/main/software
- CVE-2021-44228 - VMSA-2021-0028 Workaround instructions to address CVE-2021-44228 in vCenter Server and vCenter Cloud Gateway (87081) - https://kb.vmware.com/s/article/87081

Mitre ATT&CK

Enterprise Attack - Course of Action

- Account Discovery Mitigation - T1087
- Brute Force Mitigation - T1110
- Credential Dumping Mitigation - T1003
- Data Encrypted Mitigation - T1022
- Data from Local System Mitigation - T1005
- Exploitation for Defense Evasion Mitigation - T1211
- Exploitation for Privilege Escalation Mitigation - T1068
- Exploitation of Remote Services Mitigation - T1210
- Network Service Scanning Mitigation - T1046
- PowerShell Mitigation - T1086
- Supply Chain Compromise Mitigation - T1195

Attack Pattern

- Spearphishing Attachment - T1193
- Supply Chain Compromise - T1195
- Command-Line Interface - T1059
- PowerShell - T1086
- Rundll32 - T1085
- Regsvr32 - T1117
- Scripting - T1064
- Data Encrypted for Impact - T1486
- Data Encrypted - T1022
- Remote Access Tools - T1219
- Domain Fronting - T1172
- Data from Local System - T1005
- Data from Network Shared Drive - T1039

- Email Collection - T1114
- Pass the Hash - T1075
- Pass the Ticket - T1097
- Logon Scripts - T1037
- Exploitation of Remote Services - T1210
- Kerberoasting - T1208
- LLMNR/NBT-NS Poisoning and Relay - T1171
- Credentials in Files - T1081
- Brute Force - T1110
- Network Share Discovery - T1135
- File and Directory Discovery - T1083
- Domain Trust Discovery - T1482
- Process Hollowing - T1093
- Process Doppelgänging - T1186
- Process Injection - T1055
- New Service - T1050
- Exploitation for Privilege Escalation - T1068