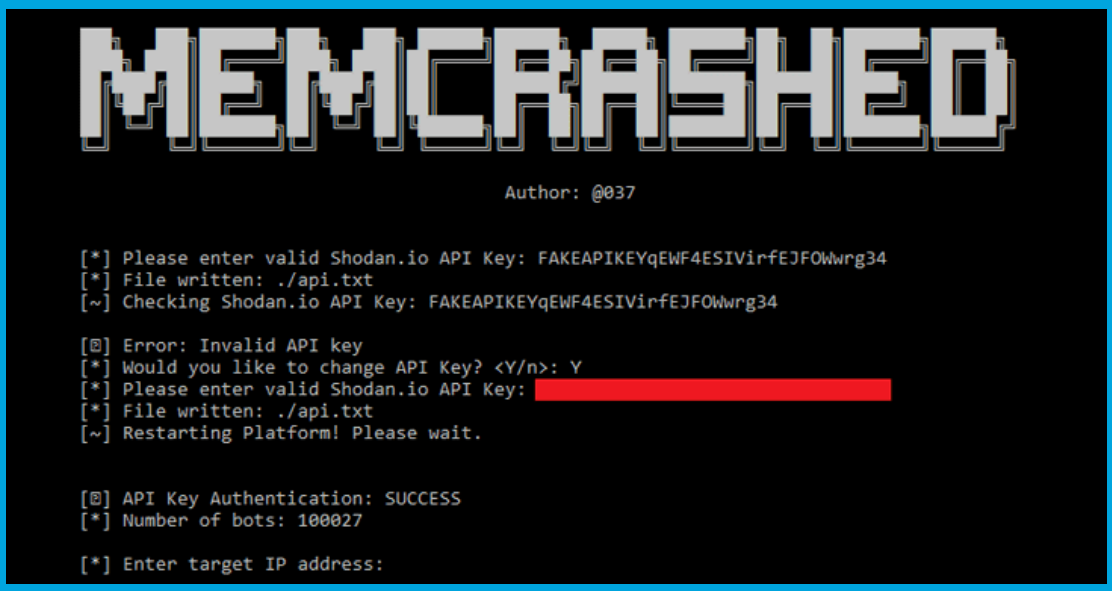
kindred

Security Newsletter

12 March 2018

Subscribe to this newsletter

MemCached DDoS continues, with new ways to mitigate the issue



Two separate proofs-of-concept (PoC) exploit code for Memcached amplification attack have been released online that could allow even script-kiddies to launch massive DDoS attacks using UDP reflections easily. Bonus—its description already includes a list of nearly 17,000 potential vulnerable Memcached servers left exposed on the Internet. The first DDoS tool is written in C programming language and works with a list of pre-compiled list of vulnerable Memcached servers. The second Memcached DDoS attack tool is written in Python that uses Shodan search engine API to obtain a fresh list of vulnerable Memcached servers and then sends spoofed source UDP packets to each server.

Memcached reflections that recently fueled two most largest amplification DDoS attacks in the history have also helped other cybercriminals launch nearly 15,000 cyber attacks against 7,131 unique targets in last ten days, a new report revealed. The maximum number of active

vulnerable Memcached servers at a time that participated in the DRDoS attacks was 20,612. Last week we saw two record-breaking DDoS attacks—1.35 Tbps hit Github and 1.7 Tbps attack against an unnamed US-based company—which were carried out using a technique called amplification/reflection attack.

Security researcher Amir Khashayar Mohammadi has released today a new tool named Memfixed that can help victims of DDoS attacks carried out via Memcached servers. The mitigation technique consists of sending a "flush_all" command to a Memcached server that is attacking a victim's network, part of a larger DDoS attack. The flush_all command wipes a Memcached server's cached memory, including the malicious payload that is executing the DDoS attack. In addition to flushing the cache, Memfixed also supports sending a "shutdown" command to attacking servers that actually shuts down the memcached daemon. If you are under attack and are considering using this tool, it should be noted that its use is most likely illegal in almost all countries. This is because you are accessing a a server that you do not own and modifying its behavior without permission. Therefore, it is strongly advised that you contact law enforcement and seek legal advice before considering the use of this tool.

Exploit Code released

Over 15 000 DDoS attacks in the last 10 days

Memfixed Tool Helps Mitigate Memcached-Based DDoS Attacks

Patch now! Half a million Exim mail servers need an urgent update

About half a million email systems running the hugely popular Exim Mail Transfer Agent (MTA) have yet to be patched for a potentially dangerous security flaw made public earlier this week. Disclosed to the software's maintainers in early February by Meh Chang, from security firm Devcore Security Consulting, the Exim vulnerability is a one-byte buffer overflow in the software's Base64 decoding.

The bug —tracked as CVE-2018-6789— is categorized as a "pre-auth remote code execution," meaning an attacker could trick the Exim email server into running malicious commands before the attacker would need to authenticate on the server. The main takeaway is that this flaw affects all Exim versions going back to its first appearance in 1995. At the time of writing, there is no public exploit code for taking advantage of vulnerable Exim servers. Would it really be hard to exploit? Granted, the PoC design involves a sophisticated sequence of memory manipulation but the MO is now in the public domain, forever.

The clock is ticking for unpatched servers and it's probably best not to wait and find out if somebody can find a way to turn a remotely triggerable bug into an RCE. Shodan, the search engine for internet-connected systems, pins the number of Exim servers in the low millions.

Read More

Even More

Hard-Coded Password in Cisco Software Lets Attackers Take Over Linux Servers

A medium yet critical vulnerability has been discovered in Cisco Prime Collaboration Provisioning software that could allow a local attacker to elevate privileges to root and take full control of a system.

Cisco Prime Collaboration Provisioning (PCP) application allows administrators to remotely control the installation and management of Cisco communication devices (integrated IP telephony, video, voicemail) deployed in the company and services for its subscribers.

The vulnerability (CVE-2018-0141) is due to a hard-coded password for Secure Shell (SSH), which could be exploited by a local attacker to connect to the PCP's Linux operating system and gain low-level privileges. The company is strongly encouraging users to update their software to the latest versions as soon as possible, as there are no workarounds to patch these vulnerabilities.

Read More

How Dutch Police Busted Hansa Dark Web Marketplace

Hansa was once the second largest dark web marketplace after AlphaBay selling everything from illegal drugs to stolen databases, credit card information and malicious software. But then Dutch Police came in, secretly took control of Hansa domain days before seizing its domain and arrested its administrators, buyers, and sellers.

The sudden bust shocked the customers as well as the IT security community keeping an eye on dark web marketplaces. However, now the Dutch police have revealed how they took over Hansa and shut down its large-scale drug-related operation.

The operation was so secretive and professional that 4 other moderators of Hansa were totally unaware of it. A couple of weeks later, Dutch police defaced Hansa with a message that said: “This hidden site has seized by the Dutch National Police.” According to officials, after shutting down Hansa, Dutch police extracted data on over 420,000 users and 10,000 home addresses leading to the arrests of a number of vendors while the search for more vendors is still on by Europol Moreover, they have also seized millions of dollars worth of Bitcoins.

Read More

Even More

Cutting room floor

- How to Use Bucket Policies to Help Secure Your Amazon S3 Data
- CIGslip Attack Bypasses Windows Code Integrity Guard (CIG)
- Debunking the fallacy that paid certificates are better than free certificates
- ComboJack Trojan Replaces Cryptocurrency Addresses Copied to Windows Clipboard
- Look-Alike Domains and Visual Confusion
- Group Policy Support Coming to Firefox 60
- Coinminer Campaigns Target Redis, Apache Solr, and Windows Servers
- Chinese Intelligence Agencies Are Doctoring the Country's Vulnerability Database
- Only Half of Those Who Paid a Ransomware Were Able to Recover Their Data
- ISPs Caught Injecting Cryptocurrency Miners and Spyware In Some Countries
- Avast Shares New Info on 2017 CCleaner Incident: Possible 3rd Stage Payload
- Researchers find 29 types of USB attacks, recommend never plugging into a USB you don't own

#Tech and #Tools

- Any.Run - An Interactive Malware Analysis Tool
- AppBandit - Fast web security proxy
- Paper on Kerberos decryption
- Amass: Subdomain enumeration tool
- XBruteForcer: CMS sign-in bruteforce tool
- Top Five Ways I Got Domain Admin on Your Internal Network before Lunch
- Encryption 101: How to break encryption
- Facebook now enforces HTTPS on website that supports it
- New Cryptocurrency Mining Malware Infected Over 500,000 PCs in Just Few Hours

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.